| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insira aqui a designação da entidade jurídica registada | | | | | | | |
| Número do documento:<br>PII15-FS | | | | | Título do documento:<br>**Política de Gestão de Incidentes e Violações de PII do Setor Financeiro** | | | | | | | |
| Versão:<br>1.0 | | Data de entrada em vigor:<br>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

| Standard / Regulation | Clause / Control / Article | Applicability | Coverage Type | Comment |
|---|---|---|---|---|
| ISO/IEC 27701:2025 | Clause 7.4; Clause 7.5 | Both | Supporting | Comunicações do PIMS e evidência documentada de incidentes |
| ISO/IEC 27701:2025 | Clause 8.1; Clause 8.2; Clause 8.3 | Both | Supporting | Controlo operacional, avaliação de riscos de privacidade e ligação ao tratamento de riscos de privacidade |
| ISO/IEC 27701:2025 | Clause 9.1; Clause 10.2 | Both | Supporting | Monitorização, avaliação, não conformidade, ação corretiva e melhoria |
| ISO/IEC 27701:2025 | Annex A.3.11 | Both | Primary | Planeamento e preparação da gestão de incidentes para o tratamento de PII |
| ISO/IEC 27701:2025 | Annex A.3.12 | Both | Primary | Resposta a incidentes de segurança da informação que envolvam PII |
| ISO/IEC 27701:2025 | Annex A.3.13; Annex A.3.14 | Both | Supporting | Requisitos legais, estatutários, regulamentares e contratuais, e proteção de registos |
| ISO/IEC 27701:2025 | Annex A.2.2.2; Annex A.2.2.6 | Processor | Supporting | Apoio ao acordo do cliente do subcontratante e às obrigações do cliente |
| GDPR | Article 5(2); Article 24 | Controller | Supporting | Responsabilização e responsabilidade do responsável pelo tratamento |
| GDPR | Article 26 | Joint Controller | Supporting | Coordenação da responsabilidade por incidentes |

| | | | | |
|---|---|---|---|---|
| | | | | entre responsáveis conjuntos pelo tratamento |
| GDPR | Article 28 | Both | Supporting | Assistência do subcontratante e obrigações contratuais do subcontratante |
| GDPR | Article 32 | Both | Supporting | Segurança do tratamento e capacidade de deteção de violações |
| GDPR | Article 33 | Both | Primary | Notificação de violação de dados pessoais e documentação de violações |
| GDPR | Article 34 | Controller | Primary | Comunicação de violações de dados pessoais aos titulares dos dados afetados |
| GDPR | Article 39 | Conditional | Supporting | Aconselhamento do DPO, monitorização, cooperação e apoio como ponto de contacto |
| DORA Regulation (EU) 2022/2554 | Article 17 | Conditional | Primary | Processo de gestão de incidentes relacionados com ICT para entidades financeiras abrangidas pelo âmbito |
| DORA Regulation (EU) 2022/2554 | Article 18 | Conditional | Primary | Critérios de classificação de incidentes relacionados com ICT e de ciberameaças significativas |
| DORA Regulation (EU) 2022/2554 | Article 19 | Conditional | Primary | Reporte de incidentes graves relacionados com ICT e notificação |

| | | | | |
|---|---|---|---|---|
| | | | | de ciberameaças significativas |
| DORA Regulation (EU) 2022/2554 | Article 20 | Conditional | Supporting | Conteúdo, prazos, modelos e procedimentos de reporte |
| NIS2 Directive (EU) 2022/2555 | Article 23 | Conditional | Supporting | Reporte de incidentes significativos quando aplicável |
| ISO/IEC 29100:2020 | Clause 5.11; Clause 5.12 | Both | Supporting | Princípios de segurança da informação e de conformidade em matéria de privacidade |
| ISO/IEC 29151:2022 | Clause 16.1.2; Clause 16.1.3 | Both | Supporting | Responsabilidades de resposta a incidentes de PII e reporte de eventos |
| ISO/IEC 27002:2022 | Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28 | Both | Supporting | Planeamento, avaliação, resposta, lições aprendidas e recolha de evidência de incidentes |
| ISO/IEC 27035-1:2023 | Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6 | Both | Supporting | Ciclo de vida do processo de gestão de incidentes |
| ISO/IEC 27035-2:2023 | Clause 4; Clause 6; Clause 10; Clause 11; Clause 12 | Both | Supporting | Política, plano, sensibilização, testes e lições aprendidas de incidentes |
| ISO/IEC 27035-3:2020 | Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12 | Both | Supporting | Operações de deteção, notificação, triagem, análise, resposta e reporte |
| ISO/IEC 27018:2020 | Annex A.10.1 | Conditional | Supporting | Expectativas de notificação por subcontratante de nuvem pública e de registo de violações |

## 1. Âmbito

1.1 Esta política define os requisitos para identificar, reportar, triar, classificar, avaliar, conter, notificar, documentar, encerrar e melhorar com base em incidentes de PII e violações de PII em âmbitos de PIMS do setor financeiro.

1.2 **Aviso de implementação:** Esta política é uma variante de substituição, para o setor financeiro, da PII15. Não deve ser implementada em simultâneo com a PII15 para o mesmo âmbito de PIMS, unidade de negócio, produto, ambiente de cliente, serviço regulado ou perímetro de evidência. As organizações devem selecionar a PII15 ou a PII15-FS para o mesmo âmbito, a fim de evitar obrigações duplicadas de gestão de incidentes, registos duplicados e trabalho duplicado de evidência de auditoria.

**1.3 Esta política aplica-se a:**

1.3.1 a organização quando atua como responsável pelo tratamento de PII num contexto do setor financeiro;

1.3.2 a organização quando atua como responsável conjunto pelo tratamento, sempre que seja necessária coordenação de responsabilidades por incidente ou violação;

1.3.3 a organização quando atua como subcontratante de PII para clientes do setor financeiro;

1.3.4 a organização quando atua como subcontratante subsequente para clientes do setor financeiro ou subcontratantes a montante;

1.3.5 sistemas, aplicações, serviços, processos, fornecedores, subcontratantes, subcontratantes subsequentes e terceiros que tratem, armazenem, transmitam, apoiem, acedam ou afetem de outro modo PII no âmbito de PIMS do setor financeiro.

1.4 Esta política utiliza o REG10 - Registo de Incidentes e Violações de PII como objeto de evidência principal para a gestão de incidentes e violações de PII do setor financeiro.

**1.5 Esta política utiliza objetos de evidência de suporte da seguinte forma:**

1.5.1 REG01 para o âmbito do PIMS e o contexto aplicável de partes interessadas, setor, clientes, contratos e reporte.

1.5.2 REG02 para atividades de tratamento afetadas, categorias de PII, categorias de titulares dos dados, finalidades, sistemas e serviços.

1.5.3 REG03 para a Declaração de Aplicabilidade e atualizações da aplicabilidade dos controlos, incluindo a substituição da PII15 pela PII15-FS para o mesmo âmbito.

1.5.4 REG04 para a ligação a riscos de privacidade, DPIA, risco residual e tratamento de riscos.

1.5.5 REG08 para evidência das interfaces de incidentes com subcontratantes, subcontratantes subsequentes, clientes, fornecedores e terceiros.

1.5.6 REG09 para ligação a transferências internacionais quando um incidente afete tratamento transfronteiriço.

1.5.7 REG11 para evidência de formação, sensibilização e competência de resposta a incidentes.

1.5.8 REG12 para evidência de auditoria, não conformidade, ação corretiva, revisão pela gestão e melhoria.

**1.6 Esta política depende das políticas PIMS relacionadas para controlos especializados:**

1.6.1 A PII03 rege o inventário de tratamento e os registos de fundamento de licitude.

1.6.2 A PII04 rege o aviso de privacidade e os controlos de transparência fora das comunicações específicas de violações.

1.6.3 A PII06 rege os pedidos de exercício de direitos dos titulares dos dados que surjam antes, durante ou após um incidente.

1.6.4 A PII07 rege a avaliação de riscos de privacidade e a metodologia de DPIA.

1.6.5 A PII08 rege os controlos de privacidade desde a conceção e por defeito.

1.6.6 A PII10 rege os controlos de retenção, apagamento e eliminação.

1.6.7 A PII12 rege os controlos das relações de privacidade com subcontratantes, subcontratantes subsequentes, fornecedores e terceiros.

1.6.8 A PII13 rege os mecanismos de transferência internacional de PII e os registos de risco de transferência.

1.6.9 A PII14 rege os controlos preventivos e de deteção de segurança e acesso a PII.

1.6.10 A PII16 rege a formação, sensibilização e competência em privacidade.

1.6.11 A PII17 rege a informação documentada e a gestão de evidência.

1.6.12 A PII18 rege a monitorização, auditoria interna, revisão pela gestão, não conformidade, ação corretiva e melhoria contínua.

1.6.13 A PII23 rege os controlos de subcontratante de PII na nuvem quando as obrigações de subcontratante de nuvem estejam no âmbito.

**1.7 Para efeitos desta política:**

1.7.1 "Incidente de PII" significa um evento suspeito ou confirmado que afetou, possa ter afetado ou possa razoavelmente afetar a confidencialidade, integridade, disponibilidade, tratamento lícito ou manuseamento autorizado de PII.

1.7.2 "Violação de PII" significa um incidente de PII confirmado que envolva destruição, perda, alteração, divulgação, acesso, indisponibilidade ou comprometimento de PII de forma não autorizada, ilícita, acidental ou não intencional.

1.7.3 "Incidente de dados pessoais do setor financeiro" significa um incidente de PII que afeta, possa afetar ou esteja razoavelmente relacionado com serviços financeiros regulados, clientes do setor financeiro, contrapartes financeiras, transações financeiras, operações financeiras ou tratamento de PII do setor financeiro.

1.7.4 "Incidente grave do setor financeiro" significa um incidente de dados pessoais do setor financeiro ou incidente ICT relacionado que cumpra os critérios documentados de materialidade ou reporte no REG10.

1.7.5 "Ciberameaça significativa" significa uma ciberameaça registada no REG10 que possa afetar materialmente serviços do setor financeiro, tratamento de PII, clientes, contrapartes ou operações abrangidos pelo âmbito.

1.7.6 "Avaliação da violação de dados pessoais" significa a avaliação documentada sobre se um incidente de PII constitui uma violação de PII, que PII e titulares dos dados são afetados, que riscos podem surgir, que notificações ou comunicações são exigidas e que ação corretiva é necessária.

1.7.7 "Tomada de conhecimento" significa o momento em que a organização tem um grau razoável de certeza de que ocorreu um incidente de segurança ou privacidade e de que PII foi ou pode ter sido comprometida.

1.7.8 "Incidente de alto impacto relativo a dados pessoais no setor financeiro" significa um incidente de PII que envolva tratamento de alto risco, categorias especiais ou PII altamente sensível, PII em larga escala, pessoas vulneráveis, clientes regulados, interrupção material do serviço, contrapartes financeiras, transações financeiras, impacto multijurisdicional, comprometimento de acesso privilegiado, exposição pública, ransomware, indisponibilidade de serviço ou impacto operacional, de cliente, financeiro ou reputacional significativo.

1.7.9 "Alteração material do incidente" significa informação nova ou alterada que afete o âmbito do incidente, a severidade, as categorias de PII, o impacto nos titulares dos dados, o impacto

no serviço, a classificação do setor financeiro, a decisão de notificação, o impacto no cliente, a causa raiz, a contenção, a recuperação, a ação corretiva ou as obrigações de reporte externo.

## 2. Finalidade

2.1 A finalidade desta política é assegurar que incidentes e violações de PII em contextos do setor financeiro sejam tratados de forma consistente, célere, lícita, segura e com evidência preparada para auditoria.

2.2 Esta política apoia a responsabilização ao exigir que incidentes e violações de PII do setor financeiro sejam registados no REG10 e ligados a registos de tratamento afetados, riscos de privacidade, relações com subcontratantes e subcontratantes subsequentes, registos de transferência, ações corretivas, registos de formação, decisões de reporte do setor financeiro e evidência de revisão pela gestão, quando acionados.

2.3 Esta política assegura que as obrigações de responsável pelo tratamento, responsável conjunto pelo tratamento, subcontratante e subcontratante subsequente sejam tratadas por regras de aplicabilidade distintas, mantendo simultaneamente um modelo integrado de evidência de incidentes e violações do setor financeiro.

## 3. Objetivos

### 3.1 Os objetivos desta política são:

3.1.1 assegurar que suspeitas de incidentes de dados pessoais do setor financeiro sejam reportadas e registadas prontamente;

3.1.2 assegurar que incidentes de dados pessoais do setor financeiro sejam triados e classificados através de critérios consistentes de privacidade, segurança, operação e setor;

3.1.3 assegurar que as avaliações de violações considerem PII afetada, titulares dos dados, sistemas, serviços, atividades de tratamento, subcontratantes, subcontratantes subsequentes, transferências, riscos, clientes, contrapartes e ações de remediação;

3.1.4 assegurar que as decisões de notificação do responsável pelo tratamento e de comunicação aos titulares dos dados sejam documentadas;

3.1.5 assegurar que as notificações de violação por subcontratantes e subcontratantes subsequentes a clientes ou partes a montante sejam efetuadas sem demora injustificada e de acordo com os acordos aplicáveis;

3.1.6 assegurar que os desencadeadores de reporte do setor financeiro sejam avaliados, documentados e acompanhados quando aplicável;

3.1.7 assegurar que a evidência seja preservada e protegida durante o tratamento do incidente;

3.1.8 assegurar que contenção, erradicação, recuperação e validação sejam acompanhadas através do REG10;

3.1.9 assegurar que ciberameaças significativas e incidentes graves do setor financeiro sejam encaminhados para os fluxos de decisão e reporte adequados;

3.1.10 assegurar que as lições aprendidas com incidentes resultem em ação corretiva, formação, melhoria de controlos e revisão pela gestão;

3.1.11 assegurar que os registos de incidentes e violações estejam disponíveis para auditoria, revisão pela gestão, garantia ao cliente e revisão regulatória quando aplicável;

3.1.12 assegurar que a PII15-FS substitui a PII15 para o mesmo âmbito do setor financeiro e não duplica o trabalho de evidência da PII15.

## 4. Declarações da política

### 4.1 Ativação da variante, preparação e receção

4.1.1 [Conditional] The Privacy Lead / PIMS Manager MUST documentar a ativação da PII15-FS no REG01 e no REG03 antes de esta política ser utilizada para um âmbito de PIMS do setor financeiro.

4.1.2 [Conditional] The Privacy Lead / PIMS Manager MUST documentar no REG03 e no REG12 que a PII15 não está implementada em simultâneo para o mesmo âmbito de PIMS do setor financeiro antes da aprovação da PII15-FS.

4.1.3 [All] The Incident Response Coordinator MUST registar todos os incidentes de dados pessoais do setor financeiro suspeitos, reportados ou detetados, no REG10 no prazo de um dia útil após a receção, ou antes quando possa ser acionado um prazo aplicável de notificação, cliente ou reporte.

4.1.4 [Conditional] The Privacy Lead / PIMS Manager MUST manter critérios de tratamento de incidentes e violações de PII do setor financeiro no REG10, pelo menos anualmente e após qualquer alteração material ao âmbito do PIMS, contexto legal, obrigações de clientes, obrigações contratuais, contexto de reporte setorial ou tratamento de alto risco.

4.1.5 [Both] The Information Security Lead MUST confirmar os requisitos de preservação de evidência de incidentes no REG10 no prazo de 24 horas após um incidente suspeito afetar um sistema, serviço ou aplicação que trate PII.

4.1.6 [Conditional] The Vendor / Procurement Owner MUST manter no REG08 os requisitos de contactos de incidentes de terceiros do setor financeiro e de encaminhamento de evidência antes da integração e, pelo menos anualmente, para subcontratantes, subcontratantes subsequentes, fornecedores e prestadores externalizados de reporte abrangidos pelo âmbito.

**4.2 Classificação e avaliação da violação**

4.2.1 [All] The Incident Response Coordinator MUST classificar cada entrada do REG10 no prazo de 24 horas após a receção como evento não relacionado com PII, incidente de PII suspeito, incidente de PII confirmado, violação de PII confirmada, incidente de dados pessoais do setor financeiro, incidente grave do setor financeiro, ciberameaça significativa ou entrada pendente de classificação.

4.2.2 [Conditional] The Information Security Lead MUST avaliar serviços, clientes, contrapartes, transações, tempo de indisponibilidade do serviço, dispersão geográfica, perda de dados, criticidade do serviço e impacto económico afetados no REG10 quando um incidente de PII possa afetar serviços ou operações do setor financeiro.

4.2.3 [Both] The Privacy Lead / PIMS Manager MUST identificar a atividade de tratamento afetada, categorias de PII, categorias de titulares dos dados, sistemas, subcontratantes, subcontratantes subsequentes, locais de transferência e riscos de privacidade no REG02, REG04, REG08, REG09 e REG10 antes de a decisão de notificação de violação ser finalizada.

4.2.4 [Controller] The Data Protection Officer / Privacy Advisor MUST avaliar o risco para os titulares dos dados afetados para cada violação de PII confirmada ou razoavelmente suspeita e registar a recomendação de notificação, a fundamentação do risco e o aconselhamento no REG10 antes de ser tomada a decisão de notificação externa.

4.2.5 [Joint Controller] The Privacy Lead / PIMS Manager MUST registar a repartição de responsabilidades por incidente entre responsáveis conjuntos pelo tratamento no REG08 e no REG10 no prazo de 24 horas após identificar responsabilidade partilhada por uma violação de PII suspeita ou confirmada.

4.2.6 [Processor] The Privacy Lead / PIMS Manager MUST avaliar instruções do cliente, obrigações contratuais de notificação e obrigações de cooperação no REG08 e no REG10 no prazo de 24 horas após uma violação de PII suspeita ou confirmada afetar tratamento realizado na qualidade de subcontratante.

4.2.7 [Subprocessor] The Vendor / Procurement Owner MUST identificar a cadeia de notificação a montante e o encaminhamento de evidência exigido no REG08 e no REG10 no prazo de 24 horas após um incidente de PII suspeito ou confirmado afetar tratamento realizado na qualidade de subcontratante subsequente.

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

**9. Exceções**

9.1.1 [All] The Privacy Lead / PIMS Manager MUST registar qualquer exceção a esta política no REG12 antes da implementação, ou no prazo de 24 horas após ação de emergência quando a aprovação prévia não tenha sido viável.

9.1.2 [Conditional] Top Management MUST aprovar qualquer exceção que afete materialmente o prazo de notificação de violações, o prazo de reporte do setor financeiro, a comunicação pública, o compromisso com clientes, a preservação de evidência ou o risco para titulares dos dados antes de o incidente ser encerrado, com evidência de aprovação retida no REG10 e no REG12.

9.1.3 [Conditional] The Data Protection Officer / Privacy Advisor MUST documentar aconselhamento para qualquer notificação atrasada, decisão de não notificar, exceção de reporte ou abordagem excecional de comunicação antes do encerramento do incidente, com aconselhamento retido no REG10.

9.1.4 [Both] The Vendor / Procurement Owner MUST registar exceções de fornecedores, subcontratantes, subcontratantes subsequentes, clientes ou prestadores externalizados que afetem a resposta a incidentes do setor financeiro no REG08 e no REG12 no prazo de cinco dias úteis após identificar a exceção.

9.1.5 [All] The Privacy Lead / PIMS Manager MUST rever exceções abertas a esta política, pelo menos mensalmente até ao encerramento, com o estado da revisão retido no REG12.

**10. Aplicação**

10.1.1 [All] The Process Owner / Business Owner MUST escalar a falha em reportar um incidente de dados pessoais do setor financeiro suspeito, preservar evidência, seguir ações atribuídas ou cooperar com a avaliação da violação para o Privacy Lead / PIMS Manager no prazo de dois dias úteis após a descoberta, com evidência retida no REG12.

10.1.2 [Both] The Incident Response Coordinator MUST escalar reporte tardio, classificação em falta, evidência em falta, escalonamento em falta ou ação de contenção em atraso para o Privacy Lead / PIMS Manager no prazo de um dia útil após identificar o problema, com evidência retida no REG10 e no REG12.

10.1.3 [Both] The Privacy Lead / PIMS Manager MUST registar uma não conformidade no REG12 quando uma violação desta política afetar a receção de incidentes, triagem, contenção, notificação, reporte, integridade da evidência, comunicação ou ação corretiva.

10.1.4 [Both] The Vendor / Procurement Owner MUST iniciar a remediação de fornecedor, subcontratante, subcontratante subsequente ou prestador externalizado através do REG08 e do REG12 no prazo de cinco dias úteis quando um terceiro não cumprir as obrigações acordadas relativas a incidentes, violações, evidência ou reporte.

10.1.5 [Conditional] Top Management MUST rever não conformidades materiais ou recorrentes da PII15-FS na próxima revisão pela gestão programada, com decisões e ações exigidas retidas no REG12.

10.1.6 [All] The Privacy Lead / PIMS Manager MUST acionar formação corretiva no REG11 no prazo de 30 dias de calendário quando uma não conformidade da política envolver

sensibilização da função, reporte tardio, falha de escalonamento, falha de tratamento de evidência ou falha de comunicação.

## 11. Revisão e manutenção

11.1.1 [Conditional] The Privacy Lead / PIMS Manager MUST rever esta política pelo menos anualmente e registar o resultado da revisão, as alterações exigidas e o estado de aprovação no REG12.

11.1.2 [Conditional] The Incident Response Coordinator MUST acionar uma revisão pós-incidente desta política no prazo de 30 dias de calendário após o encerramento de qualquer incidente de alto impacto relativo a dados pessoais no setor financeiro, violação de PII confirmada, incidente grave do setor financeiro ou ciberameaça significativa, com evidência da revisão retida no REG10 e no REG12.

11.1.3 [Conditional] The Privacy Lead / PIMS Manager MUST rever esta política no prazo de 30 dias de calendário após tomar conhecimento de uma alteração material a requisitos legais, setoriais, de clientes, contratuais, de subcontratantes, de subcontratantes subsequentes, de modelos de reporte, de prazos de reporte ou de requisitos de reporte de incidentes relacionados com transferências, com evidência da revisão retida no REG01, REG08, REG09 e REG12.

11.1.4 [Both] The Internal Audit / Compliance Reviewer MUST rever a implementação desta política, pelo menos anualmente, através do programa de auditoria interna do PIMS, com constatações de auditoria e ações corretivas retidas no REG12.

11.1.5 [Conditional] Top Management MUST rever tendências de incidentes, violações significativas, desempenho de reporte, ações corretivas em atraso e eficácia da política durante a revisão pela gestão programada, com resultados retidos no REG12.

11.1.6 [Conditional] The Privacy Lead / PIMS Manager MUST rever a relação de substituição entre a PII15-FS e a PII15 pelo menos anualmente e após qualquer alteração de âmbito do PIMS para verificar que ambas as políticas não estão implementadas para o mesmo âmbito do setor financeiro, com evidência de revisão retida no REG03 e no REG12.

## 12. Políticas relacionadas

### 12.1 Esta política deve ser lida em conjunto com:

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

12.1.2 PII02 - Política de Papéis, Responsabilidades e Responsabilização em Privacidade

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

12.1.4 PII04 - Política de Aviso de Privacidade e Transparência

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

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

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

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

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

12.1.10 PII13 - Política de Transferência Internacional de PII

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

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

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

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

12.1.15 PII23 - Política de Subcontratante de PII na Nuvem, quando as obrigações de subcontratante de nuvem do setor financeiro estejam no âmbito

12.2 A PII15 - Política de Gestão de Incidentes e Violações de PII é a política de referência para incidentes e violações. A PII15-FS é uma variante de substituição, para o setor financeiro, da PII15. A PII15 e a PII15-FS não devem ser implementadas em simultâneo para o mesmo âmbito de PIMS, unidade de negócio, produto, ambiente de cliente, serviço regulado ou perímetro de evidência.

## 13. Normas e referenciais de referência

13.1 ISO/IEC 27701:2025 - Clause 7.4; Clause 7.5. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.8; 4.5.1; 4.5.4; 4.5.5; 5.2.2; 7.1.1; 11.1.3].

13.2 ISO/IEC 27701:2025 - Clause 8.1; Clause 8.2; Clause 8.3. Addressed by clauses [4.1.3; 4.2.3; 4.3.1; 4.3.4; 4.3.5; 4.7.3; 6.1.4; 7.1.4].

13.3 ISO/IEC 27701:2025 - Clause 9.1; Clause 10.2. Addressed by clauses [4.7.1; 4.7.2; 4.7.6; 6.1.3; 8.1.1; 8.1.2; 8.1.3; 8.1.4; 8.1.5; 8.1.6; 9.1.1; 10.1.1; 11.1.4; 11.1.5].

13.4 ISO/IEC 27701:2025 - Annex A.3.11. Addressed by clauses [4.1.1; 4.1.2; 4.1.4; 4.1.6; 5.1.1; 6.1.1; 7.1.2; 7.1.6; 7.1.7].

13.5 ISO/IEC 27701:2025 - Annex A.3.12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.3; 4.3.4; 4.6.1; 4.6.2].

13.6 ISO/IEC 27701:2025 - Annex A.3.13; Annex A.3.14. Addressed by clauses [4.4.1; 4.4.2; 4.4.3; 4.4.4; 4.4.5; 4.4.6; 4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.1; 4.5.2; 4.5.3; 4.5.4; 4.5.5; 4.5.6; 4.5.7; 9.1.2; 11.1.3].

13.7 ISO/IEC 27701:2025 - Annex A.2.2.2; Annex A.2.2.6. Addressed by clauses [4.2.6; 4.2.7; 4.3.6; 4.4.4; 4.4.5; 4.4.10; 4.5.6; 5.7.1; 7.1.3; 8.1.5; 10.1.4].

13.8 GDPR - Article 5(2); Article 24. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.5.1; 4.7.2; 5.2.1; 6.1.1; 8.1.2; 11.1.6].

13.9 GDPR - Article 26. Addressed by clauses [4.2.5; 4.4.6; 4.5.1].

13.10 GDPR - Article 28. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3; 10.1.4].

13.11 GDPR - Article 32. Addressed by clauses [4.1.5; 4.3.1; 4.3.2; 4.3.4; 4.5.2; 4.7.3; 7.1.4].

13.12 GDPR - Article 33. Addressed by clauses [4.2.3; 4.2.4; 4.4.1; 4.4.2; 4.5.4; 8.1.2].

13.13 GDPR - Article 34. Addressed by clauses [4.4.3; 4.5.4].

13.14 GDPR - Article 39. Addressed by clauses [4.2.4; 4.4.3; 5.3.1; 6.1.4; 9.1.3].

13.15 DORA Regulation (EU) 2022/2554 - Article 17. Addressed by clauses [4.1.3; 4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.3; 4.3.4; 4.3.6; 4.4.7; 4.5.1; 4.7.1; 5.4.1; 6.1.2; 7.1.7].

13.16 DORA Regulation (EU) 2022/2554 - Article 18. Addressed by clauses [4.2.1; 4.2.2; 4.6.1; 4.6.2; 4.6.3; 8.1.3].

13.17 DORA Regulation (EU) 2022/2554 - Article 19. Addressed by clauses [4.4.7; 4.4.8; 4.4.9; 4.4.10; 4.5.5; 8.1.3].

13.18 DORA Regulation (EU) 2022/2554 - Article 20. Addressed by clauses [4.4.8; 4.5.5; 6.1.4; 7.1.2; 8.1.3; 11.1.3].

13.19 NIS2 Directive (EU) 2022/2555 - Article 23. Addressed by clauses [4.4.7; 4.4.8; 4.5.5; 6.1.4; 8.1.3; 11.1.3].

13.20 ISO/IEC 29100:2020 - Clause 5.11; Clause 5.12. Addressed by clauses [4.1.2; 4.2.3; 4.4.1; 4.4.3; 4.5.1; 4.5.3; 4.7.2; 5.2.1; 8.1.2].

13.21 ISO/IEC 29151:2022 - Clause 16.1.2; Clause 16.1.3. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.5.2; 4.7.1].

13.22 ISO/IEC 27002:2022 - Control 5.24; Control 5.25; Control 5.26; Control 5.27; Control 5.28. Addressed by clauses [4.1.4; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.3.4; 4.3.6; 4.5.2; 4.7.1; 4.7.2; 7.1.7; 10.1.2].

13.23 ISO/IEC 27035-1:2023 - Clause 5.2; Clause 5.3; Clause 5.4; Clause 5.5; Clause 5.6. Addressed by clauses [4.1.4; 4.2.1; 4.3.1; 4.4.1; 4.5.1; 4.7.1; 7.1.7].

13.24 ISO/IEC 27035-2:2023 - Clause 4; Clause 6; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.4; 4.1.6; 4.7.1; 4.7.5; 7.1.6; 7.1.7; 10.1.6].

13.25 ISO/IEC 27035-3:2020 - Clause 7; Clause 8; Clause 9; Clause 10; Clause 11; Clause 12. Addressed by clauses [4.1.3; 4.1.5; 4.2.1; 4.3.1; 4.3.2; 4.4.7; 4.5.1; 4.7.1].

13.26 ISO/IEC 27018:2020 - Annex A.10.1. Addressed by clauses [4.2.6; 4.2.7; 4.4.4; 4.4.5; 4.5.6; 7.1.3].