					Insira aqui a designação da entidade jurídica registada							
Número do documento: P28					Título do documento: **Política de Desenvolvimento Externalizado**							
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**

Alinhamento com normas e regulamentos aplicáveis

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8.1	N/A
ISO/IEC 27002:2022	Controlos 5.19-5.22, 8	N/A
NIST SP 800-53 Rev. 5	SA-4, SA-9, SA-10	N/A
RGPD da UE	Artigos 28, 32	N/A
Diretiva NIS2 da UE	Artigos 21(2)(a), (h), 23	N/A
DORA da UE	Artigos 28(1), (2)	N/A
COBIT 2019	APO10, BAI03, DSS	N/A

1. Finalidade

1.1 Esta política define os controlos obrigatórios para a externalização do desenvolvimento de software ou sistemas a fornecedores externos, prestadores de serviços ou agências, assegurando que práticas seguras são incorporadas em todo o ciclo de vida de desenvolvimento.

1.2 Visa prevenir vulnerabilidades de segurança, perda de dados, exposição de propriedade intelectual (PI) e violações de conformidade decorrentes da contratação de desenvolvimento externo.

1.3 A política estabelece requisitos de governação de fornecedores, desenvolvimento seguro, gestão de acessos, obrigações de monitorização e processo de descontinuação no termo do contrato, de modo a salvaguardar a Confidencialidade, Integridade e Disponibilidade do software desenvolvido.

2. Âmbito

2.1 Esta política aplica-se a todas as unidades da organização que recorram a entidades externas para o desenvolvimento de software ou sistemas, incluindo:

2.1.1 Aplicações web, aplicações móveis, sistemas embebidos, APIs, scripts, fluxos de automatização ou módulos de plataforma

2.1.2 Desenvolvimento à medida para plataformas internas, sistemas orientados para o cliente ou produtos comerciais

2.1.3 Contratação de programadores terceiros, freelancers, agências ou equipas offshore

2.2 A política rege igualmente qualquer entidade externa que aceda a código-fonte, ambientes de teste ou pipelines de CI/CD durante o desenvolvimento.

2.3 Os requisitos aplicam-se independentemente do tipo de contrato, da metodologia de desenvolvimento ou da localização geográfica do prestador externalizado.

3. Objetivos

3.1 Aplicar práticas de ciclo de vida de desenvolvimento seguro (SDLC) em todas as contratações externalizadas, desde o planeamento até à validação pós-implementação.

3.2 Assegurar que todos os contratos com programadores externos incluem cláusulas obrigatórias relativas à proteção de dados, desenvolvimento seguro e retenção da PI.

3.3 Definir requisitos de controlo de acesso, monitorização e auditoria para programadores terceiros que interajam com sistemas internos.

3.4 Proteger a organização contra ameaças da cadeia de fornecimento, violações legais e danos reputacionais relacionados com software desenvolvido externamente.

3.5 Manter a conformidade contínua com referenciais de segurança, incluindo ISO/IEC 27001, NIST, RGPD da UE, Diretiva NIS2 da UE, DORA da UE e COBIT 2019.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova projetos de desenvolvimento externalizado de alto risco e valida exceções à política quando justificadas.

4.1.2 Assegura que as decisões de externalização estão alinhadas com os objetivos estratégicos e com o apetite pelo risco da organização.

4.2 Diretor de Segurança da Informação (CISO)

4.2.1 Aprova a integração de fornecedores na perspetiva da segurança da informação.

4.2.2 Define os requisitos de controlos de segurança para contratações externalizadas e revê relatórios de incidentes.

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

9. Requisitos de revisão e atualização

9.1 Esta política deve ser revista pelo menos uma vez por ano ou com maior frequência nas seguintes circunstâncias:

9.1.1 Introdução de novos modelos de externalização de desenvolvimento, fornecedores ou jurisdições

9.1.2 Atualizações de referenciais regulamentares como o RGPD da UE, a Diretiva NIS2 da UE ou a DORA da UE

9.1.3 Na sequência de um incidente de segurança que envolva código externalizado, acessos ou entregáveis

9.1.4 Como parte de constatações de auditoria interna ou de melhorias do SGSI

9.2 O Diretor de Segurança da Informação (CISO) é responsável por iniciar e coordenar a revisão da política, em consulta com:

9.2.1.1 Jurídico e Compras (para alinhamento da aplicação contratual)

9.2.1.2 Proprietários de Projeto e de Produto (para viabilidade operacional)

9.2.1.3 Segurança da Informação (para atualização de ameaças e controlos)

9.2.1.4 Alta Direção (para aprovação final)

9.3 Todas as atualizações da política devem ser:

9.3.1.1 Sujeitas a controlo de versões e armazenadas num repositório documental designado

9.3.1.2 Comunicadas às partes interessadas envolvidas em atividades de desenvolvimento externalizado

9.3.1.3 Articuladas com quaisquer atualizações em políticas relacionadas ou documentação processual

9.4 Cada versão da política deve ser acompanhada de um registo de alterações para assegurar a rastreabilidade das modificações e aprovações.

10. Políticas relacionadas e articulações

10.1 Esta política suporta e é suportada pelos seguintes documentos relacionados:

10.1.1 P1 - Política de Segurança da Informação: Estabelece princípios de segurança ao nível da organização aplicáveis em contextos de desenvolvimento interno e por terceiros.

10.1.2 P5 - Política de Gestão de Alterações: Assegura que todas as alterações relacionadas com implementações provenientes de bases de código externalizadas são revistas e aprovadas antes da implementação.

10.1.3 P13 - Política de Classificação e Rotulagem da Informação: Determina como os dados sensíveis são identificados antes de serem expostos a fornecedores de desenvolvimento ou repositórios.

10.1.4 P18 - Política de Controlos Criptográficos: Orienta a forma como chaves, segredos e credenciais sensíveis devem ser tratados durante o desenvolvimento e a entrega.

10.1.5 P24 - Política de Desenvolvimento Seguro: Define requisitos de base para práticas de desenvolvimento de software internas e externas.

10.1.6 P30 - Política de Resposta a Incidentes: Rege a forma como violações ou problemas de segurança envolvendo desenvolvimento externalizado são escalados, investigados e resolvidos.

10.1.7 P33 - Política de Monitorização de Auditoria e Conformidade: Estabelece requisitos para a revisão de atividades de desenvolvimento externalizado durante auditorias ou revisões de conformidade.

11. Normas e referenciais aplicáveis

11.1 Esta política está alinhada com referenciais e regulamentos de segurança internacionalmente reconhecidos, de modo a assegurar a externalização segura do desenvolvimento de software e práticas adequadas de gestão de fornecedores.

11.2 ISO/IEC 27001

11.2.1 Cláusula 8.1 - Planeamento e controlo operacionais: Estabelece controlos de processo para desenvolvimento seguro e entrega por terceiros.

11.3 ISO/IEC 27002:2022 - Controlos 5.19 a 5.21, 8.

11.3.1 Controlo do Anexo A 5.19 - Gestão da relação com fornecedores: Exige acordos formais com cláusulas de segurança e conformidade.

11.3.2 Controlo do Anexo A 5.20 - Tratamento da segurança da informação em acordos com fornecedores: Assegura que controlos específicos de desenvolvimento são incorporados nos contratos.

11.3.3 Controlo do Anexo A 5.21 - Gestão da prestação de serviços do fornecedor: Envolve a monitorização dos entregáveis e dos riscos do desenvolvimento por terceiros.

11.3.4 Controlo do Anexo A 8.27 - Desenvolvimento externalizado: Determina requisitos de segurança definidos e controlo de acesso sobre software desenvolvido externamente.

11.3.5 Estes controlos definem requisitos estruturados para selecionar, contratar e supervisionar programadores externalizados, incluindo práticas de desenvolvimento seguro, tratamento de código e validação de desempenho.

11.4 NIST SP 800-53 Rev. 5

11.4.1 SA-4 - Processo de aquisição: Exige que os requisitos de desenvolvimento seguro sejam definidos no momento da aquisição.

11.4.2 SA-9 - Serviços de sistemas externos: Rege a forma como programadores terceiros interagem de forma segura com serviços internos.

11.4.3 SA-10 - Gestão da configuração do programador: Alinha-se com obrigações de controlo de versões, acesso ao código e acompanhamento de alterações para equipas externas.

11.5 RGPD da UE (2016/679)

11.5.1 Artigo 28 - Obrigações do subcontratante: Exige que os contratos com programadores terceiros especifiquem requisitos de segurança, controlo e auditoria para o tratamento de dados pessoais.

11.5.2 Artigo 32 - Segurança do tratamento: Exige salvaguardas adequadas (por exemplo, cifragem, controlo de acesso) no desenvolvimento de sistemas que tratem dados pessoais.

11.6 Diretiva NIS2 da UE (2022/2555)

11.6.1 Artigos 21(2)(a), (h), 23: Determinam a aplicação de práticas de desenvolvimento seguro em contratações com terceiros e cadeias de fornecimento digitais, com supervisão e verificação técnica.

11.7 DORA da UE (2022/2554)

11.7.1 Artigos 28(1), (2): Exigem que as entidades financeiras gerem o risco de terceiros nas TIC através de controlos contratuais e supervisão do desenvolvimento seguro, em especial no desenvolvimento externalizado crítico.

11.8 COBIT 2019

11.8.1 APO10 - Gerir Fornecedores: Estabelece requisitos estruturados para avaliação de fornecedores, contratos e monitorização do desempenho.

11.8.2 BAI03 - Gerir Construção de Soluções: Corresponde diretamente a processos de SDLC seguro, revisões de código e validação do desenvolvimento.

11.8.3 DSS05 - Gerir Serviços de Segurança: Alinha-se com a monitorização e proteção de sistemas desenvolvidos externamente ou por terceiros.