					Insira aqui a designação da entidade jurídica registada							
Número do documento: P28S					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

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 5.1, 6.1, 8	Controlos aplicáveis do SGSI e controlos relacionados com fornecedores
ISO/IEC 27002:2022	Controlos 5.19, 5.20, 8.25–8.27	Controlos relativos a fornecedores e ao ciclo de vida de desenvolvimento seguro
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Requisitos de aquisição, cadeia de fornecimento, desenvolvimento seguro e acordos com fornecedores
RGPD da UE	Artigo 28	Requisitos contratuais e de proteção de dados para o tratamento por terceiros
Diretiva NIS2 da UE	Artigo 21(2)(a), (h)	Controlos de segurança da cadeia de fornecimento e de desenvolvimento seguro de aplicações
DORA da UE	Artigo 10	Gestão do risco de terceiros em TIC, incluindo desenvolvimento externalizado
COBIT 2019	BAI03, DSS05	Requisitos aplicáveis ao desenvolvimento externo e a prestadores externos de serviços de TI

1. Finalidade

1.1 Esta política assegura que todo o desenvolvimento de software externalizado — quer seja realizado por freelancers, agências ou fornecedores terceiros — é conduzido de forma segura, sujeito a controlo contratual e alinhado com os requisitos legais, regulamentares e de auditoria aplicáveis.

1.2 Esta política protege a organização contra riscos relacionados com código inseguro, titularidade pouco clara, exposição de dados e gestão inadequada de fornecedores, impondo normas vinculativas de desenvolvimento e supervisão de fornecedores, mesmo na ausência de um departamento de TI dedicado.

1.3 Esta política apoia a certificação ISO/IEC 27001:2022, através da definição clara de expectativas de desenvolvimento, responsabilização e controlos documentados sobre atividades de desenvolvimento realizadas por terceiros.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os programadores externos, incluindo freelancers e agências de desenvolvimento

2.1.2 Qualquer trabalho de desenvolvimento que envolva ferramentas internas, sítios Web públicos, aplicações informáticas ou automatização empresarial

2.1.3 Colaboradores responsáveis por selecionar, gerir ou supervisionar programadores externos

2.1.4 Qualquer integração de sistemas de terceiros, scripting ou desenvolvimento que interaja com dados ou sistemas da empresa

2.2 Inclui igualmente qualquer entidade ou plataforma com acesso a credenciais da empresa, repositórios de dados, repositórios de código-fonte, ambientes de pré-produção ou sistemas de produção.

3. Objetivos

3.1 Assegurar que todo o desenvolvimento externalizado cumpre os princípios de programação segura e que os programadores ficam contratualmente obrigados a seguir normas documentadas e cláusulas de confidencialidade.

3.2 Estabelecer a titularidade de todos os entregáveis — código, ativos, credenciais e documentação — assegurando a transferência integral de direitos para a empresa e uma transferência de conhecimento rastreável no encerramento do projeto.

3.3 Prevenir riscos comuns de desenvolvimento, incluindo reutilização de código proprietário, ataques à cadeia de fornecimento através de bibliotecas, utilização de frameworks não suportadas e acessos administrativos não validados.

3.4 Exigir documentação prévia à contratação para cada projeto externalizado, incluindo contratos, acordos de confidencialidade (NDA) e requisitos mínimos de segurança.

3.5 Proteger dados de clientes, sistemas e processos internos, assegurando supervisão adequada do desenvolvimento, testes após a entrega e gestão segura de acessos aos sistemas.

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Aprova todas as relações com fornecedores e assina os acordos de desenvolvimento.

4.1.2 Assegura que todo o desenvolvimento externalizado cumpre esta política.

4.1.3 Remove os acessos aos sistemas da empresa após a conclusão do projeto.

4.1.4 Revê a documentação e os resultados após a entrega.

4.2 Responsável de Projeto (tipicamente colaborador interno ou coordenador designado)

4.2.1 Gere a coordenação diária com o programador externo.

4.2.2 Verifica que os requisitos funcionais são cumpridos e que os entregáveis são testados.

4.2.3 Assegura a entrega segura do código e das credenciais.

4.2.4 Comunica ao GM quaisquer problemas ou incidentes relacionados com o desenvolvimento.

[... 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 Revisão anual

9.1.1 Esta política deve ser revista pelo Diretor-Geral (GM) pelo menos uma vez por ano. A revisão assegura que continua a cumprir:

9.1.1.1 Os requisitos de certificação ISO/IEC 27001

9.1.1.2 As alterações das obrigações legais (por exemplo, Artigo 28 do RGPD da UE, Artigo 10 do DORA da UE)

9.1.1.3 As práticas atuais de desenvolvimento no contexto das PME e os riscos de terceiros

9.2 Revisões intercalares

9.2.1 As revisões da política devem também ocorrer quando:

9.2.1.1 É integrado um novo fornecedor ou plataforma de desenvolvimento externalizado

9.2.1.2 Ocorre um incidente significativo relacionado com desenvolvimento externalizado

9.2.1.3 Existem alterações materiais nas ferramentas, plataformas ou ambientes utilizados

9.3 Processo de revisão

9.3.1 O GM é responsável por:

9.3.1.1 Verificar que os contratos, acordos de confidencialidade (NDA) e processos de controlo de acesso permanecem eficazes

9.3.1.2 Confirmar que os fornecedores e freelancers atuais estão alinhados com a política

9.3.1.3 Rever os termos com base no feedback de projetos ou incidentes anteriores

9.4 Controlo de versões e comunicação

9.4.1 Todas as alterações devem ser:

9.4.1.1 Registadas com a data, o motivo e a descrição da alteração

9.4.1.2 Aprovadas pelo GM e adicionadas ao histórico de versões

9.4.1.3 Comunicadas a todos os colaboradores ou responsáveis de projeto que trabalhem com programadores externos

9.4.1.4 Redistribuídas a todos os fornecedores e terceiros afetados, quando necessário

10. Políticas relacionadas e ligações

10.1 Esta política apoia diretamente e depende da implementação das seguintes políticas alinhadas com PME:

10.1.1 P2S – Política de Papéis e Responsabilidades de Governação: Clarifica quem é responsável pela aprovação de fornecedores, controlo de acesso e aceitação do risco na utilização de programadores externos.

10.1.2 P4S – Política de Controlo de Acesso: Define a criação, restrição e cessação adequadas de contas de utilizador e acesso administrativo utilizados durante o desenvolvimento externalizado.

10.1.3 P8S – Política de Sensibilização e Formação em Segurança da Informação: Assegura que os colaboradores internos compreendem como coordenar de forma segura com programadores externos, incluindo o tratamento de credenciais e ficheiros de projeto.

10.1.4 P17S – Política de Proteção de Dados e Privacidade: Estabelece requisitos de segurança e legais para o tratamento de dados pessoais que possam ser tratados por programadores externos ao abrigo do RGPD da UE.

10.1.5 P24S – Política de Desenvolvimento Seguro: Especifica como o desenvolvimento interno e externo deve seguir práticas de programação segura e validação de bibliotecas e frameworks.

10.1.6 P30S – Política de Resposta a Incidentes: Necessária quando o desenvolvimento externalizado conduz a incidentes de segurança ou vulnerabilidades, orientando a investigação e remediação coordenadas.

10.2 Estas políticas devem ser implementadas em paralelo para assegurar que o desenvolvimento externalizado não cria risco não gerido nem viola obrigações de cumprimento aplicáveis às PME.

11. Normas e referenciais aplicáveis

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1 – As organizações devem avaliar e tratar os riscos de segurança da informação associados a fornecedores.

11.1.2 Cláusula 8.1 – Exige planeamento e controlo operacionais, incluindo serviços de terceiros, como o desenvolvimento externalizado.

11.2 ISO/IEC 27002

11.2.1 Controlo 5.19 – Recomenda a avaliação da capacidade dos fornecedores para cumprir os requisitos de segurança da informação.

11.2.2 Controlo 5.20 – Incentiva a monitorização regular e a revisão periódica dos serviços de terceiros.

11.2.3 Controlos 8.25–8.27 – Definem práticas de ciclo de vida de desenvolvimento seguro aplicáveis ao desenvolvimento externalizado.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – Exige que as estratégias de aquisição incluam medidas de segurança da informação.

11.3.2 SA-9 – Trata o desenvolvimento de sistemas externos e os riscos da cadeia de fornecimento.

11.3.3 SA-11 – Define práticas de desenvolvimento seguro, incluindo revisões de código e remediação de falhas.

11.3.4 SA-15 – Incentiva a utilização de ferramentas automatizadas para deteção de falhas e garantia de software.

11.3.5 SR-3 – Exige que os acordos com fornecedores incluam requisitos de cibersegurança.

11.4 Regulamento Geral sobre a Proteção de Dados da UE (RGPD)

11.4.1 Artigo 28 – Exige contratos com subcontratantes responsáveis pelo tratamento de dados por terceiros para assegurar salvaguardas adequadas de proteção de dados, aplicáveis diretamente a programadores que tratem ou acedam a dados pessoais.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(a), (h) – Exige controlos de segurança da cadeia de fornecimento e práticas de desenvolvimento seguro de software para prestadores de serviços digitais abrangidos, incluindo PME, quando aplicável.

11.6 DORA da UE

11.6.1 Artigo 10 – Exige gestão do risco de terceiros em TIC, incluindo acordos de desenvolvimento, obrigações de segurança e controlos de risco relacionados com fornecedores terceiros.

11.7 COBIT 2019

11.7.1 BAI03 – Gerir a Identificação e Construção de Soluções – Assegura que o desenvolvimento externo cumpre os requisitos do negócio e as expectativas de segurança.

11.7.2 DSS05 – Gerir Serviços de Segurança – Exige que serviços de segurança externos e fornecedores de desenvolvimento operem ao abrigo de regras de segurança aplicadas e supervisão.