					Insira aqui a designação da entidade jurídica registada							
Número do documento: P24					Título do documento: **Política de Desenvolvimento Seguro**							
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**

1. Finalidade

1.1 A presente política define os requisitos de segurança obrigatórios aplicáveis às atividades de desenvolvimento de software e sistemas na organização, incluindo projetos internos, desenvolvimento externalizado e integração de código de terceiros.

1.2 O objetivo é assegurar que a segurança seja incorporada ao longo de todo o ciclo de vida de desenvolvimento de software (SDLC) e que as vulnerabilidades sejam identificadas, mitigadas e prevenidas antes da entrada em produção.

1.3 Esta política apoia a aplicação da Cláusula 8.1 da ISO/IEC 27001:2022 e dos Controlos 8.25–8.27 do Anexo A, através da normalização da governação do desenvolvimento seguro, das práticas de validação de código e da supervisão do desenvolvimento por terceiros.

2. Âmbito

2.1 Esta política aplica-se a todos os seguintes elementos:

2.1.1 Software, aplicações, scripts, integrações e ferramentas de automatização desenvolvidos interna ou externamente

2.1.2 Equipas de desenvolvimento, proprietários de produto, equipas de DevOps, QA, arquitetos, gestores de projeto e contratados

2.1.3 Ambientes do SDLC, incluindo sistemas de desenvolvimento, teste, homologação e pré-produção

2.1.4 Componentes open source e de terceiros integrados em aplicações internas

2.1.5 Software implementado em infraestrutura on-premises, em ambientes de cloud privada, híbrida ou cloud pública

2.2 Todos os utilizadores e entidades que participem no desenvolvimento, teste ou implementação de sistemas no contexto organizacional estão sujeitos a esta política, incluindo prestadores de serviços geridos e fornecedores de plataformas.

3. Objetivos

3.1 Incorporar controlos de segurança em todas as fases do desenvolvimento de software, desde a conceção até à implementação, assegurando uma redução do risco proativa e contínua.

3.2 Prevenir a introdução de vulnerabilidades exploráveis, tais como falhas de injeção, autenticação insegura e exposição a fraquezas conhecidas em componentes de terceiros.

3.3 Estabelecer e aplicar práticas de programação segura alinhadas com a OWASP, a SANS CWE e orientações específicas dos frameworks utilizados.

3.4 Assegurar que todo o código seja sujeito a revisão por pares, análise automatizada e validação de segurança antes da implementação.

3.5 Gerir os riscos de desenvolvimento decorrentes de atividades externalizadas, da inclusão de código de terceiros e da reutilização de software open source.

3.6 Proteger os ambientes de desenvolvimento, teste e homologação contra acessos não autorizados e impedir a utilização de dados de produção sem mascaramento ou anonimização aprovados.

3.7 Promover a sensibilização para a segurança entre programadores, proprietários de produto e profissionais de garantia da qualidade, através de formação baseada em funções e de atualizações contínuas sobre ameaças emergentes.

4. Papéis e responsabilidades

4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É responsável por esta política e assegura que os requisitos de desenvolvimento seguro sejam aplicados em toda a organização.

4.1.2 Aprova as normas de programação segura e os acordos de desenvolvimento com terceiros.

4.1.3 Valida as decisões de tratamento do risco relativas a vulnerabilidades não resolvidas ou adiadas.

4.2 Responsável pela Segurança das Aplicações / Gestor de DevSecOps

4.2.1 Desenvolve, mantém e promove orientações de programação segura.

4.2.2 Integra testes de segurança estáticos e dinâmicos nos pipelines de CI/CD.

4.2.3 Realiza revisões de segurança ao código e define ações de remediação obrigatórias.

[... 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 anualmente, ou com maior frequência em resposta a:

9.1.1 Revisões significativas das metodologias de desenvolvimento ou do conjunto de ferramentas de DevOps

9.1.2 Incidentes de segurança materiais decorrentes de vulnerabilidades de aplicações

9.1.3 Alterações nos requisitos regulamentares relacionados com software seguro (por exemplo, RGPD da UE, DORA da UE)

9.1.4 Novas normas da indústria ou informações sobre ameaças (por exemplo, OWASP Top 10, SLSA, MITRE CWE)

9.2 A revisão da política deve ser conduzida pelo Responsável pela Segurança das Aplicações, em coordenação com o CISO, arquitetos de software, liderança de QA e assessoria jurídica (quanto às implicações de código de terceiros).

9.3 Quaisquer revisões devem ser registadas no Registo de Documentos do SGSI, sujeitas a controlo de versões e comunicadas às equipas afetadas através de notas de versão ou formação obrigatória.

9.4 As versões anteriores devem ser mantidas no repositório de arquivo para fins de rastreabilidade jurídica e de auditoria.

10. Políticas relacionadas e ligações

10.1 P1 – Política de Segurança da Informação. Estabelece o mandato estratégico para incorporar a segurança em todos os sistemas de informação, sendo o desenvolvimento seguro um controlo operacional fundamental.

10.2 P4 – Política de Controlo de Acesso. Define as medidas de controlo para restringir o acesso a ambientes de desenvolvimento, repositórios, ferramentas de build e pipelines de CI/CD.

10.3 P5 – Política de Gestão de Alterações. Assegura que as alterações de código, lançamentos e implementações estejam sujeitas a aprovação adequada, planeamento de reversão e verificação pós-implementação.

10.4 P12 – Política de Gestão de Ativos. Suporta o inventário dos ambientes de desenvolvimento, repositórios de código-fonte e sistemas de build enquanto ativos geridos sujeitos a classificação e proteção.

10.5 P22 – Política de Registo e Monitorização. Aplica-se aos pipelines de desenvolvimento, assegurando que os processos de build, promoções de código e eventos de implementação sejam registados, monitorizados e analisados quanto a anomalias de segurança.

10.6 P30 – Política de Resposta a Incidentes (P30). Fornece o enquadramento para análise e resposta a falhas de segurança descobertas após a implementação ou durante testes de segurança das aplicações.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 8.1 – Planeamento e controlo operacional: exige a integração de processos e controlos de desenvolvimento seguro nas operações.

11.2 ISO/IEC 27002:2022 – Controlos 8.25–8.27

11.2.1 Controlo 8.25 do Anexo A – Ciclo de vida de desenvolvimento seguro: exige a inclusão formal da segurança na conceção e no desenvolvimento de software.

11.2.2 Controlo 8.26 do Anexo A – Requisitos de segurança das aplicações: exige a definição de práticas de programação segura e de critérios de aceitação de segurança.

11.2.3 Controlo 8.27 do Anexo A – Arquitetura segura de sistemas e princípios de engenharia: exige a aplicação de princípios de conceção de segurança e a mitigação de fraquezas conhecidas.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-3 a SA-15: estabelecem práticas estruturadas de desenvolvimento seguro de aplicações, incluindo requisitos de conceção, integridade do código e testes.

11.3.2 SI-10 – Validação de entradas de informação: aborda defesas de programação segura.

11.3.3 SR-3 – Proteção da cadeia de abastecimento: exige a validação de software, componentes e prestadores terceiros de desenvolvimento.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 25 – Proteção de dados desde a conceção e por defeito: determina a incorporação da segurança e da privacidade no desenvolvimento de sistemas.

11.4.2 Artigo 32 – Segurança do tratamento: sustenta medidas técnicas como validação de entradas, controlos de acesso e implementação segura.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(e–f): exige práticas de desenvolvimento de software que incluam gestão de vulnerabilidades, segurança do código e notificação de incidentes.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 9 – Gestão do risco das TIC: exige práticas de desenvolvimento seguro para entidades financeiras, incluindo controlos de qualidade de software e remediação de defeitos.

11.6.2 Artigo 10 – Continuidade do negócio e testes: incentiva testes e validação rigorosos dos sistemas TIC, incluindo aplicações.

11.7 COBIT 2019

11.7.1 BAI03 – Gerir a identificação e construção de soluções: rege a conceção, o desenvolvimento e a integração da segurança em novas soluções.

11.7.2 BAI07 – Gerir a aceitação e transição da mudança: assegura a implementação segura e a avaliação pós-implementação.

11.7.3 DSS05 – Gerir serviços de segurança: aplica a validação de segurança ao software e à prestação de serviços.