					Insira aqui a designação da entidade jurídica registada							
Número do documento: P24S					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**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	Controlos de segurança relevantes para práticas operacionais, incluindo o desenvolvimento seguro
ISO/IEC 27002:2022	Controlos 8.25–8.27	Abrange o ciclo de vida de desenvolvimento seguro, os testes e as responsabilidades de segurança de programadores terceiros
NIST SP 800-53 Rev.5	SA-3 – SA-15, SI-10	Aborda o SDLC seguro, o controlo de acesso e o tratamento de vulnerabilidades no desenvolvimento
RGPD da UE	Artigo 25	Exige Proteção de Dados desde a Conceção e por Defeito no desenvolvimento de software
Diretiva NIS2 da UE	Artigo 21(2)(a), (e), (h)	Exige políticas de desenvolvimento seguro, supervisão da utilização de componentes open source e documentação das medidas de mitigação
DORA da UE	Artigos 6(7), 9(1)(c), 10(2)(c)	Segurança do ciclo de vida para sistemas críticos de TIC no setor financeiro
COBIT 2019	BAI	Quadro de referência para uma gestão do desenvolvimento seguro estruturada, rastreável e resiliente

1. Finalidade

1.1

Esta política assegura que todo o software, scripts e ferramentas baseadas na web criados ou modificados pela organização ou pelos seus parceiros externos são desenvolvidos de forma segura, minimizando o risco de vulnerabilidades, acesso não autorizado a dados ou perturbações operacionais.

1.2

Define regras obrigatórias de desenvolvimento seguro e práticas de programação segura que todos os programadores internos, contratados e fornecedores devem cumprir, independentemente da dimensão ou complexidade do projeto.

1.3

Esta política foi concebida para proteger dados de clientes, prevenir violações de segurança e assegurar que o software criado ou personalizado pela organização, ou para a organização, possa ser aprovado em

auditorias de segurança, cumprir requisitos legais (por exemplo, RGPD da UE, Diretiva NIS2 da UE, DORA da UE) e apoiar a certificação ISO/IEC 27001.

2. Âmbito

2.1

Esta política aplica-se a todas as pessoas e entidades envolvidas no desenvolvimento, personalização, implementação ou gestão, em nome da organização, dos seguintes elementos:

2.1.1

Websites, aplicações ou ferramentas de automatização

2.1.2

Scripts ou software desenvolvidos internamente

2.1.3

Código criado por programadores terceiros ou freelancers

2.1.4

Plugins, bibliotecas e componentes de software integrados em sistemas de produção

2.2

Abrange todos os ambientes utilizados em atividades de desenvolvimento, incluindo:

2.2.1

Ambientes de desenvolvimento e de teste

2.2.2

Ambientes de staging e de pré-produção

2.2.3

Sistemas de produção utilizados para executar código desenvolvido à medida

2.3

A política rege igualmente o tratamento de dados durante o desenvolvimento e a implementação, em especial qualquer utilização de dados de produção em sistemas de não produção.

3. Objetivos

3.1

Prevenir a introdução de falhas de segurança ou vulnerabilidades em software desenvolvido à medida ou por terceiros.

3.2

Assegurar que as práticas de programação segura e a prevenção de vulnerabilidades são integradas em todas as fases do ciclo de vida de desenvolvimento de software.

3.3

Reduzir os riscos associados à utilização de componentes open source ou de terceiros, impondo a devida validação e o respetivo acompanhamento.

3.4

Exigir revisão formal de código e testes de segurança das aplicações antes da disponibilização.

3.5

Controlar o acesso aos ambientes de desenvolvimento e assegurar a sua separação dos sistemas de produção em utilização.

3.6

Cumprir os requisitos obrigatórios previstos em normas e regulamentos internacionais (por exemplo, ISO/IEC 27001, RGPD da UE, DORA da UE, Diretiva NIS2 da UE).

4. Papéis e responsabilidades

4.1

Diretor-Geral (GM)

4.1.1

Aprova esta política e assume a sua titularidade.

4.1.2

Assegura que todo o desenvolvimento de software, interno ou externalizado, cumpre esta política.

4.1.3

Revê e assina contratos de desenvolvimento ou de prestação de serviços que incluam cláusulas de desenvolvimento seguro.

4.1.4

Verifica o cumprimento por parte dos fornecedores através de pontos de situação regulares ou mediante solicitação de evidências de segurança.

4.2

Programador interno ou responsável pela aplicação

4.2.1

Cumpre práticas de programação segura e de implementação segura.

4.2.2

Aplica a lista de verificação de desenvolvimento seguro a cada projeto.

4.2.3

Valida a segurança de quaisquer componentes open source ou de terceiros utilizados.

4.2.4

Comunica imediatamente ao Diretor-Geral (GM) quaisquer vulnerabilidades detetadas.

4.3

Programador externo ou fornecedor

4.3.1

Deve cumprir as orientações de desenvolvimento seguro da organização e os termos contratuais aplicáveis.

4.3.2

Compromete-se a não reutilizar credenciais, dados ou código da organização para qualquer outro cliente ou projeto.

4.3.3

Realiza, no mínimo, testes básicos de segurança e partilha os resultados com a organização.

4.3.4

Formaliza a aceitação das obrigações de segurança antes da entrega do projeto.

4.4

Prestador de Suporte de TI / Administrador Web

4.4.1

Controla e limita o acesso aos ambientes de desenvolvimento, staging e produção.

4.4.2

Assegura a separação entre sistemas de teste e sistemas de produção em utilização.

4.4.3

Implementa e monitoriza práticas de implementação, incluindo cópias de segurança, registo de alterações e capacidade de reversão.

4.4.4

Coordena-se com programadores internos ou externos para aplicar patches de segurança ou alterações de configuração.

5. Requisitos de governação

5.1

A organização deve estabelecer controlos de desenvolvimento seguro aplicados de forma consistente a todos os projetos de software, independentemente da sua dimensão ou de o desenvolvimento ser interno ou externalizado.

5.2

Todos os acordos de desenvolvimento de software com fornecedores terceiros devem incluir cláusulas de segurança vinculativas que abranjam:

5.2.1

Normas de programação segura, por exemplo, OWASP Top 10 ou equivalente

5.2.2

Confidencialidade do código-fonte e restrições à sua reutilização

5.2.3

Requisitos de testes de vulnerabilidades e respetiva remediação

5.2.4

Procedimentos de entrega e implementação

5.2.5

Direitos de solicitar evidências de programação segura e de testes

5.3

O Diretor-Geral (GM) deve manter registo de:

5.3.1

Todos os projetos ativos de desenvolvimento de software e dos respetivos programadores ou fornecedores responsáveis

5.3.2

Listas de verificação de segurança utilizadas por projeto

5.3.3

Revisões de código realizadas e respetivos revisores

5.3.4

Resultados dos testes antes da implementação

5.3.5

Componentes de terceiros e respetivo estado de licenciamento ou de risco

5.4

Deve existir aprovação formal de segurança antes de qualquer aplicação, script, plugin ou ferramenta de automatização desenvolvida à medida ser colocada em ambiente de produção.

5.5

Os ambientes de desenvolvimento e teste devem obedecer aos seguintes controlos obrigatórios:

5.5.1

Acesso restrito exclusivamente a pessoal autorizado

5.5.2

Proibição da utilização de dados reais de clientes ou dados sensíveis, salvo quando explicitamente anonimizados e aprovados pelo Diretor-Geral (GM)

5.5.3

Separação dos sistemas de produção através de segmentação de rede ou de controlos da plataforma

5.5.4

Registo ativado para acessos administrativos e alterações

5.6

O Diretor-Geral (GM) é responsável por assegurar que estes requisitos de governação são aplicados, monitorizados e revistos pelo menos anualmente, ou após qualquer incidente relevante de desenvolvimento ou alteração de sistema.

6. Requisitos de implementação da política

6.1

Práticas de programação segura

6.1.1

Todos os programadores de software, internos ou externos, devem cumprir práticas básicas de programação segura adequadas à sua linguagem de programação, plataforma e âmbito do projeto. Estas incluem, entre outras:

6.1.1.1

Validação de entradas para todos os dados fornecidos pelos utilizadores

6.1.1.2

Proibição de credenciais ou segredos codificados no código-fonte

6.1.1.3

Utilização de consultas parametrizadas para prevenir ataques de injeção

6.1.1.4

Gestão segura de sessões e autenticação segura

6.1.1.5

Evitar a exposição de mensagens de erro detalhadas em produção

6.1.2

O Diretor-Geral (GM) deve assegurar que os programadores recebem uma lista de verificação de programação segura ou a folha de referência OWASP Top 10 antes do início de qualquer novo projeto.

6.1.3

Qualquer código que não cumpra as normas de programação segura deve ser remediado antes da aprovação e implementação.

6.2

Requisitos de revisão de código

6.2.1

Todo o código desenvolvido deve ser sujeito a revisão por pares ou inspecionado pelo Prestador de Suporte de TI da organização antes da disponibilização.

6.2.2

A revisão deve avaliar:

6.2.2.1

A aderência às normas de programação segura

6.2.2.2

O tratamento correto de dados sensíveis

6.2.2.3

A remoção de elementos de depuração ou de teste das compilações de produção

6.2.2.4

A implementação adequada do tratamento de erros, registo e controlo de sessões

6.3

O revisor deve formalizar a aprovação através de um formulário de aprovação normalizado, digital ou em papel, conservado com a documentação do projeto.

6.4

Se um programador externo entregar código, deve igualmente confirmar por escrito que foi realizado um teste básico de segurança e que os resultados foram revistos.

6.5

Testes de segurança das aplicações

6.5.1

Antes da implementação de qualquer software ou atualização, devem ser realizados testes para identificar falhas de segurança comuns. Isto inclui:

6.5.1.1

Contorno da autenticação e do controlo de acesso

6.5.1.2

Falhas de validação de entradas, por exemplo, cross-site scripting e injeção SQL

6.5.1.3

Exposição de informação sensível em logs ou saída de depuração

6.5.1.4

Problemas de configuração, por exemplo, erros verbosos e cabeçalhos inseguros

6.5.2

Os testes devem ser documentados com:

6.5.2.1

Data do teste

6.5.2.2

Pessoa ou fornecedor que realizou o teste

6.5.2.3

Resumo das ferramentas ou métodos de teste utilizados

6.5.2.4

Resultados e ações de remediação adotadas

6.5.3

Qualquer problema crítico ou de alto risco deve ser resolvido antes de o código entrar em produção.

6.6

Componentes de terceiros e open source

6.6.1

Os programadores apenas devem utilizar bibliotecas, frameworks ou plugins de terceiros ou open source que:

6.6.1.1

Provenham de uma fonte reputada ou repositório oficial

6.6.1.2

Sejam analisados quanto a vulnerabilidades conhecidas com recurso às ferramentas disponíveis

6.6.1.3

Tenham uma licença compatível com a utilização pretendida

6.6.2

O Diretor-Geral (GM) ou o programador designado deve manter uma lista de todos os componentes externos utilizados, incluindo:

6.6.2.1

Versão e origem

6.6.2.2

Vulnerabilidades conhecidas ou estado de aplicação de patches

6.6.2.3

Data da última atualização ou revisão

6.6.3

Os componentes devem ser atualizados regularmente quando sejam disponibilizados patches de segurança. Se for detetada uma vulnerabilidade crítica, o componente deve ser atualizado ou substituído imediatamente.

6.7

Implementação e controlo de alterações

6.7.1

Todas as implementações em sistemas de produção devem seguir um processo estruturado de controlo de alterações que inclua:

6.7.1.1

Cópia de segurança dos sistemas existentes antes da implementação

6.7.1.2

Rastreio da versão do código, da data de implementação e do aprovador

6.7.1.3

Instruções de reversão em caso de falha

6.7.2

Apenas pessoal autorizado pode implementar código em sistemas de produção.

6.7.3

As alterações de emergência devem ser documentadas posteriormente e revistas no prazo de cinco dias úteis.

6.7.4

O acesso a ferramentas ou sistemas de implementação em produção deve ser controlado, registado e periodicamente revisto pelo Diretor-Geral (GM) ou pelo prestador de TI.

7. Tratamento de riscos e exceções

7.1

Qualquer risco identificado ou desvio às práticas de desenvolvimento seguro definidas nesta política deve ser documentado e sujeito a análise de risco formal.

7.2

A documentação do risco deve incluir:

7.2.1

Uma descrição clara do problema ou desvio

7.2.2

Nível de risco e impacto potencial

7.2.3

Controlos de mitigação, se aplicável

7.2.4

Prazo para resolução ou próxima revisão

7.3

O Diretor-Geral deve aprovar por escrito todas as exceções a esta política.

7.4

As seguintes são exceções comuns que devem, ainda assim, ser documentadas:

7.4.1

Utilização de ambientes temporários de teste e desenvolvimento com controlos reduzidos

7.4.2

Atraso na aplicação de um patch devido a restrições de negócio, com controlos compensatórios

7.4.3

Utilização de componentes de software não suportados quando não existam alternativas disponíveis

7.5

Se uma preservação legal, pedido regulamentar ou contrato com cliente exigir uma norma de desenvolvimento específica, o Diretor-Geral deve assegurar que todo o código e ambientes relacionados são preservados ou configurados em conformidade.

7.6

As decisões de aceitação do risco devem ser reavaliadas a cada seis meses ou imediatamente se o contexto de risco se alterar.

8. Aplicação e cumprimento

8.1

Cumprimento obrigatório

8.1.1

O cumprimento desta política é obrigatório para todos os programadores internos, contratados, fornecedores, prestadores de TI e quaisquer partes envolvidas no desenvolvimento, teste ou implementação de software para a organização.

8.1.2

O Diretor-Geral (GM) é responsável por assegurar que as práticas de desenvolvimento seguro estão integradas em todos os contratos, planos de projeto e fluxos de trabalho técnicos relevantes.

8.1.3

Todas as partes interessadas devem ser informadas desta política antes de iniciarem quaisquer atividades relacionadas com desenvolvimento.

8.2

Exemplos de violação e consequências

8.2.1

Qualquer uma das seguintes situações constitui uma violação da política:

8.2.1.1

Implementar em produção código não testado ou não revisto

8.2.1.2

Utilizar componentes com vulnerabilidades conhecidas em software disponibilizado

8.2.1.3

Permitir acesso público a ambientes de desenvolvimento ou teste

8.2.1.4

Codificar credenciais no código ou expor dados sensíveis em logs

8.2.1.5

Contornar controlos de acesso para promover alterações de código ou de configuração

8.2.2

Em função da natureza e gravidade da violação, as ações corretivas podem incluir:

8.2.2.1

Revogação imediata de acesso a sistemas ou repositórios de código

8.2.2.2

Medidas disciplinares formais para pessoal interno

8.2.2.3

Cessação do contrato para programadores externos ou prestadores de TI

8.2.2.4

Ação judicial em casos de violação de confidencialidade ou de obrigações contratuais

8.2.3

Todas as violações devem ser comunicadas ao Diretor-Geral (GM) sem demora. As comunicações podem ser feitas de forma anónima, se necessário.

8.2.4

O Diretor-Geral (GM) deve documentar cada violação, incluindo:

8.2.4.1

A natureza da violação

8.2.4.2

Quem esteve envolvido

8.2.4.3

Quando ocorreu

8.2.4.4

Que ações foram tomadas para remediar e prevenir a recorrência

8.3

Capacidade de demonstrar conformidade em auditoria e prestação de garantia ao cliente

8.3.1

Todos os registos exigidos por esta política, incluindo listas de verificação, aprovações de revisão, relatórios de testes e inventários de componentes, devem ser conservados num local central e seguro para efeitos de auditoria.

8.3.2

Durante auditorias de segurança, a organização deve ser capaz de demonstrar conformidade com os controlos de desenvolvimento seguro como parte dos requisitos da sua certificação ISO/IEC 27001.

8.3.3

Clientes e reguladores podem solicitar evidências das práticas de desenvolvimento seguro. O Diretor-Geral (GM) deve assegurar que todos os artefactos exigidos podem ser apresentados no prazo de cinco dias úteis a contar de qualquer pedido formal.

9. Requisitos de revisão e atualização

9.1

Esta política deve ser revista pelo Diretor-Geral pelo menos uma vez por ano para:

9.1.1

Verificar a manutenção da conformidade com a ISO/IEC 27001, o RGPD da UE, a Diretiva NIS2 da UE e a DORA da UE

9.1.2

Refletir ameaças atualizadas ou alterações nas melhores práticas de desenvolvimento seguro

9.1.3

Assegurar compatibilidade com quaisquer novas ferramentas, plataformas ou relações com fornecedores

9.2

As revisões intercalares devem ser desencadeadas por:

9.2.1

Qualquer incidente de segurança de software comunicado

9.2.2

Introdução de uma nova framework de desenvolvimento ou plataforma de alojamento

9.2.3

Alteração de parceiros terceiros de desenvolvimento

9.2.4

Atualizações regulamentares que afetem obrigações de software ou de segurança

9.3

Todas as alterações a esta política devem ser:

9.3.1

Documentadas com a data, resumo da alteração e aprovação do Diretor-Geral

9.3.2

Comunicadas de forma clara a todo o pessoal interno e externo de desenvolvimento

9.3.3

Conservadas como parte do controlo de versões da política da organização e do respetivo histórico de alterações

9.4

As versões atualizadas devem ser facilmente acessíveis, quer através de plataformas internas, documentação impressa ou serviços cloud acessíveis aos fornecedores.

10. Políticas relacionadas e ligações

10.1

Esta política apoia e depende da implementação eficaz de várias outras políticas SME:

10.1.1

P2S – Política de Papéis e Responsabilidades de Governação: estabelece a responsabilização pela atribuição e verificação de controlos de segurança no desenvolvimento em projetos e fornecedores.

10.1.2

P4S – Política de Controlo de Acesso: estabelece regras de base para limitar o acesso a ambientes de desenvolvimento e repositórios de código, incluindo segregação de funções.

10.1.3

P8S – Política de Sensibilização e Formação em Segurança da Informação: assegura que programadores internos e contratados compreendem as práticas de programação segura e as responsabilidades de segurança associadas.

10.1.4

P17S – Política de Proteção de Dados e Privacidade: clarifica a forma como os dados pessoais devem ser tratados durante processos de desenvolvimento, teste e registo, para cumprimento do RGPD da UE.

10.1.5

P30S – Política de Resposta a Incidentes (P30): define como os incidentes de segurança relacionados com desenvolvimento devem ser comunicados, avaliados e remediados, incluindo exposições relacionadas com código.

10.2

Estas políticas funcionam em conjunto para assegurar que o desenvolvimento seguro é operacionalizável e verificável, mesmo numa organização pequena ou com reduzida maturidade técnica.

11. Normas e quadros de referência

11.1

ISO/IEC 27001

11.1.1

Cláusula 8.1 – Exige a implementação de controlos operacionais, incluindo desenvolvimento seguro, alinhados com os objetivos de negócio e a postura de risco.

11.2

ISO/IEC 27002

11.2.1

Controlo 8.25 – Recomenda a integração da segurança ao longo de todo o ciclo de vida do software, incluindo controlo de código-fonte, controlo de versões e acesso de programadores.

11.2.2

Controlo 8.26 – Especifica métodos para testes de aplicações e verificação das funcionalidades de segurança antes da entrada em produção.

11.2.3

Controlo 8.27 – Exige que programadores terceiros cumpram as mesmas normas de desenvolvimento e que as suas responsabilidades de segurança estejam claramente definidas.

11.3

NIST SP 800-53 Rev.5

11.3.1

SA-3 a SA-15 – Definem processos de desenvolvimento seguro, incluindo controlo de acesso de programadores, testes, modelação de ameaças e documentação.

11.3.2

SI-10 – Exige que os programadores identifiquem e mitiguem fraquezas comuns de software e utilizem ferramentas automatizadas, quando aplicável.

11.4

RGPD da UE (2016/679)

11.4.1

Artigo 25 – «Proteção de Dados desde a Conceção e por Defeito» impõe a integração de salvaguardas de segurança e privacidade durante a conceção e o desenvolvimento de software, em especial quando sejam tratados dados pessoais.

11.5

Diretiva NIS2 da UE (2022/2555)

11.5.1

Artigo 21(2)(a), (e) e (h) – Exige políticas de desenvolvimento seguro, supervisão da utilização de componentes open source e mitigação documentada dos riscos relacionados com aplicações em entidades essenciais e importantes.

11.6

DORA da UE (2022/2554)

11.6.1

Artigos 6(7), 9(1)(c) e 10(2)(c) – Impõem obrigações de segurança no ciclo de vida de desenvolvimento para entidades do setor financeiro, incluindo PME, em particular para sistemas críticos de TIC.

11.7

COBIT 2019

11.7.1

BAI03 – «Gerir a identificação e construção de soluções» apoia a implementação de controlos de desenvolvimento estruturados que enfatizam segurança, rastreabilidade e resiliência, adaptados às limitações das PME.