					Insira aqui a designação da entidade jurídica registada							
Número do documento: P25S					Título do documento: **Política de Requisitos de Segurança das Aplicações**							
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 operacionais, incluindo a segurança das aplicações
ISO/IEC 27002:2022	Controlos 8.25–8.26	Conceção segura, desenvolvimento, testes e revisão de código
NIST SP 800-53 Rev.5	SA-11, SI-10	Testes de programadores/aplicações, análise de código e prevenção de falhas
RGPD da UE	Artigo 25	Proteção de Dados desde a Conceção e por Defeito
Diretiva NIS2 da UE	Artigo 21(2)(a), (e)	Medidas técnicas para proteger aplicações e detetar riscos
DORA da UE	Artigos 9(2)(c), 10(2)(c)	Segurança das aplicações para a resiliência operacional digital
COBIT 2019	BAI03	Gerir a construção/aquisição segura de software

1. Finalidade

1.1 A presente política define os controlos mínimos obrigatórios de segurança das aplicações aplicáveis a todas as soluções de software e sistemas utilizados pela organização, independentemente de serem desenvolvidos internamente ou adquiridos a fornecedores externos.

1.2 Assegura que as aplicações são concebidas, implementadas e mantidas de modo a proteger os dados de clientes, trabalhadores e do negócio contra acesso não autorizado, utilização indevida, alteração ou destruição.

1.3 Esta política apoia os esforços da organização para obter e manter a certificação ISO/IEC 27001, cumprir as obrigações do RGPD da UE e da Diretiva NIS2 da UE, e reduzir os riscos operacionais associados a implementações de software inseguras.

1.4 Contribui para uma abordagem consistente e auditável à segurança das aplicações em PME, ao estabelecer uma lista de verificação uniforme de funcionalidades e práticas de segurança, adaptada a ambientes com recursos técnicos internos limitados.

2. Âmbito

2.1 Esta política aplica-se a todas as aplicações, sistemas, ferramentas e plataformas que:

2.1.1 Sejam desenvolvidos internamente, personalizados ou criados por script para utilização interna

2.1.2 Sejam adquiridos como software comercial, SaaS ou sistemas baseados na cloud

2.1.3 Tratem, armazenem ou transmitam dados pessoais, registos do negócio ou informação operacional sensível

2.1.4 Sejam acedidos por trabalhadores, contratados, clientes ou parceiros através de redes internas, da Internet ou de plataformas móveis

2.2 A política abrange:

2.2.1 Programadores internos ou contratados

2.2.2 Fornecedores de software e prestadores de serviços cloud

2.2.3 Pessoal de suporte de TI ou administradores responsáveis pela implementação e suporte

2.2.4 Proprietários das aplicações e utilizadores de negócio envolvidos na aprovação e supervisão dos sistemas

3. Objetivos

3.1 Assegurar que todas as aplicações utilizadas pela organização dispõem de controlos de segurança incorporados e verificáveis que mitiguem vulnerabilidades comuns de software.

3.2 Proteger a Confidencialidade, Integridade e Disponibilidade dos dados tratados pelas aplicações, independentemente do local onde estejam alojadas.

3.3 Exigir testes formais, revisão e validação da segurança das aplicações antes de qualquer nova aplicação ou atualização com impacto significativo ser aprovada para utilização em produção.

3.4 Garantir o tratamento consistente e seguro das credenciais de autenticação, dos dados de sessão e dos direitos de acesso em todos os sistemas críticos para o negócio.

3.5 Exigir funcionalidades seguras de registo, rastreabilidade de auditoria e monitorização em todas as aplicações, para apoiar a deteção e a resposta a atividade suspeita.

3.6 Reduzir os riscos legais e de conformidade, assegurando que as aplicações cumprem os requisitos regulamentares de segurança aplicáveis.

4. Papéis e responsabilidades

4.1 Diretor-Geral (GM)

4.1.1 Detém a responsabilidade global pela segurança das aplicações em toda a organização.

4.1.2 Aprova esta política e assegura que todas as aquisições ou projetos de desenvolvimento a cumprem.

4.1.3 Assegura que fornecedores e prestadores de serviços ficam contratualmente vinculados aos requisitos de segurança das aplicações.

4.1.4 Revê e aprova exceções ao risco quando o cumprimento integral não puder ser alcançado devido a restrições do negócio.

4.2 Proprietário da aplicação (quando designado)

4.2.1 Identifica as necessidades específicas de segurança da aplicação durante a seleção do sistema ou o arranque do projeto.

4.2.2 Verifica que funcionalidades essenciais, como proteção da autenticação, cifragem e registo de atividades, estão incluídas.

4.2.3 Participa nas revisões prévias à implementação e confirma que os controlos de segurança satisfazem as necessidades do negócio.

[... 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 Diretor-Geral pelo menos uma vez por ano civil para:

9.1.1 Refletir alterações nos requisitos regulamentares (por exemplo, RGPD da UE, Diretiva NIS2 da UE, DORA da UE)

9.1.2 Incorporar ameaças novas ou emergentes e técnicas de ataque

9.1.3 Atualizar a redação e os requisitos para refletir alterações em plataformas, fornecedores ou métodos de desenvolvimento

9.2 Devem igualmente ser realizadas revisões intercalares quando:

9.2.1 Sejam introduzidas novas aplicações

9.2.2 As aplicações existentes sofram atualizações significativas ou integrações

9.2.3 Ocorra um incidente ou violação relacionado com a aplicação

9.2.4 Sejam identificados novos riscos a partir de avisos externos ou alertas setoriais

9.3 Todas as atualizações desta política devem ser:

9.3.1 Aprovadas pelo Diretor-Geral

9.3.2 Documentadas com histórico de versões e motivo da alteração

9.3.3 Comunicadas a todos os trabalhadores, programadores e fornecedores envolvidos na gestão de aplicações

9.3.4 Armazenadas de forma segura para referência de auditoria e conformidade

10. Políticas relacionadas e articulações

10.1 Esta política é diretamente suportada pelas seguintes políticas de segurança alinhadas com PME e contribui para a respetiva aplicação:

10.1.1 P2S – Política de Papéis e Responsabilidades de Governação: atribui a responsabilidade pela aprovação de aplicações, aplicação da política e gestão de fornecedores.

10.1.2 P4S – Política de Controlo de Acesso: assegura que o acesso às aplicações está alinhado com o princípio do menor privilégio e com os princípios de controlo de sessão.

10.1.3 P8S – Política de Sensibilização e Formação em Segurança da Informação: assegura que utilizadores e programadores recebem formação para reconhecer e comunicar ameaças relacionadas com aplicações.

10.1.4 P17S – Política de Proteção de Dados e Privacidade: estabelece salvaguardas de privacidade de dados que devem ser aplicadas por qualquer aplicação que trate informações de identificação pessoal (PII).

10.1.5 P14S – Política de Retenção e Eliminação de Dados: rege a forma como os registos gerados pela aplicação, as cópias de segurança e os dados sensíveis devem ser retidos, arquivados e eliminados de forma segura.

10.1.6 P30S – Política de Resposta a Incidentes (P30): define as etapas para identificar, comunicar e conter eventos de segurança relacionados com aplicações.

10.2 Em conjunto, estas políticas asseguram que a segurança das aplicações está plenamente integrada no Sistema de Gestão da Segurança da Informação (SGSI) da organização e que existe capacidade de demonstrar conformidade em auditoria.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 A Cláusula 8.1 exige que as organizações estabeleçam controlos operacionais para tratar riscos de segurança da informação, incluindo os relacionados com aplicações e sistemas de software.

11.2 ISO/IEC 27002

11.2.1 O Controlo 8.25 recomenda a implementação de práticas seguras de conceção, desenvolvimento e revisão de código em todas as aplicações, incluindo as fornecidas por fornecedores.

11.2.2 O Controlo 8.26 recomenda testes formais aos controlos de segurança das aplicações, em particular nas áreas de controlo de acesso, validação de entradas e gestão de sessões.

11.3 NIST SP 800-53 Rev.5

11.3.1 O SA-11 especifica requisitos para testes de programadores, análise de código e varrimento dinâmico de aplicações antes da implementação.

11.3.2 O SI-10 trata da deteção e prevenção de falhas comuns de software, com ênfase na sensibilização dos programadores e nas salvaguardas técnicas.

11.4 RGPD da UE (2016/679)

11.4.1 O Artigo 25 – «Proteção de Dados desde a Conceção e por Defeito» exige a incorporação da privacidade e da segurança na conceção de base das aplicações que tratam dados pessoais.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 O Artigo 21(2)(a) e (e) exige que as entidades essenciais e importantes implementem medidas técnicas para proteger aplicações e detetar riscos relacionados com software.

11.6 DORA da UE (2022/2554)

11.6.1 Os Artigos 9(2)(c) e 10(2)(c) exigem que as PME do setor financeiro incorporem controlos de segurança ao nível da aplicação e realizem avaliações regulares para manter a resiliência operacional digital.

11.7 COBIT 2019

11.7.1 O BAI03 – «Manage Solutions Identification and Build» orienta o desenvolvimento ou a aquisição de software seguro, alinhado com requisitos de risco, conformidade e negócio, mesmo em ambientes de PME com recursos limitados.