| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Insira aqui a designação da entidade jurídica registada | | | | | | | |
| Número do documento:<br>P25 | | | | | Título do documento:<br>**Política de Requisitos de Segurança das Aplicações** | | | | | | | |
| Versão:<br>1.0 | | Data de entrada em vigor:<br>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 | — |
| ISO/IEC 27002:2022 | Controlos 8.25–8.26 | — |
| NIST SP 800-53 Rev.5 | SA-11, SA-15, SI-10 | — |
| RGPD da UE | Artigos 25, 32 | — |
| Diretiva NIS2 da UE | Artigos 21(2)(f), 23 | — |
| DORA da UE | Artigos 9, 11 | — |
| COBIT 2019 | BAI03, BAI09, DSS05 | — |

**1. Finalidade**

1.1 Esta política define requisitos obrigatórios de segurança aplicacional para software desenvolvido, adquirido, integrado ou implementado pela organização. Assegura que todas as aplicações são concebidas, implementadas e mantidas em conformidade com princípios de desenvolvimento seguro, obrigações regulamentares e o apetite ao risco da organização.

1.2 A política impõe a integração da segurança ao longo de todo o ciclo de vida das aplicações, abrangendo a autenticação de utilizadores, o tratamento de dados, a proteção de interfaces e a interação segura com APIs ou serviços.

1.3 Ao adotar esta política, a organização pretende prevenir a introdução de vulnerabilidades de software, proteger dados sensíveis e assegurar rastreabilidade e resiliência contra exploração e abuso.

**2. Âmbito**

**2.1 Esta política aplica-se a:**

2.1.1 Aplicações desenvolvidas internamente ou adquiridas externamente, incluindo SaaS e ferramentas desenvolvidas à medida

2.1.2 Aplicações que suportam operações críticas de negócio, acesso de clientes ou tratamento de dados regulados

2.1.3 Equipas de desenvolvimento, DevOps, QA, produto e segurança

2.1.4 Desenvolvedores terceiros, fornecedores de software e parceiros de integração com acesso a aplicações da organização ou a APIs

2.2 Aplica-se a todos os ambientes: desenvolvimento, testes, staging, produção e recuperação de desastre, independentemente de estarem alojados em infraestrutura on-premises, em centros de dados privados ou em ambientes de cloud pública.

**3. Objetivos**

3.1 Definir requisitos de segurança funcionais e não funcionais de referência a cumprir por todas as aplicações, independentemente da metodologia de desenvolvimento ou da stack tecnológica.

3.2 Assegurar a integração de proteções ao nível da aplicação, incluindo validação de entradas, codificação de saídas, tratamento de erros e segurança de sessões.

3.3 Exigir a implementação segura de mecanismos de autenticação, autorização e controlo de acesso alinhados com as políticas organizacionais de identidade e acesso.

3.4 Tornar obrigatória a interação segura com APIs, interfaces web e componentes de terceiros através de protocolos aprovados e controlos de segurança.

3.5 Permitir a deteção precoce e a mitigação de vulnerabilidades através de análise estática e dinâmica, revisões de código e modelação de ameaças.

3.6 Proteger dados sensíveis em conformidade com requisitos regulamentares, impondo cifragem, classificação da informação e lógica de retenção de dados.

3.7 Assegurar a validação contínua da postura de segurança das aplicações após a implementação, através de testes, monitorização e capacidade de demonstrar conformidade em auditoria.

## 4. Papéis e responsabilidades

### 4.1 Diretor de Segurança da Informação (CISO)

4.1.1 É responsável por esta política e assegura o seu alinhamento com a estratégia de segurança da informação e a postura de risco da organização.

4.1.2 Aprova os requisitos de segurança das aplicações e impõe controlos obrigatórios nas funções de desenvolvimento e aquisição.

### 4.2 Responsável pela Segurança das Aplicações / Gestor de DevSecOps

4.2.1 Define controlos de segurança de referência e metodologias de teste para componentes aplicacionais.

4.2.2 Supervisiona a integração segura de ferramentas como SAST, DAST, IAST e SCA no pipeline de entrega de software.

4.2.3 Mantém a Lista de Verificação de Requisitos de Segurança das Aplicações e os critérios de validação.

[ ... 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 Divulgação de vulnerabilidades críticas que afetem frameworks ou dependências comuns

9.1.2 Atualizações às obrigações regulamentares relativas à segurança das aplicações (por exemplo, NIS2, DORA)

9.1.3 Alterações com impacto significativo nas práticas de desenvolvimento de software, ferramentas ou arquitetura cloud da organização

9.1.4 Constatações de auditorias internas ou de testes de intrusão externos

9.2 A revisão deve ser conduzida pelo Responsável pela Segurança das Aplicações, em coordenação com o CISO, responsáveis de engenharia DevOps, Jurídico, Aquisição e QA.

9.3 Todas as revisões devem estar sujeitas a controlo de versões no registo de controlo documental do SGSI e ser distribuídas a todas as equipas de desenvolvimento e produto afetadas.

9.4 As versões substituídas devem ser arquivadas por um período não inferior a três anos para efeitos de rastreabilidade, auditabilidade e apoio à investigação de violações.

## 10. Políticas relacionadas e ligações

10.1 P1 – Política de Segurança da Informação. Estabelece a base para a proteção de sistemas e dados, no âmbito da qual são exigidos controlos ao nível da aplicação para prevenir acessos não autorizados, fuga de dados e exploração.

10.2 P4 – Política de Controlo de Acesso. Define as normas de gestão de identidade e de sessões que devem ser aplicadas por todas as aplicações, incluindo autenticação forte, princípio do menor privilégio e requisitos de revisão de acessos.

10.3 P5 – Política de Gestão de Alterações. Regula a promoção de código aplicacional e de configurações para ambientes de produção, assegurando que alterações não autorizadas ou não testadas são bloqueadas.

10.4 P17 – Política de Proteção de Dados e Privacidade. Exige que as aplicações implementem privacidade desde a conceção e assegurem o tratamento lícito, a cifragem e a retenção de dados pessoais e sensíveis em todos os ambientes.

10.5 P24 – Política de Desenvolvimento Seguro. Fornece o quadro mais abrangente para incorporar a segurança no SDLC, definindo esta política os requisitos concretos e os controlos técnicos a implementar ao nível da aplicação.

10.6 P30 – Política de Resposta a Incidentes (P30). Torna obrigatório o tratamento estruturado de incidentes de segurança das aplicações, incluindo vulnerabilidades identificadas após a implementação ou durante testes de intrusão, e define procedimentos de escalonamento, contenção e recuperação.

## 11. Normas e quadros de referência

### 11.1 ISO/IEC 27001:2022

11.1.1 Cláusula 8.1 – Planeamento e controlo operacional: Exige que a segurança das aplicações seja incorporada em processos e sistemas para assegurar confidencialidade, integridade e disponibilidade.

### 11.2 ISO/IEC 27002:2022

11.2.1 Controlos 8.25–8.26: Detalham as expectativas para a segurança ao nível da aplicação, incluindo práticas de programação segura, modelação de ameaças, controlos arquiteturais e validação de software de terceiros.

11.2.2 Controlo do Anexo A 8.25 – Ciclo de Vida de Desenvolvimento Seguro: Impõe a integração da segurança ao longo do ciclo de vida das aplicações.

11.2.3 Controlo do Anexo A 8.26 – Requisitos de Segurança das Aplicações: Torna obrigatória a definição e aplicação de controlos técnicos para proteger aplicações contra uso indevido e comprometimento.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – Testes e avaliação de segurança pelo desenvolvedor: Torna obrigatórios testes estáticos, dinâmicos e de intrusão durante o desenvolvimento.

11.3.2 SA-15 – Processo de desenvolvimento, normas e ferramentas: Estabelece normas formais para o desenvolvimento seguro de aplicações.

11.3.3 SI-10 – Validação de entradas de informação: Exige mecanismos de controlo para prevenir ataques de injeção e de parsing.

### 11.4 RGPD da UE (2016/679)

11.4.1 Artigo 25 – Proteção de Dados desde a Conceção e por Defeito: Exige a integração da proteção de dados e da privacidade na lógica aplicacional e nos fluxos de trabalho.

11.4.2 Artigo 32 – Segurança do Tratamento: Torna obrigatórias medidas técnicas adequadas, como validação de entradas, cifragem e controlos seguros de acesso.

### 11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(f): Exige tratamento de vulnerabilidades e práticas seguras ao longo do ciclo de vida das aplicações para entidades essenciais e importantes.

11.5.2 Artigo 23 – Notificação de incidentes de segurança: Exige capacidades de registo e monitorização ao nível da aplicação para detetar e notificar incidentes significativos.

### 11.6 DORA da UE (2022/2554)

11.6.1 Artigo 9 – Gestão do risco das TIC: Obriga as entidades financeiras a assegurar que as aplicações são seguras, testadas e resilientes face a ameaças cibernéticas.

11.6.2 Artigo 11 – Testes de ferramentas TIC: Incentiva a realização periódica de testes de intrusão e exercícios de red team a aplicações e serviços críticos.

**11.7 COBIT 2019**

11.7.1 BAI03 – Gerir a identificação e construção de soluções: Estabelece requisitos de conceção e controlo durante o desenvolvimento de aplicações.

11.7.2 BAI09 – Gerir aplicações: Dá ênfase à manutenção segura, monitorização e melhoria de aplicações em produção.

11.7.3 DSS05 – Gerir Serviços de Segurança: Relaciona a proteção das aplicações com operações e controlos de segurança organizacionais mais amplos.