					Insira aqui a designação da entidade jurídica registada							
Número do documento: P29S					Título do documento: **Política de Dados de Teste e Ambientes de Teste**							
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 aplicáveis

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusulas 6.1, 8	
ISO/IEC 27002:2022	Controlos 8.28–8.29	
NIST SP 800-53 Rev. 5	SA-11, SA-12, SC-32	
RGPD da UE	Artigos 5(1)(c), 25, 32	
Diretiva NIS2 da UE	Artigo 21(2)(e), (h)	
DORA da UE	Artigo 9	
COBIT 2019	BAI07, DSS05	

1. Finalidade

1.1 Esta política define a forma como os dados de teste e os ambientes de teste devem ser geridos, de modo a prevenir a exposição acidental, violações de dados ou perturbações operacionais durante atividades de teste.

1.2 Assegura que dados reais de clientes nunca são utilizados indevidamente durante testes de software ou de sistemas e que os ambientes de teste se mantêm lógica e tecnicamente separados dos sistemas de produção.

1.3 Esta política foi concebida para apoiar as PME no cumprimento dos requisitos de certificação ISO/IEC 27001 e da legislação aplicável em matéria de proteção de dados, mantendo-se prática e aplicável a organizações sem uma equipa de TI dedicada.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os ambientes de teste (por exemplo, servidores de staging, sistemas sandbox, plataformas de teste de desenvolvimento)

2.1.2 Todos os dados de teste, quer sejam criados manualmente, gerados ou derivados de dados em produção

2.1.3 Todo o pessoal envolvido em atividades de teste, incluindo trabalhadores, contratados, freelancers e prestadores de serviços de TI

2.1.4 Quaisquer testes suscetíveis de impactar plataformas de atendimento ao cliente, sistemas empresariais internos ou serviços de terceiros

2.2 Abrange tanto os ambientes técnicos como os processos utilizados para suportar:

2.2.1 Desenvolvimento de websites, aplicações e ferramentas

2.2.2 Atualizações de sistemas, testes de configuração e testes de integração

2.2.3 Testes funcionais ou de segurança, automatizados e manuais

3. Objetivos

3.1 Prevenir a utilização de dados reais e identificáveis de clientes em testes, exceto quando anonimizados e expressamente aprovados.

3.2 Manter uma separação rigorosa entre sistemas de teste e de produção, de modo a evitar exposição indevida de dados ou interferência operacional.

3.3 Proteger os sistemas e os dados de teste contra acesso não autorizado, divulgação acidental ou reutilização entre ambientes sem os controlos adequados.

3.4 Cumprir os regulamentos aplicáveis em matéria de proteção de dados (por exemplo, RGPD, NIS2), assegurando que todos os dados de teste são tratados de forma lícita, leal e segura.

3.5 Apoiar a capacidade da organização para demonstrar conformidade em auditorias externas e no âmbito da certificação ISO/IEC 27001, através da documentação das práticas de teste e da aplicação consistente de salvaguardas.

4. Papéis e responsabilidades

4.1 Diretor-Geral (DG)

4.1.1 Detém a responsabilidade global pela proteção dos dados de teste e pela segurança dos sistemas de teste.

4.1.2 Aprova qualquer utilização de dados reais em testes, após confirmar a existência de salvaguardas adequadas (por exemplo, anonimização ou mascaramento de dados).

4.1.3 Verifica que as atividades de teste estão devidamente documentadas e cumprem esta política.

4.2 Responsável pelo projeto

4.2.1 Coordena a conceção e a execução dos processos de teste.

4.2.2 Assegura que todos os membros da equipa compreendem e cumprem esta política.

4.2.3 Confirma que os sistemas de teste estão configurados de forma segura antes do início dos testes.

4.2.4 Comunica ao Diretor-Geral (DG) quaisquer incidentes relacionados com ambientes de teste ou fugas de dados.

[... 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 Revisões agendadas

9.1.1 Esta política deve ser revista pelo menos uma vez por ano pelo Diretor-Geral (DG). A revisão assegura que a política se mantém atual face a:

9.1.1.1 Alterações nas ferramentas, plataformas ou ambientes de desenvolvimento de software

9.1.1.2 Atualização das obrigações legais, incluindo requisitos de proteção de dados ou de resiliência digital

9.1.1.3 Certificação das PME e capacidade de demonstrar conformidade em auditoria no âmbito da ISO/IEC 27001

9.2 Eventos desencadeadores de revisão intercalar

9.2.1 Devem ser realizadas revisões adicionais na sequência de:

9.2.1.1 Qualquer incidente que envolva exposição de dados ou comprometimento em ambientes de teste

9.2.1.2 Utilização de dados reais em testes, mesmo quando anonimizados

9.2.1.3 Introdução de novos métodos de teste, sistemas ou fornecedores

9.2.1.4 Atualizações regulamentares que afetem a forma como os dados são tratados durante os testes

9.3 Gestão de alterações e comunicação

9.3.1 O Diretor-Geral (DG) é responsável por:

9.3.1.1 Atualizar esta política e documentar quaisquer revisões com o respetivo histórico de versões

9.3.1.2 Notificar trabalhadores, programadores e prestadores de serviços relevantes sobre as atualizações

9.3.1.3 Confirmar que todo o pessoal envolvido em atividades de teste compreende e aplica as regras mais recentes

9.3.1.4 Manter acessível a versão mais recente da política para efeitos de revisão e auditoria

9.4 Auditoria e documentação

9.4.1 Os registos de todas as revisões da política, aprovações de utilização de dados reais e justificações de exceções devem ser:

9.4.1.1 Retidos de forma segura para fins de auditoria

9.4.1.2 Disponibilizados mediante pedido durante auditorias internas ou de terceiros

9.4.1.3 Revistos anualmente para assegurar a consistência com as práticas de teste

10. Políticas relacionadas e articulação

10.1 Esta política deve ser aplicada em articulação com as seguintes políticas SME, de forma a manter a segurança e a conformidade durante os testes:

10.1.1 P2S – Política de Papéis e Responsabilidades de Governação: Define quem é responsável pela supervisão do desenvolvimento, dos testes e das responsabilidades de segregação de sistemas.

10.1.2 P4S – Política de Controlo de Acesso: Regula a atribuição, gestão e remoção das credenciais de acesso aos sistemas de teste.

10.1.3 P8S – Política de Sensibilização e Formação em Segurança da Informação: Assegura que os trabalhadores compreendem os riscos associados aos dados de teste, as práticas de tratamento seguro e a separação adequada dos ambientes.

10.1.4 P13S – Política de Classificação e Rotulagem da Informação: Apoia a classificação clara dos dados de teste e orienta as estratégias de anonimização ou mascaramento de dados.

10.1.5 P17S – Política de Proteção de Dados e Privacidade: Alinha-se com as obrigações do RGPD, incluindo salvaguardas relativas ao tratamento e armazenamento de dados pessoais, mesmo em ambientes de teste.

10.1.6 P24S – Política de Desenvolvimento Seguro: Define as expectativas gerais de segurança para as equipas de desenvolvimento, incluindo a utilização segura de dados durante as fases de teste.

10.1.7 P30S – Política de Resposta a Incidentes: Define a forma de resposta a qualquer violação ou problema identificado num ambiente de teste ou causado por tratamento inadequado de dados de teste.

10.2 Estas políticas constituem um quadro de segurança unificado para suportar a integridade dos testes, a minimização de dados e o alinhamento integral com a ISO/IEC 27001 nas operações de desenvolvimento e garantia da qualidade.

11. Normas e referenciais aplicáveis

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1 – Exige avaliação de riscos e ações de tratamento, incluindo riscos relacionados com testes.

11.1.2 Cláusula 8.1 – Exige o planeamento e o controlo dos processos operacionais, incluindo a configuração de ambientes de sistemas de teste.

11.2 ISO/IEC 27002

11.2.1 Controlo 8.28 – Exige que as organizações protejam os dados de teste e assegurem que estes não contêm dados sensíveis nem dados reais de produção.

11.2.2 Controlo 8.29 – Exige a separação clara entre ambientes de desenvolvimento, teste e produção.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SA-11 – Abrange os requisitos de controlo aplicáveis ao desenvolvimento e aos testes.

11.3.2 SA-12 – Aborda os riscos de teste na cadeia de abastecimento e as avaliações de segurança.

11.3.3 SC-32 – Exige a separação de ambientes e a proteção da confidencialidade e integridade dos dados de teste.

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

11.4.1 Artigo 5(1)(c) – Exige a minimização de dados, incluindo a utilização apenas dos dados necessários para testes.

11.4.2 Artigo 25 – Exige proteção de dados desde a conceção e por defeito, incluindo controlos sobre ambientes de teste.

11.4.3 Artigo 32 – Exige o tratamento seguro de dados pessoais em todos os sistemas, incluindo ambientes de não produção.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(e, h) – Exige desenvolvimento seguro e testes de sistemas, em particular quando os serviços digitais estão expostos a risco cibernético.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 9 – Salienta a importância da resiliência operacional digital, incluindo os testes seguros dos sistemas TIC pelas PME do setor financeiro.

11.7 COBIT 2019

11.7.1 BAI07 – Gerir a aceitação da mudança e a transição: Inclui controlos de teste para validar novos sistemas e o tratamento de dados.

11.7.2 DSS05 – Gerir Serviços de Segurança: Exige práticas de teste e desenvolvimento que previnam a utilização indevida ou a exposição de dados do negócio.