					Insira aqui a designação da entidade jurídica registada							
Número do documento: P29					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

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 8	Relevante para o planeamento e controlo operacional seguros dos dados e dos ambientes de teste
ISO/IEC 27002:2022	Controlos 8.28–8.29	Abrange dados de teste seguros e a proteção dos ambientes de teste
NIST SP 800-53 Rev.5	SA-11, SC-28, SC-32	Aborda testes e avaliação por programadores, proteção de dados em repouso e integridade
RGPD da UE	Artigos 5, 25, 32	Abrange minimização de dados, privacidade desde a conceção e segurança do tratamento em contextos de teste
Diretiva NIS2 da UE	Artigo 21(2)(e), (h)	Relaciona-se com práticas seguras de desenvolvimento e teste
DORA da UE	Artigo 9	Diz respeito a sistemas e protocolos de TIC e à segurança dos dados de teste
COBIT 2019	DSS05, BAI07	Trata da gestão de serviços de segurança e da aceitação e transição de alterações

1. Finalidade

1.1. A presente política define os requisitos obrigatórios para a gestão de ambientes de teste e de dados de teste, de forma a assegurar a segurança, a confidencialidade e a integridade operacional ao longo do ciclo de vida de desenvolvimento e teste de software.

1.2. Esta política visa prevenir acessos não autorizados, fugas de dados e contaminação de sistemas de produção resultantes de ambientes de teste inadequadamente geridos ou da utilização de dados reais em atividades de teste.

1.3. A política estabelece o tratamento seguro dos dados utilizados para testes, o reforço da infraestrutura de teste e o controlo de acesso baseado em funções, em alinhamento com as obrigações regulamentares e contratuais aplicáveis.

2. Âmbito

2.1. Esta política aplica-se a todos os ambientes de teste, dados, ferramentas e processos utilizados para testes de software, sistemas, aplicações e infraestruturas em toda a organização.

2.2. Abrange:

2.2.1. Ambientes de teste provisionados em infraestrutura local, na cloud ou através de plataformas de terceiros

2.2.2. Dados de teste utilizados em testes funcionais, de desempenho, de regressão e de segurança

2.2.3. Testes manuais, executados por scripts ou automatizados (por exemplo, pipelines de CI/CD)

2.2.4. Todo o pessoal envolvido em testes, incluindo equipas internas, fornecedores e prestadores de serviços

2.3. A política aplica-se independentemente da criticidade do sistema, do tipo de aplicação ou de o desenvolvimento ser interno ou externalizado.

3. Objetivos

3.1. Prevenir a utilização de dados de produção, sensíveis ou regulados (por exemplo, informações de identificação pessoal (PII), dados de titulares de cartões) em ambientes de teste, salvo se estiverem anonimizados ou especificamente aprovados.

3.2. Assegurar a segregação completa de rede e de acessos entre ambientes de teste e de produção, para evitar acessos não autorizados a dados ou contaminação de sistemas.

3.3. Exigir cifragem, mascaramento de dados ou geração de dados sintéticos sempre que sejam necessários dados representativos para fins de teste.

3.4. Reduzir a probabilidade de falhas de conformidade, exposição de dados de clientes ou interrupções operacionais resultantes de dados ou ambientes de teste inseguros.

3.5. Alinhar o tratamento de dados de teste com normas da indústria (ISO, NIST, COBIT) e regulamentos como o RGPD da UE, a Diretiva NIS2 da UE e o DORA da UE.

4. Papéis e responsabilidades

4.1. Diretor de Segurança da Informação (CISO)

4.1.1. É responsável por esta política e assegura a implementação de salvaguardas técnicas e administrativas para os dados e os ambientes de teste.

4.1.2. Aprova a utilização de dados reais ou sensíveis em testes, mediante justificação adequada e controlos compensatórios.

4.2. Responsáveis de QA/Testes

4.2.1. Coordenam o planeamento dos testes e asseguram que todas as atividades de teste cumprem os requisitos desta política.

4.2.2. Validam a segregação adequada, os acessos e a preparação dos dados para cada fase de teste.

[... 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 e atualizada sempre que necessário para refletir:

9.1.1. Alterações nos requisitos regulamentares (por exemplo, RGPD da UE, DORA da UE, Diretiva NIS2 da UE)

9.1.2. A adoção de novas ferramentas, plataformas ou pipelines de automatização de testes

9.1.3. Constatações de auditoria interna ou recomendações pós-incidente

9.1.4. A expansão de processos de desenvolvimento ou de QA que alterem o tratamento de dados de teste ou a utilização dos ambientes

9.2. O CISO é responsável por iniciar a revisão em colaboração com:

9.2.1. Responsáveis de QA/Testes

9.2.2. Gestores de DevOps e de Infraestruturas

9.2.3. Equipas de Desenvolvimento de Aplicações

9.2.4. Encarregado da Proteção de Dados (EPD) e assessoria jurídica

9.3. Todas as revisões devem ser:

9.3.1. Sujeitas a controlo de versões e armazenadas no repositório documental central

9.3.2. Comunicadas ao pessoal afetado através de canais formais (por exemplo, notificações do SGSI, briefings de equipa)

9.3.3. Associadas a atualizações de normas técnicas, controlos e procedimentos operacionais relacionados

9.4. Devem ser realizadas revisões intercalares com base em eventos desencadeadores, imediatamente após qualquer:

9.4.1. Fuga de dados ou violação envolvendo ambientes de teste

9.4.2. Não conformidade de auditoria relacionada com o tratamento de dados de teste

9.4.3. Alteração significativa das obrigações legais ou da arquitetura de TI

10. Políticas relacionadas e ligações

10.1. Esta política está estreitamente integrada com as seguintes políticas, a fim de assegurar o tratamento seguro e conforme dos dados e dos ambientes de teste:

10.1.1. P1 – Política de Segurança da Informação: Estabelece os princípios gerais de segurança que regem a proteção dos dados de teste e a gestão dos ambientes.

10.1.2. P5 – Política de Gestão de Alterações: Aplica-se à criação, atualização e desativação de ambientes de teste e pipelines de implementação.

10.1.3. P13 – Política de Classificação e Rotulagem da Informação: Orienta a seleção de dados de teste e a aplicação de controlos com base na sensibilidade.

10.1.4. P14 – Política de Retenção e Eliminação de Dados: Define os prazos de retenção e os requisitos de eliminação segura para conjuntos de dados de teste.

10.1.5. P15 – Política de Cópias de Segurança e Restauro: Determina as práticas de cópia de segurança e a validação da recuperação para ambientes de teste.

10.1.6. P18 – Política de Controlos Criptográficos: Especifica as normas obrigatórias de cifragem para dados em repouso e em trânsito nas plataformas de teste.

10.1.7. P22 – Política de Registo de Logs e Monitorização: Regula a visibilidade e a deteção de anomalias nas atividades dos ambientes de teste.

10.1.8. P30 – Política de Resposta a Incidentes: Define o escalonamento e a remediação para violações ou incidentes que envolvam sistemas de teste.

10.1.9. P33 – Política de Monitorização de Auditoria e Conformidade: Permite validar o cumprimento da política e a garantia contínua.

11. Normas e referenciais aplicáveis

11.1. Esta política está alinhada com normas globais de cibersegurança e referenciais regulamentares que exigem o tratamento seguro de dados de teste e a proteção de ambientes de não produção.

11.2. ISO/IEC 27001:

11.2.1. Cláusula 8.1 - Exige o planeamento e controlo seguros dos dados e dos ambientes de teste.

11.3. ISO/IEC 27002:2022 – Controlos 8.28–8.29:

11.3.1. Controlo 8.28 do Anexo A – Dados de teste seguros: Exige a proteção dos dados de teste utilizados nas fases de desenvolvimento e teste através de anonimização, mascaramento ou geração sintética.

11.3.2. Controlo 8.29 do Anexo A – Proteção dos ambientes de teste: Exige segregação face à produção, controlos de acesso e reforço dos ambientes de sistemas de teste.

11.3.3. Estes controlos definem requisitos para gerir com segurança os dados utilizados durante os testes e para proteger sistemas de não produção contra utilização indevida, comprometimento ou contaminação.

11.4. NIST SP 800-53 Rev.5:

11.4.1. SA-11 – Testes e avaliação por programadores: Estabelece expectativas para procedimentos de teste seguros e repetíveis com controlos de dados adequados.

11.4.2. SC-28 – Proteção da informação em repouso: Alinha-se com a cifragem de dados de teste armazenados em sistemas de não produção.

11.4.3. SC-32 – Integridade da informação: Suporta validação de dados, prevenção de corrupção e controlos de entrada/saída durante os testes.

11.5. RGPD da UE (2016/679):

11.5.1. Artigo 5 – Minimização de dados: Proíbe a utilização desnecessária de dados pessoais em testes.

11.5.2. Artigo 25 – Privacidade desde a conceção: Exige que técnicas de proteção de dados sejam aplicadas desde o início do ciclo de desenvolvimento e teste.

11.5.3. Artigo 32 – Segurança do tratamento: Impõe salvaguardas para ambientes de teste que tratem dados pessoais ou sensíveis.

11.6. Diretiva NIS2 da UE (2022/2555):

11.6.1. Artigo 21(2)(e, h): Exige processos seguros de desenvolvimento e teste de software, com ênfase na proteção contra acessos não autorizados e fugas de dados.

11.7. DORA da UE (2022/2554):

11.7.1. Artigo 9 – Sistemas e protocolos de TIC: Exige que os processos de teste suportem a resiliência e protejam os dados operacionais contra comprometimento ou divulgação não autorizada.

11.8. COBIT 2019:

11.8.1. DSS05 – Gerir Serviços de Segurança: Suporta a aplicação de políticas de segurança em todos os ambientes, incluindo os de não produção.

11.8.2. BAI07 – Gerir a Aceitação e Transição de Alterações: Abrange o processo formal de transição de teste para produção, incluindo controlos sobre dados e ambientes.