					Insira aqui a designação da entidade jurídica registada							
Número do documento: P40					Título do documento: **Política de Testes de Segurança e Red Teaming**							
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**

Alinhada com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
RGPD da UE	Art. 32(1)(d)	
Diretiva NIS2 da UE	Art. 21(2)(f)	
DORA da UE	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Finalidade

1 Definir um programa estruturado para a realização regular de testes de segurança às redes, sistemas e aplicações da organização, incluindo avaliações de vulnerabilidades, testes de intrusão e exercícios de red teaming, de modo a cumprir os requisitos do artigo 21.º, n.º 2, alínea f), da Diretiva NIS2 da UE relativos à avaliação da eficácia das medidas de cibersegurança.

1.1 Assegurar que as fragilidades nas medidas técnicas e organizativas são identificadas e corrigidas proativamente através de testes controlados, promovendo a melhoria contínua da postura de segurança da organização.

2. Âmbito

2 Esta política abrange todos os sistemas de informação críticos, aplicações e infraestruturas de suporte detidos ou operados pela organização. Inclui igualmente testes de segurança física das instalações, quando relevantes para a cibersegurança (por exemplo, engenharia social ou testes de intrusão física, quando incluídos no âmbito de exercícios de red teaming).

2.1 A política aplica-se às equipas internas de segurança, a quaisquer entidades externas contratadas para a realização de testes de segurança e aos respetivos Proprietários de Sistemas e Aplicações. Todas as atividades de teste devem ser autorizadas e seguir os procedimentos aqui definidos, de modo a evitar perturbações não intencionais.

3. Objetivos

3 Verificar a eficácia dos controlos de cibersegurança implementados (técnicos, operacionais e organizativos) através de testes e simulações periódicos, em conformidade com a exigência da Diretiva NIS2 da UE de medição da eficácia.

3.1 Identificar vulnerabilidades ou lacunas que os processos operacionais regulares possam não detetar, incluindo vulnerabilidades zero-day ou problemas de configuração, em cenários de ataque realistas (red teaming), antes de serem explorados por agentes de ameaça.

3.2 Fornecer à gestão garantia sobre a eficácia dos controlos e recomendações acionáveis através do reporte das constatações dos testes, permitindo decisões informadas de tratamento de riscos e a melhoria contínua do programa de segurança.

4. Papéis e responsabilidades

4 Coordenador de Testes de Segurança (STC): Designado pelo Diretor de Segurança da Informação, é responsável pelo planeamento e pela supervisão de todas as atividades de testes de segurança.

Assegura que os testes têm âmbito definido, estão devidamente autorizados e que os resultados são reportados e objeto de acompanhamento.

4.1 Equipa Interna de Segurança (Blue Team): Colabora nos testes (por exemplo, fornecendo informação para a definição do âmbito e monitorizando os sistemas durante os testes). Nos exercícios de red teaming, a Blue Team responde a ataques simulados, sendo a sua capacidade de deteção e resposta avaliada.

4.2 Red Team / Testadores de intrusão: Pode tratar-se de uma equipa interna de segurança ofensiva ou de consultores externos. Executam os testes de acordo com as regras de atuação acordadas, documentam todas as vulnerabilidades identificadas e os vetores de exploração e mantêm a confidencialidade.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Monitorização e auditoria

9 O STC deve manter um calendário e um registo de todas as atividades de testes de segurança realizadas. Esse registo deve incluir a data, o âmbito, quem executou o teste e um resumo dos resultados. Deve ser revisto para assegurar o cumprimento do calendário exigido (por exemplo, que nenhum sistema crítico fique sem testes para além do ciclo anual).

9.1 O progresso da remediação das constatações dos testes deve ser monitorizado e reportado mensalmente. Os problemas pendentes de elevada severidade devem ser revistos em reuniões de gestão até ao respetivo encerramento.

9.2 A Auditoria Interna ou um auditor independente deve rever anualmente o programa de testes de segurança para verificar que os testes são devidamente autorizados, executados e reportados, que as constatações críticas foram tratadas e que o programa cumpre as expectativas regulamentares (por exemplo, os auditores podem verificar que foi realizado um teste de intrusão antes do lançamento de um novo serviço online, quando exigido). Quaisquer desvios devem dar origem a planos de ação corretiva.

10. Revisão e manutenção

10 Esta política e o plano global de testes devem ser revistos pelo menos uma vez por ano. A revisão deve ter em conta alterações no panorama de ameaças (por exemplo, o surgimento de novas técnicas de ataque que os testes atuais possam não abranger) e adaptar os âmbitos ou as frequências em conformidade.

10.1 Após qualquer incidente de cibersegurança ou violação de maior impacto, esta política deve ser revista para determinar se testes adicionais ou mais frequentes poderiam ter prevenido ou detetado o problema. A política deve então ser atualizada para incorporar esses ajustamentos (por exemplo, acrescentando um novo cenário aos exercícios de red teaming com base em padrões de ataque observados).

10.2 As atualizações a esta política devem ser aprovadas pelo Diretor de Segurança da Informação e registadas pelo Conselho de Administração. Todo o pessoal relevante deve ser informado das alterações, e os parceiros externos de testes devem ser notificados se alguma alteração afetar os termos da sua colaboração.

11. Políticas relacionadas e ligações

11.1 P06 – Política de Gestão de Riscos. Os resultados dos testes suportam a avaliação e o tratamento do risco.

11.2 P22 – Política de Registo de Logs e Monitorização. Valida a cobertura de deteção durante os exercícios.

11.3 P24 – Política de Desenvolvimento Seguro. Integra as constatações dos testes nos controlos do SDLC.

11.4 P25 – Política de Requisitos de Segurança das Aplicações. Assegura que os requisitos refletem os ensinamentos retirados dos testes.

11.5 P30 – Política de Resposta a Incidentes. Os cenários de red teaming refinam os playbooks e a resposta.

11.6 P31 – Política de Recolha de Evidência e Análise Forense. Recolhe artefactos durante os testes de forma segura.

11.7 P32 – Política de Continuidade de Negócio e Recuperação de Desastre. Os exercícios verificam a resiliência sob ataque.

11.8 P33 – Política de Auditoria e Monitorização da Conformidade. Assegura a supervisão independente da eficácia do programa de testes.

12. Referências

12.1 Diretiva NIS2 (UE 2022/2555), artigo 21.º, n.º 2, alínea f) (políticas e procedimentos para avaliar a eficácia das medidas de gestão do risco de cibersegurança)

12.2 Regulamento de Execução da Comissão (UE) 2024/2690, Anexo, Secção 7 (requisitos para monitorizar, testar e avaliar a eficácia das medidas de cibersegurança)

12.3 Orientação Técnica da ENISA (2025) – Anexo sobre testes de segurança e auditoria (orientações sobre a realização de exercícios de cibersegurança e testes técnicos)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Melhores práticas da indústria: OWASP Testing Guide, NIST SP 800-115 (guia técnico para testes de segurança), CBEST/GREEN Team (referenciais de red teaming do setor financeiro para referência)