					Inserire qui la denominazione dell'entità giuridica registrata							
Numero del documento: P40					Titolo del documento: **Politica di sicurezza per i test di sicurezza e le esercitazioni di red teaming**							
Versione: 1.0		Data di entrata in vigore: 01.01.2025			Proprietario del documento:							
X	Politica		Standard		Procedura		Modulo		Registro		Altro	

Cronologia delle revisioni				
Numero di revisione	**Data di revisione**	**Modifiche**	**Riesaminato da**	**Proprietario del processo**

Approvazioni			
Nome	**Ruolo**	**Data**	**Firma**

Nota legale (diritti d'autore e limitazioni d'uso)

(C) 2025 Clarysec LLC. All rights reserved.

Il presente documento è proprietà intellettuale di Clarysec LLC. Nessuna parte del presente documento può essere copiata, riutilizzata, distribuita o modificata per finalità commerciali o di implementazione senza previa autorizzazione scritta espressa.

L'uso non autorizzato è severamente vietato e può comportare azioni legali.

Per richieste di licenza, contattare: info@clarysec.com

Allineamento a standard e normative applicabili

Standard/Regolamento	Clausola/Articolo	Commento
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	
GDPR UE	Art. 32(1)(d)	
NIS2 UE	Art. 21(2)(f)	
DORA UE	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Finalità

1 Definire un programma strutturato per i test periodici di sicurezza di reti, sistemi e applicazioni dell'organizzazione, comprese le valutazioni delle vulnerabilità, i test di penetrazione e le esercitazioni di red teaming, al fine di soddisfare i requisiti dell'articolo 21(2)(f) della NIS2 in materia di valutazione dell'efficacia delle misure di cibersicurezza.

1.1 Garantire che le debolezze delle misure tecniche e organizzative siano individuate e corrette in modo proattivo mediante test controllati, migliorando continuamente il livello di sicurezza dell'organizzazione.

2. Ambito di applicazione

2 La presente politica si applica a tutti i sistemi informativi critici, alle applicazioni e all'infrastruttura di supporto di proprietà dell'organizzazione o da essa gestiti. Include inoltre i test di sicurezza fisica delle strutture, ove rilevanti ai fini della cibersicurezza, ad esempio esercitazioni di ingegneria sociale o test di intrusione fisica, se inclusi nell'ambito delle attività di red teaming.

2.1 La politica si applica ai team di sicurezza interni, alle eventuali società esterne incaricate dei test di sicurezza e ai pertinenti proprietari di sistemi e applicazioni. Tutte le attività di test devono essere autorizzate e svolte secondo le procedure qui definite, al fine di evitare interruzioni non intenzionali.

3. Obiettivi

3 Verificare l'efficacia dei controlli di cibersicurezza implementati, tecnici, operativi e organizzativi, mediante test periodici e simulazioni, in linea con quanto previsto dalla NIS2 in merito alla misurazione dell'efficacia.

3.1 Individuare vulnerabilità o lacune che i normali processi operativi potrebbero non rilevare, comprese vulnerabilità zero-day o problemi di configurazione, in scenari di attacco realistici di red teaming, prima che possano essere sfruttati da attori della minaccia.

3.2 Fornire alla direzione assurance e raccomandazioni attuabili attraverso la rendicontazione delle risultanze dei test, consentendo decisioni informate sul trattamento del rischio e il miglioramento continuo del programma di sicurezza.

4. Ruoli e responsabilità

4 Coordinatore dei test di sicurezza (STC): nominato dal Responsabile della sicurezza delle informazioni (CISO), è responsabile della pianificazione e della supervisione di tutte le attività di

test di sicurezza. Garantisce che i test siano correttamente perimetrati, autorizzati e che i risultati siano rendicontati e seguiti dalle conseguenti azioni.

4.1 Team di sicurezza interno (Blue Team): collabora alle attività di test, ad esempio fornendo informazioni per la definizione dell'ambito e monitorando i sistemi durante i test. Nelle esercitazioni di red teaming, il Blue Team risponde agli attacchi simulati e ne vengono valutate le capacità di rilevazione e risposta.

4.2 Red Team / Penetration Tester: possono essere un team interno di sicurezza offensiva o consulenti esterni. Eseguono i test secondo regole di ingaggio concordate, documentano tutte le vulnerabilità individuate e i percorsi di sfruttamento e mantengono la riservatezza.

[... Le sezioni 4.3–8 non sono incluse in questa anteprima. Acquistare il documento completo per accedere all'intero contenuto. ...]

9. Monitoraggio e audit

9 Lo STC deve mantenere un calendario e un registro di tutte le attività di test di sicurezza svolte. Tale registro deve includere la data, l'ambito, chi ha eseguito il test e una sintesi dei risultati. Esso deve essere riesaminato per garantire il rispetto della pianificazione richiesta, ad esempio che nessun sistema critico resti privo di test oltre il ciclo annuale.

9.1 L'avanzamento della risoluzione delle risultanze dei test deve essere monitorato e rendicontato mensilmente. Le problematiche aperte ad alta gravità devono essere riesaminate nelle riunioni direzionali fino alla loro chiusura.

9.2 La Funzione Internal Audit/Compliance o un auditor indipendente deve riesaminare annualmente il programma di test di sicurezza per verificare che: i test siano correttamente autorizzati, eseguiti e rendicontati; le risultanze critiche siano state affrontate; e il programma soddisfi le aspettative normative. Ad esempio, gli auditor possono verificare che un test di penetrazione sia stato eseguito prima dell'avvio di un nuovo servizio online, ove richiesto. Eventuali scostamenti devono dare luogo a piani di azione correttiva.

10. Riesame e manutenzione

10 La presente politica e il piano complessivo di test devono essere riesaminati almeno una volta all'anno. Il riesame deve tenere conto dei cambiamenti nel panorama delle minacce, ad esempio l'emergere di nuove tecniche di attacco non coperte dalle attività di test correnti, e adeguare di conseguenza l'ambito o la frequenza dei test.

10.1 A seguito di qualsiasi grave incidente di cibersicurezza o violazione, la presente politica deve essere riesaminata per stabilire se attività di test aggiuntive o più frequenti avrebbero potuto prevenire o rilevare il problema. La politica deve quindi essere aggiornata per recepire tali adeguamenti, ad esempio aggiungendo un nuovo scenario alle esercitazioni di red teaming sulla base dei modelli di attacco osservati.

10.2 Gli aggiornamenti alla presente politica devono essere approvati dal Responsabile della sicurezza delle informazioni (CISO) e portati all'attenzione del Consiglio di amministrazione. Tutto il personale pertinente deve essere informato delle modifiche e i partner esterni incaricati dei test devono essere informati se le modifiche incidono sulle condizioni del loro incarico.

11. Politiche correlate e collegamenti

11.1 P06 – Politica di gestione del rischio. Gli output dei test alimentano la valutazione e il trattamento del rischio.

11.2 P22 – Politica di registrazione e monitoraggio. Convalida la copertura di rilevazione durante le esercitazioni.

11.3 P24 – Politica di sviluppo sicuro. Integra le risultanze dei test nei controlli del ciclo di vita dello sviluppo del software (SDLC).

11.4 P25 – Politica sui requisiti di sicurezza delle applicazioni. Garantisce che i requisiti riflettano le lezioni apprese dai test.

11.5 P30 – Politica di risposta agli incidenti (P30). Gli scenari di red teaming affinano i playbook e la risposta.

11.6 P31 – Politica per la raccolta delle evidenze e l'analisi forense. Raccoglie artefatti durante i test in modo sicuro.

11.7 P32 – Politica di continuità operativa e disaster recovery. Le esercitazioni verificano la resilienza in caso di attacco.

11.8 P33 – Politica di audit e monitoraggio della conformità. Garantisce una supervisione indipendente dell'efficacia del programma di test.

12. Riferimenti

12.1 Direttiva NIS2 (UE 2022/2555), articolo 21(2), lettera (f) (politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi di cibersicurezza)

12.2 Regolamento di esecuzione della Commissione (UE) 2024/2690, allegato sezione 7 (requisiti per il monitoraggio, il test e la valutazione dell'efficacia delle misure di cibersicurezza)

12.3 Guida tecnica ENISA (2025) – allegato sui test di sicurezza e audit (linee guida per lo svolgimento di esercitazioni di cibersicurezza e test tecnici)

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

12.5 Best practice di settore: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (quadri di riferimento per attività di red teaming nel settore finanziario, a titolo di riferimento)