

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6058 di Lunedì 13 aprile 2026

ENISA: metodologia per esercitazioni di cybersicurezza

Guida operativa end-to-end per pianificare, eseguire e valutare esercitazioni di cybersicurezza, con indicazioni pratiche per simulare scenari di attacco, definire ruoli e responsabilità e migliorare la gestione dei rischi informatici.

Ormai da anni ENISA-European National information security agency- cerca di sensibilizzare gli utenti sui problemi della sicurezza informatica, mettendo spesso a disposizione preziosi strumenti sperimentali.

A febbraio 2026 ha messo a disposizione "**The ENISA Cybersecurity Exercise Methodology - End-to-end guide on how to plan, run and evaluate an exercise**", un documento che offre preziose indicazioni su come i responsabili della sicurezza informatica possono impostare degli esercizi, che permettano di ipotizzare scenari di attacco informatico e mitigare i rischi relativi.

Questa metodologia offre un quadro completo per la pianificazione, la gestione e la valutazione degli esercizi di sicurezza informatica. La metodologia garantisce che tutti i soggetti coinvolti siano correttamente informati ed assegna responsabilità ai vari ruoli. Questa metodologia è basata su materiale teorico, che è stato però sperimentato praticamente in numerose esercitazioni, con risultati oltremodo positivi.

Gli obiettivi di questo documento sono i seguenti:

- offrire indicazioni su come si deve organizzare e pianificare un esercizio di sicurezza informatica,
- valutare le capacità di risposta aziendale, a fronte di attacchi informatici,
- convincere l'alta direzione sull'importanza dell'organizzazione di esercizi di sicurezza informatica,
- valutare le competenze e le capacità dell'azienda a fronte di attacchi informatici, rispettando i requisiti legali e regolamentari applicabili.

Pubblicità

Un notevole pregio di questo documento è che la sua metodologia è stata sviluppata in conformità alle normative ISO 22398-2013 ed ISO 22361-2022, garantendo pertanto una piena conformità alla regola d'arte.

Il documento si articola in varie parti, così suddivise:

- l'avvio della progettazione dell'esercizio,
- la progettazione dell'esercizio,
- la preparazione e la definizione dello scenario,
- le modalità di attuazione dell'esercizio previsto,

- la valutazione dell'accaduto, al termine dell'esercizio.

Il documento dà anche preziose indicazioni su come impostare la squadra di pronto intervento, a fronte di incidenti informatici, ed anche la squadra legale, che potrebbe essere coinvolta per fronteggiare possibili riflessi negativi, di natura non tecnologica.

[ENISA - The ENISA Cybersecurity Exercise Methodology - End-to-end guide on how to plan, run and evaluate an exercise.](#)

Adalberto Biasiotti



Licenza [Creative Commons](#)

www.puntosicuro.it