Phishing
AI POWERED PROTECTION

COMPLIANCE

NIS2 e DORA: la formazione sulla cybersecurity non è più facoltativa

Obblighi di legge, responsabilità del CDA e strategie pratiche per la compliance

A cura del team CENANT di GPI Cyberdefence

28 febbraio 2026 www.gpiphishing.com

COMPLIANCE

Obblighi di legge, responsabilità del CDA e strategie pratiche per la compliance

01 Il quadro normativo è cambiato

Con l'entrata in vigore di NIS2 (Direttiva UE 2022/2555) e DORA (Digital Operational Resilience Act, Regolamento UE 2022/2554), la sicurezza informatica ha smesso di essere esclusivamente una questione tecnica per diventare una responsabilità formale del vertice aziendale.

NIS2 si applica a un perimetro molto più ampio di organizzazioni rispetto alla precedente NIS1, includendo settori come energia, trasporti, sanità, infrastrutture digitali, servizi postali e manifatturiero avanzato. DORA si rivolge specificamente alle entità finanziarie, imponendo requisiti rigorosi di resilienza operativa digitale.

02 La responsabilità esplicita del management

NIS2 richiede esplicitamente che il management aziendale segua una formazione periodica sulla cybersecurity e promuova una cultura della sicurezza a tutti i livelli dell'organizzazione. Non è una raccomandazione: è un obbligo normativo.

Entrambe le normative introducono un principio chiave: i vertici aziendali, come CDA, CEO e direttori, non possono delegare integralmente la responsabilità della sicurezza all'IT. Devono essere coinvolti, informati e, in caso di violazioni, possono essere ritenuti personalmente responsabili.

03 La formazione come requisito, non come opzione

Uno dei punti centrali di entrambe le normative è la formazione strutturata del personale, non episodica, ma continua, documentata e verificabile. Questo include simulazioni di attacco, aggiornamento periodico sulle minacce emergenti, e la capacità di dimostrare numericamente il miglioramento nel tempo.

Per i CISO e i responsabili della sicurezza, questo si traduce in un'esigenza concreta: costruire programmi di awareness con indicatori oggettivi di performance (tasso di click su e-mail di phishing simulate, tempo di segnalazione degli incidenti, percentuale di dipendenti formati) che possano essere presentati al board e, in caso di audit, alle autorità competenti.

> *NIS2 prevede sanzioni fino a 10 milioni di euro o il 2% del fatturato globale per le violazioni più gravi. DORA introduce requisiti di test periodici di resilienza operativa.*

04 Una opportunità, non solo un vincolo

Le organizzazioni più lungimiranti non stanno affrontando NIS2 e DORA come un adempimento burocratico, ma come un'opportunità per strutturare programmi di sicurezza che generano valore reale: riduzione del rischio, maggiore fiducia da parte di clienti e partner, e competitività in settori dove la resilienza digitale è un requisito sempre più richiesto.

GPI PHISHING — CYBERSECURITY PLATFORM

Rendi la tua azienda conforme a NIS2 e DORA con la formazione giusta

Programmi certificati, reportistica per il CDA
e formazione continua su misura per il tuo settore.

Phishing
AI POWERED PROTECTION

www.gpiphishing.com