

Cosa dice davvero la NIS2 sulla formazione

La Direttiva NIS2 non considera la formazione una **buona pratica**,
ma parte integrante delle misure di gestione del rischio.

La sicurezza non è solo **tecnologia**:
le **persone** sono una componente critica della difesa.

Cosa dice davvero la NIS2 sulla formazione?

Directive



La Direttiva NIS2 (UE
2022/2555)

non tratta la formazione
come una “buona pratica”,

ma come parte integrante
delle misure di gestione del
rischio.

Articolo 21 – Misure di gestione dei rischi

IL MANAGEMENT DEVE:

- consapevolezza e formazione del **personale**
- riduzione del rischio **umano**
- capacità di prevenire, rilevare e rispondere agli **incidenti**

Senza formazione, le misure organizzative sono incomplete.

Articolo 20 – Responsabilità degli organi di gestione

IL MANAGEMENT DEVE:

- approvare le misure di **sicurezza**
- garantire che il **personale** sia formato
- essere in grado di **dimostrarlo**

Qui il punto è cruciale:
la responsabilità è diretta, non delegabile solo all'IT.

Per chi è obbligatoria la formazione

La formazione è obbligatoria per tutte le aziende soggette alla NIS2, quindi:

- Soggetti **essenziali**
- Soggetti **importanti**

nei settori:



Energia, trasporti, sanità, digitale, manifatturiero, acqua, PA, servizi IT, MSP, cloud, data center, ecc.

Non importa se sei “piccolo ma critico”: se rientri nel perimetro, la formazione è richiesta.

Chi deve essere formato (errore comune)

Altro errore frequente:
pensare che basti formare l'IT.

In realtà la NIS2 richiede formazione differenziata per:

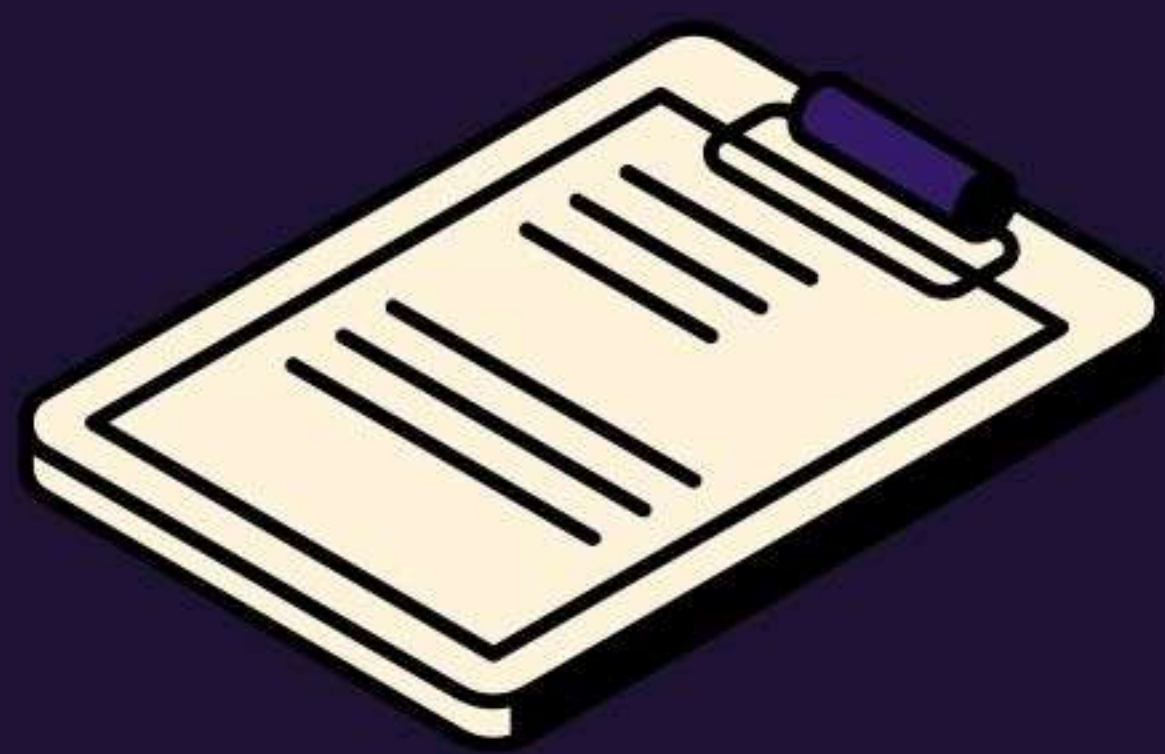
- **Dipendenti** → phishing, comportamenti, segnalazione incidenti
- **IT / SysAdmin / CSIRT** → logging, hardening, incident response, notifiche
- **Management** → responsabilità, governance, decisioni in crisi

Formare solo una categoria non è sufficiente.

Serve una prova? Sì.

Non basta “aver fatto un corso”.
In caso di:

- audit
- incidente
- ispezione ACN



devi poter **dimostrare:**

- chi è stato formato..
- su cosa
- quando
- con quale verifica (quiz, attestato)



Attestati, registri e contenuti
formativi sono evidenze di
compliance.

Cosa succede se non formi il personale

LA MANCATA FORMAZIONE PUÒ ESSERE VISTA COME:

- inadeguata gestione del rischio
- violazione dell'art. 21
- responsabilità del management

CON POSSIBILI:

- sanzioni amministrative
- rilievi gravi in audit
- aggravanti in caso di incidente cyber

In sintesi :



Sì, la formazione è obbligatoria



Non è facoltativa



Non basta una slide o una mail interna



Non riguarda solo l'IT



Deve essere strutturata, documentata e verificabile