

CORSI DI FORMAZIONE NIS2

Governance, consapevolezza e prove per una formazione NIS2 strutturata.



enterprise



Cosa dice davvero la NIS2 sulla formazione

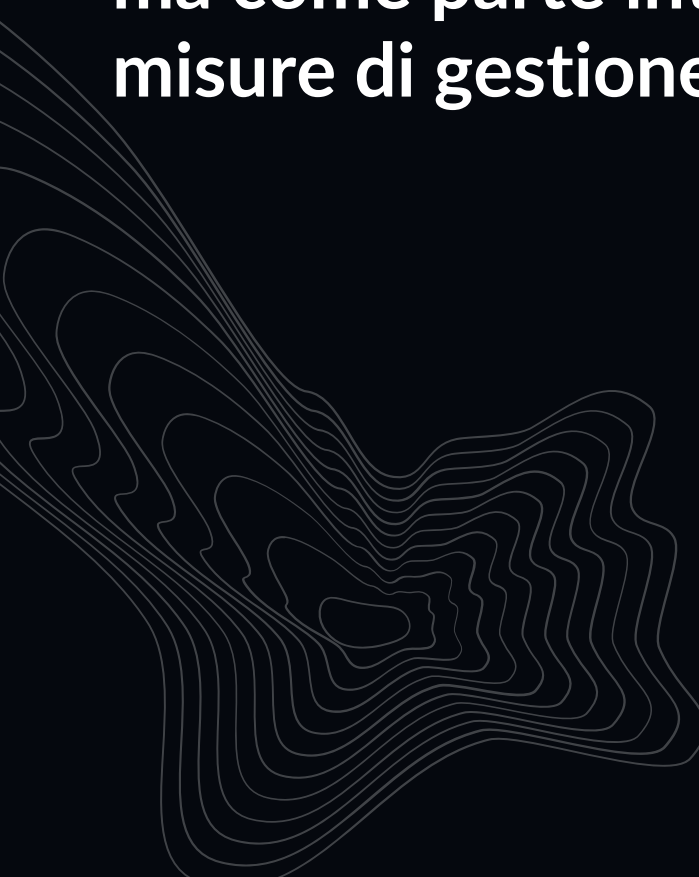
La Direttiva NIS2 non considera la formazione una buona pratica, ma parte integrante delle misure di gestione del rischio.

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

Cosa dice davvero la NIS2 sulla formazione?

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:

01

02

03

consapevolezza e
formazione del
personale

riduzione del
rischio umano

capacità di
prevenire, rilevare
e rispondere agli
incidenti

**Senza formazione, le
misure organizzative sono
incomplete.**

RISK MANAGEMENT / PEOPLE

Articolo 20 – Responsabilità degli organi di gestione

IL MANAGEMENT DEVE:

01

approvare le misure di
sicurezza

02

promuovere periodicamente
la formazione del personale

03

essere in grado di
dimostrarlo

RESPONSABILITÀ DIRETTA

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

Per chi è obbligatoria la formazione

La formazione rientra nelle misure di gestione del rischio previste per i soggetti NIS2, quindi:

Soggetti essenziali

Soggetti importanti

nei settori:

01 Energia

02 trasporti

03 sanità

04 digitale

05 manifatturiero

06 acqua

07 PA

08 servizi IT

09 MSP

10 cloud

11 data center

12 ecc.

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

Chi deve essere formato

PERSONE

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

La formazione deve essere adeguata a ruoli e responsabilità

(errore comune)

-
- 01** Dipendenti → phishing, comportamenti, segnalazione incidenti

 - 02** IT / SysAdmin / CSIRT → logging, hardening, incident response, notifiche

 - 03** 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:

IN CASO DI:

- 01 audit
- 02 incidente
- 03 ispezione ACN

devi poter dimostrare:

- 01 chi è stato formato
- 02 su cosa
- 03 quando
- 04 le modalità di verifica adottate

Attestati, registri e contenuti formativi sono evidenze di compliance.

Cosa succede se non formi il personale

LA MANCATA FORMAZIONE PUÒ ESSERE VISTA COME:

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

CON POSSIBILI:

01

sanzioni
amministrative

02

rilievi gravi
in audit

03

possibile rilievo 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**
