

A che punto è la tua azienda con NIS2?

Quindici domande per un'autovalutazione rapida. Non sostituiscono un'analisi formale, ma ti indicano dove guardare per primo.

Perimetro e registrazione

- 01 Hai verificato se la tua azienda rientra nel perimetro NIS2 per settore e dimensione, o se ne riceve comunque i requisiti come fornitore di soggetti NIS2? ☐ Sì ☐ In parte ☐ No
- 02 Se sei nel perimetro, la registrazione sulla piattaforma dell'ACN è completa e aggiornata ogni anno, con un punto di contatto designato? ☐ Sì ☐ In parte ☐ No

Governance

- 03 Gli organi di amministrazione hanno approvato le misure di sicurezza e ne supervisionano l'attuazione? ☐ Sì ☐ In parte ☐ No
- 04 I vertici aziendali hanno seguito una formazione sulla gestione dei rischi informatici? ☐ Sì ☐ In parte ☐ No
- 05 Ruoli e responsabilità per la sicurezza informatica sono assegnati e documentati? ☐ Sì ☐ In parte ☐ No

Rischi e misure di sicurezza

- 06 Esiste un'analisi dei rischi documentata e aggiornata, basata su un inventario di sistemi, dati e servizi? ☐ Sì ☐ In parte ☐ No
- 07 L'autenticazione a più fattori è attiva su posta elettronica, accessi remoti e account amministrativi? ☐ Sì ☐ In parte ☐ No
- 08 I backup sono isolati dalla rete principale e il ripristino viene provato con regolarità? ☐ Sì ☐ In parte ☐ No
- 09 Vulnerabilità e aggiornamenti di sicurezza sono gestiti con un processo e tempi definiti? ☐ Sì ☐ In parte ☐ No
- 10 Esiste un piano di continuità operativa e di gestione delle crisi? ☐ Sì ☐ In parte ☐ No
- 11 Tutto il personale riceve una formazione periodica di igiene informatica? ☐ Sì ☐ In parte ☐ No

Catena di fornitura

- 12 I fornitori critici sono individuati e valutati, con requisiti di sicurezza inseriti nei contratti? ☐ Sì ☐ In parte ☐ No

Incidenti

- 13 Esiste una procedura di gestione degli incidenti con ruoli, criteri di gravità e contatti? ☐ Sì ☐ In parte ☐ No
- 14 Sapresti notificare un incidente significativo al CSIRT Italia nei tempi previsti: pre-notifica entro 24 ore, notifica entro 72 ore, relazione finale entro un mese? ☐ Sì ☐ In parte ☐ No

Verifica

- 15 L'efficacia delle misure viene verificata periodicamente con audit, test o esercitazioni? ☐ Sì ☐ In parte ☐ No

Punteggio

SÌ = 2 • IN PARTE = 1 • NO
= 0 • MASSIMO 30

24-30 • Buona base Le fondamenta ci sono. Verifica che ogni risposta sia supportata da evidenze documentate e mantieni il sistema aggiornato.

12-23 • Lavori in corso Ci sono lacune su punti richiesti dalla normativa. Convienne un piano con priorità chiare, partendo da governance e gestione degli incidenti.

0-11 • Da impostare Il rischio di non conformità è alto. Parti dal perimetro, dalla governance e dall'analisi dei rischi: sono la base di tutto il resto.