

AUTOVALUTAZIONE PER PMI

18 punti per capire a che punto siete.

Sono le domande che vi verranno fatte in caso di verifica, o da un cliente che deve mettere in sicurezza la propria catena di fornitura. Se a qualcuna non sapete rispondere, quella è la vostra prossima attività.

Capire se vi riguarda

- 01 Avete verificato sul portale ACN se la vostra impresa è in elenco fra i soggetti essenziali o importanti.
- 02 Sapete in quale settore fra quelli previsti dalla norma ricade la vostra attività.
- 03 Avete controllato se un vostro cliente vi ha già inserito fra i fornitori rilevanti per la sua conformità.
- 04 Se non siete soggetti, lo avete messo per iscritto con la data della verifica: serve se un cliente ve lo chiede.

Governo e responsabilità

- 05 Esiste una persona formalmente incaricata della sicurezza delle informazioni, indicata per nome.
- 06 L'organo dirigente ha ricevuto una formazione sulla cybersicurezza documentata.
- 07 Esiste una politica di gestione del rischio approvata e con una data di revisione.
- 08 I rischi principali sono censiti in un registro, non solo nella testa di qualcuno.

Misure tecniche minime

- 09 I backup sono automatici, conservati anche fuori sede e il ripristino è stato provato almeno una volta.
- 10 L'accesso ai sistemi critici richiede autenticazione a più fattori.
- 11 Gli aggiornamenti di sicurezza sono applicati secondo una procedura, non quando capita.
- 12 Esiste un inventario aggiornato di sistemi, applicativi e accessi.
- 13 I log dei sistemi principali sono raccolti e conservati per un periodo definito.

Incidenti e continuità

- 14 Esiste una procedura scritta che dice chi fa cosa nelle prime 24 ore da un incidente.
- 15 Sapete come e dove si notifica un incidente significativo al CSIRT Italia.
- 16 Esiste un piano di continuità che indica quali servizi vanno ripristinati per primi e in quanto tempo.

Fornitori

- 17 Avete l'elenco dei fornitori ICT che trattano dati o accedono ai vostri sistemi.
- 18 I contratti con quei fornitori contengono obblighi di sicurezza e di notifica degli incidenti.

Nota. Riferimenti: D.Lgs. 138/2024 e determinazioni dell'Agenzia per la Cybersicurezza Nazionale. Questa checklist è uno strumento di autovalutazione: non sostituisce una verifica di conformità né un parere legale, e il perimetro va confermato caso per caso. La scadenza del 31 ottobre 2026 riguarda i soggetti già in elenco; chi vi è entrato nel 2026 ha tempo fino al 31 luglio 2027.