Checklist di Conformità NIS2

Piccole e medie organizzazioni — 16 punti essenziali

AMBITO DI APPLICAZIONE

- [ ] Verificate se il vostro settore rientra tra i 18 settori coperti dalla NIS2 (sanità, infrastrutture digitali, produzione di dispositivi medici…).
- [ ] Determinate la vostra categoria — soggetto essenziale o importante. Di norma: 50 dipendenti o 10 M€ di fatturato, ma realtà più piccole rientrano se il servizio è critico.
- [ ] Registrate la vostra organizzazione presso l'ACN — in Italia la NIS2 è recepita con il D.lgs. 138/2024.

GOVERNANCE

- [ ] Nominate un responsabile della sicurezza delle informazioni — la direzione resta giuridicamente responsabile.
- [ ] Formate i vertici aziendali sulla gestione del rischio cyber: la NIS2 lo richiede espressamente.
- [ ] Redigete e approvate una politica di sicurezza delle informazioni.

MISURE TECNICHE

- [ ] Effettuate un'analisi dei rischi e tenetela aggiornata — è la base di tutta la conformità.
- [ ] Attivate l'autenticazione a più fattori (MFA) su e-mail, accessi remoti e sistemi critici.
- [ ] Cifrate i dati sensibili, a riposo e in transito.
- [ ] Predisponete backup regolari, offline, e testatene il ripristino.
- [ ] Applicate le patch di sicurezza con un processo documentato.

INCIDENTI E CONTINUITÀ

- [ ] Preparate la procedura di notifica: preallarme entro 24 ore, notifica entro 72 ore, relazione finale entro un mese.
- [ ] Individuate i vostri referenti ACN / CSIRT Italia — prima dell'incidente, non durante.
- [ ] Predisponete un piano di continuità operativa e testatelo almeno una volta l'anno.

FORNITORI

- [ ] Valutate la sicurezza dei fornitori critici: hosting, servizi gestiti, software.
- [ ] Inserite clausole di cybersicurezza nei contratti.

> **Sanzioni NIS2: fino a 10 M€ o al 2 % del fatturato mondiale per i soggetti essenziali (7 M€ / 1,4 % per quelli importanti).**

Serve aiuto con la conformità? Scriveteci — la prima conversazione è gratuita.

SECURENOMAD.AI · @SECURENOMAD.AI · #LIVINLAVIDASECURITY

Documento informativo di carattere generale — non costituisce consulenza legale.