CHECKLIST OPERATIVA

Checklist NIS2

Per enti pubblici e strutture sanitarie

PER CHI	TEMPO	AGGIORNATO
Direzione, responsabili IT e sicurezza, DPO	30–40 minuti	agosto 2026

La Direttiva UE 2022/2555, recepita in Italia con il D.lgs. 138/2024, amplia sensibilmente la platea dei soggetti obbligati. Il settore sanitario e la pubblica amministrazione vi rientrano ampiamente.

La differenza rispetto al passato non è solo tecnica: la NIS2 attribuisce responsabilità dirette agli **organi direttivi**, che devono approvare le misure e vigilare sulla loro attuazione.

01 Siete nell’ambito di applicazione?

Verificate la vostra posizione. In caso di dubbio sulla classificazione, la valutazione va documentata.

- [ ] Siamo un’azienda sanitaria, un’azienda ospedaliera, un IRCCS o una casa di cura
- [ ] Siamo una pubblica amministrazione centrale o locale rientrante nel perimetro
- [ ] Produciamo dispositivi medici o diagnostici in vitro
- [ ] Forniamo servizi digitali o infrastrutturali a soggetti dei punti precedenti
- [ ] Abbiamo verificato se siamo qualificati come soggetto **essenziale** o **importante**

> La distinzione tra soggetti essenziali e importanti incide sul regime di vigilanza e sull’entità delle sanzioni. Verificate la classificazione sui canali ufficiali ACN.

02 Registrazione e adempimenti formali

- [ ] Ci siamo registrati sulla piattaforma ACN entro la finestra prevista
- [ ] Abbiamo designato il punto di contatto e comunicato i riferimenti
- [ ] Manteniamo aggiornati i dati dichiarati (variazioni societarie, contatti, servizi)
- [ ] Abbiamo verificato le scadenze di adeguamento applicabili alla nostra categoria

> Le finestre di registrazione e le scadenze di adeguamento sono definite da ACN e possono variare di anno in anno: verificatele sul sito ufficiale, non su fonti secondarie.

03 Le misure minime di sicurezza

L'articolo 21 individua le categorie di misure che ogni soggetto deve adottare, proporzionate al rischio. Spuntate quelle documentate e attuate, non quelle solo previste.

- [ ] Analisi dei rischi e politica di sicurezza dei sistemi informativi
- [ ] Gestione degli incidenti: rilevazione, risposta, ripristino
- [ ] Continuità operativa: backup, disaster recovery, gestione della crisi
- [ ] Sicurezza della catena di approvvigionamento, inclusi i fornitori diretti
- [ ] Sicurezza nell'acquisizione, sviluppo e manutenzione dei sistemi, con gestione delle vulnerabilità
- [ ] Procedure per valutare l'efficacia delle misure adottate
- [ ] Igiene informatica di base e formazione periodica del personale
- [ ] Politiche in materia di crittografia e, ove opportuno, cifratura
- [ ] Sicurezza del personale, controllo degli accessi, gestione degli asset
- [ ] Autenticazione a più fattori, comunicazioni sicure, comunicazioni di emergenza

04 Notifica degli incidenti: i tre tempi

È l'adempimento che mette più in difficoltà, perché i tempi sono stretti e scattano anche di notte e nei festivi. Verificate di avere una procedura che regga in condizioni reali.

- [ ] Esiste una procedura scritta che indica chi decide se un incidente è significativo
- [ ] La catena di reperibilità copre notti, festivi e periodi di ferie
- [ ] Chi risponde sa dove trovare le credenziali della piattaforma di notifica
- [ ] La procedura è stata provata almeno una volta con una simulazione

ENTRO	COSA	PRONTO?
24 ore	Pre-notifica: segnalazione iniziale dell'incidente significativo	☐
72 ore	Notifica: valutazione iniziale, gravità, impatto, indicatori di compromissione	☐
1 mese	Relazione finale: descrizione dettagliata, cause, misure adottate	☐

> La domanda che smaschera le procedure di facciata: se l'incidente accade alle 23 di un sabato di agosto, chi lo qualifica come significativo e chi apre la pratica entro 24 ore?

05 Responsabilità degli organi direttivi

È la novità che cambia la natura dell'adempimento: non è più solo un tema IT.

- [ ] L'organo direttivo ha approvato formalmente le misure di gestione del rischio
- [ ] L'approvazione è tracciata in una delibera o in un verbale
- [ ] I componenti hanno seguito una formazione specifica in materia
- [ ] È previsto un flusso informativo periodico verso l'organo direttivo
- [ ] I ruoli e le responsabilità sono assegnati per iscritto

06 Catena di fornitura

Il punto più oneroso per sanità e PA, dove i fornitori sono numerosi e stratificati nel tempo.

- ☐ Abbiamo un elenco dei fornitori che accedono a sistemi o dati critici
- ☐ I contratti prevedono obblighi di sicurezza e di notifica degli incidenti
- ☐ Valutiamo la sicurezza dei fornitori prima dell’affidamento
- ☐ Sappiamo quali fornitori sono a loro volta soggetti NIS2

Come leggere il risultato

Sezione 01 o 02 incompleta	Priorità assoluta: gli adempimenti formali hanno scadenze perentorie.
Sezione 03 sotto il 70%	Serve un piano di adeguamento con priorità e responsabilità assegnate.
Sezione 04 incompleta	È il rischio più concreto: un incidente reale non aspetta che la procedura sia pronta.
Sezione 05 incompleta	Espone direttamente l’organo direttivo. Da sanare per primo, costa poco.

Aggiornato a agosto 2026 · inteGroup — Integroup S.r.l., Via Ippolito Nievo 11, 20145 Milano · dpo@integroup.eu · integroup.eu