

Seconda fase ACN

Scadenze, priorità e azioni da pianificare da oggi al 2026

DA GENNAIO 2026 – Notifica incidenti significativi

Necessario implementare un sistema automatizzato per la rilevazione, classificazione e notifica tempestiva degli incidenti di sicurezza.

ENTRO APRILE 2026 – Categorizzazione servizi critici

Applicare il modello ACN per classificare asset e processi secondo la loro criticità. Fondamentale mappare sistemi, applicazioni e dipendenze.

ENTRO APRILE 2026 – Adozione obblighi a lungo termine

Oltre alle misure minime, occorre strutturare una strategia di cybersecurity sostenibile e governance continua.

ENTRO OTTOBRE 2026 – Implementazione misure minime

Dimostrare l'adozione di MFA, EDR, backup affidabili, logging, gestione patch e altri strumenti essenziali.

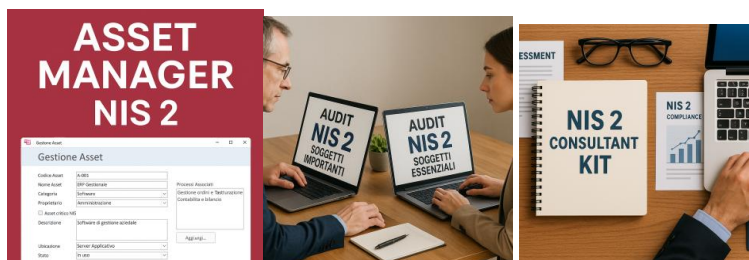
Checklist sintetica delle azioni da pianificare

Obbligo Normativo	Azione da Pianificare	Scadenza	Soluzioni Consigliate
Notifica degli incidenti	Sistema di rilevamento e notifica	Gennaio 2026	Kit Audit NIS 2
Categorizzazione servizi critici	Mappatura asset e dipendenze	Aprile 2026	Asset Manager NIS 2
Obblighi a lungo termine	Strategia di sicurezza e governance	Aprile 2026	Kit documentazione NIS 2 Kit Audit NIS 2
Misure di sicurezza di base	Implementazione strumenti tecnici	Ottobre 2026	Kit documentazione NIS 2 Kit Audit NIS 2

Azioni consigliate per prepararsi alla seconda fase attuativa dell'ACN:

- **Analizzare il punto di partenza.** È essenziale comprendere quali aree dell'organizzazione risultano più esposte. Un Security Assessment consente di valutare policy, configurazioni e vulnerabilità presenti, fornendo una base solida per la pianificazione.
- **Mappare infrastrutture e rischi.** Occorre realizzare una mappatura dettagliata degli asset, dei sistemi critici, dei flussi informativi e delle dipendenze, interne ed esterne, per identificare le potenziali debolezze che potrebbero compromettere la sicurezza.
- **Attuare subito le misure di base.** Autenticazione multifattoriale (MFA), sistemi EDR, backup affidabili e logging centralizzato devono essere implementati senza ritardi: rappresentano i pilastri indispensabili di ogni strategia di cybersicurezza.

ACCEDI ALLA COLLANA EDITORIALE NIS 2



Kit Formazione NIS 2 per
Dipendenti – Corso Completo
con Slide e Test Finale