La Direttiva NIS2: Nuove regole per la cybersicurezza in Europa

La Direttiva NIS2 è entrata in vigore il 17 gennaio 2023. Rafforza significativamente la cybersicurezza nell'Unione Europea.

Coinvolge ben 18 settori critici. Rappresenta un importante passo avanti per la sicurezza digitale europea.

by FM CARTIERE SPA

A chi si applica la NIS2?

Soggetti Essenziali

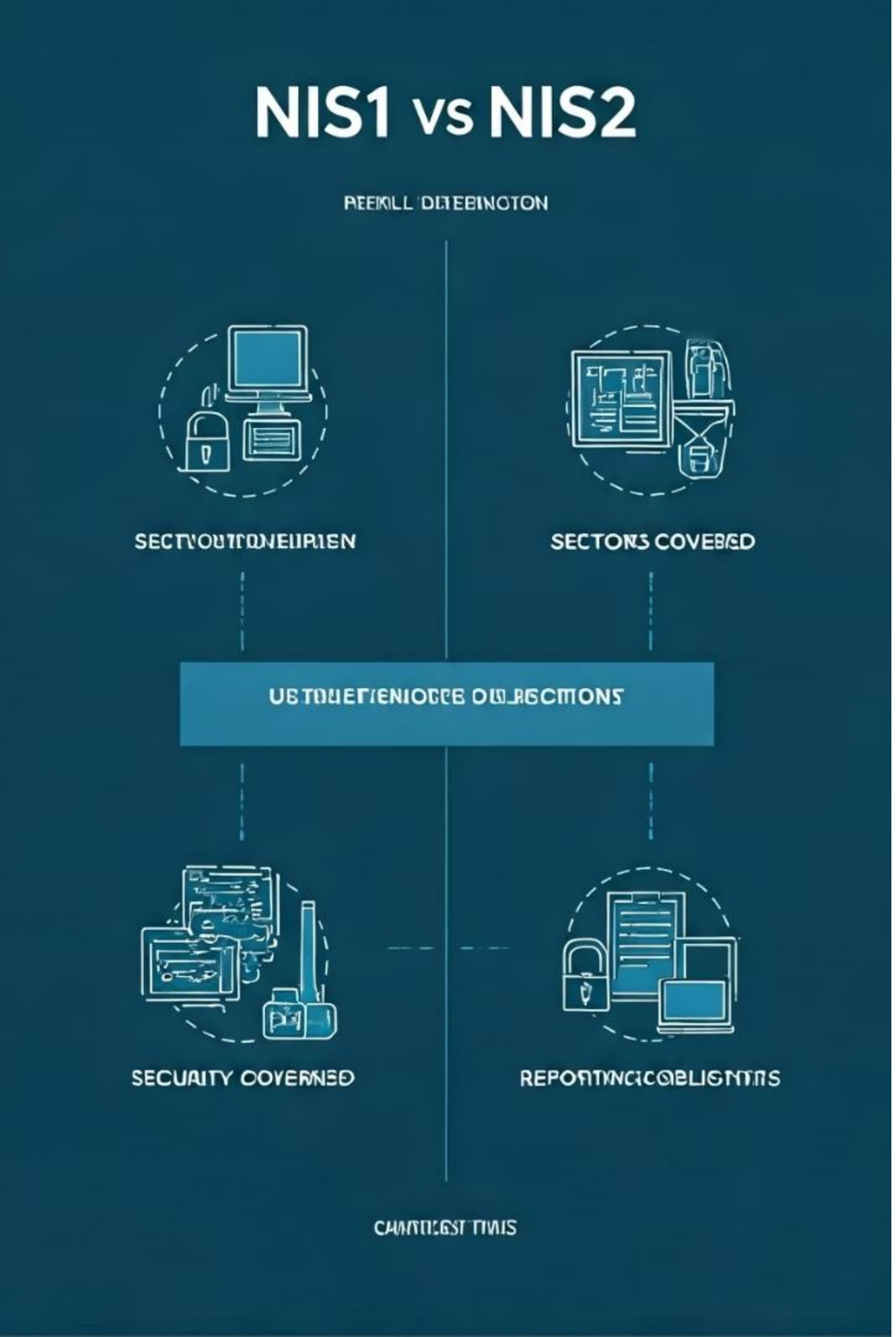
Operatori in settori strategici con impatto critico sulla sicurezza nazionale.

Soggetti Importanti

Organizzazioni con impatto significativo ma non critico sulla sicurezza nazionale.

Autoriconoscimento

Le aziende devono identificarsi e registrarsi autonomamente come soggetti coperti dalla direttiva.



Novità principali rispetto alla NIS1

Ambito ampliato

Maggiore copertura di soggetti e settori rispetto alla precedente normativa.

Analisi dei rischi

Adozione obbligatoria di processi strutturati di valutazione.

Misure contestuali

Sicurezza adeguata al contesto specifico dell'azienda.

Autocertificazione

Eliminata la designazione d'autorità, sostituita dall'autoidentificazione.

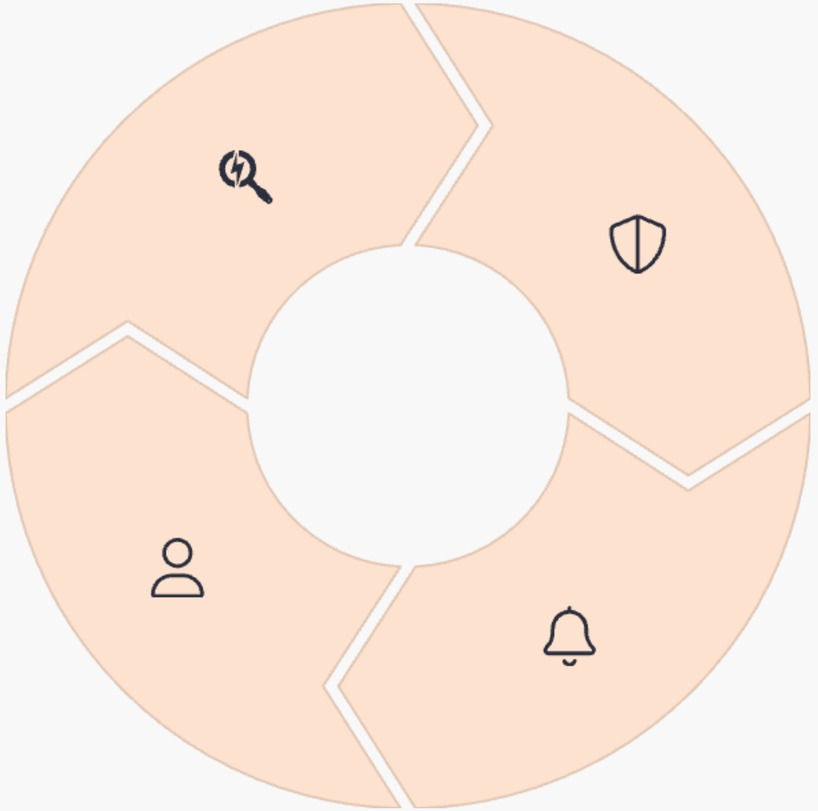
Obblighi per aziende e organizzazioni

Analisi rischi

Identificazione e valutazione sistematica delle minacce cyber.

Misure adeguate

Implementazione di controlli tecnici e organizzativi efficaci.



Formazione

Aggiornamento continuo delle competenze del personale.

Notifica incidenti

Comunicazione tempestiva degli eventi significativi alle autorità.

Tempistiche di recepimento in Italia

1. **Gennaio 2023**

   Entrata in vigore della Direttiva NIS2 nell'Unione Europea.

2. **2024**

   Recepimento con Decreto Legislativo 138 del 2024.

3. **Ottobre 2024**

   Scadenza per l'adeguamento normativo nazionale completo.

4. **Aprile 2025**

   Pubblicazione dell'elenco dei soggetti coinvolti.

5. **Gennaio 2026**

   Entrata in vigore dell'obbligo di notifica degli incidenti.

6. **Ottobre 2026**

   Completamento delle misure di sicurezza informatica di base.

7. **A partire da Aprile 2026**

   L'ACN attiverà diverse azioni di supporto e monitoraggio per le aziende

Il secondo set di obblighi prevede diverse fasi attuative con diktat scaglionati nel corso del 2026: la strategia dell'ACN, infatti, è quella di accompagnare step by step le imprese nel percorso di compliance, fornendo progressivamente tutti gli strumenti tecnici e normativi necessari per arrivare alla compliance.

Da **gennaio 2026**, entrerà ufficialmente in vigore l'obbligo di notifica degli incidenti significativi. Gli attacchi subiti devono essere segnalati tempestivamente alla autorità competenti, con l'adozione strutturata di un piano di risposta efficace che deve essere testato periodicamente per garantire sempre una gestione strutturata in caso di violazioni. Nello specifico, i soggetti importanti saranno obbligati a notificare:

- la perdita di riservatezza dei dati digitali, anche solo parziale;
- la perdita di integrità dei dati digitali, anche in questo caso anche qualora fosse solo parziale;
- la violazione dei livelli di servizio attesi.

Per quanto riguarda i soggetti essenziali, questi dovranno notificare anche l'accesso ai dati digitali non autorizzato o con abuso dei privilegi concessi.

Entro **aprile 2026**, sarà l'ACN ad avere in carico un compito di rilievo. Si dovrà definire, infatti, un **modello di categorizzazione delle attività e dei servizi** dei soggetti destinatari, con l'obiettivo di determinare gli specifici livello di rischio associati al settore di appartenenza, determinando di conseguenza gli obblighi in maniera proporzionata a seconda della criticità in essere. È in questo caso che verrà comunicato il **secondo set di obblighi**, questa volta a lungo termine. A differenza del primo set, si entrerà in merito relativamente a **piani di governance, risk management e auditing di sicurezza periodici**.

Attenzione alla scadenza di settembre 2026, entro la quale le aziende devono garantire la completa **implementazione** delle misure di sicurezza di base, applicate a tutti i sistemi informativi e di rete e con diverse modalità per soggetti essenziali o importanti. Nel rispetto del Framework Nazionale per la Cybersecurity e la Data Protection, sono 37 misure e 87 requisiti per soggetti categorizzati come importanti e 43 misure con 116 requisiti da soddisfare per i soggetti essenziali.

Una sfida di assoluta importanza in termini di governance aziendale per l'adeguamento degli organi di amministrazione e direttivi alle nuove responsabilità. È necessario quindi un cambiamento sostanziale nella cultura aziendale, soprattutto per quanto riguarda i cosiddetti **decision makers**.

Settori coperti dalla NIS2

Energia

Elettricità, gas, petrolio

Sanità

Ospedali, laboratori, farmacie

Trasporti

Aereo, ferroviario, marittimo, stradale

Banche

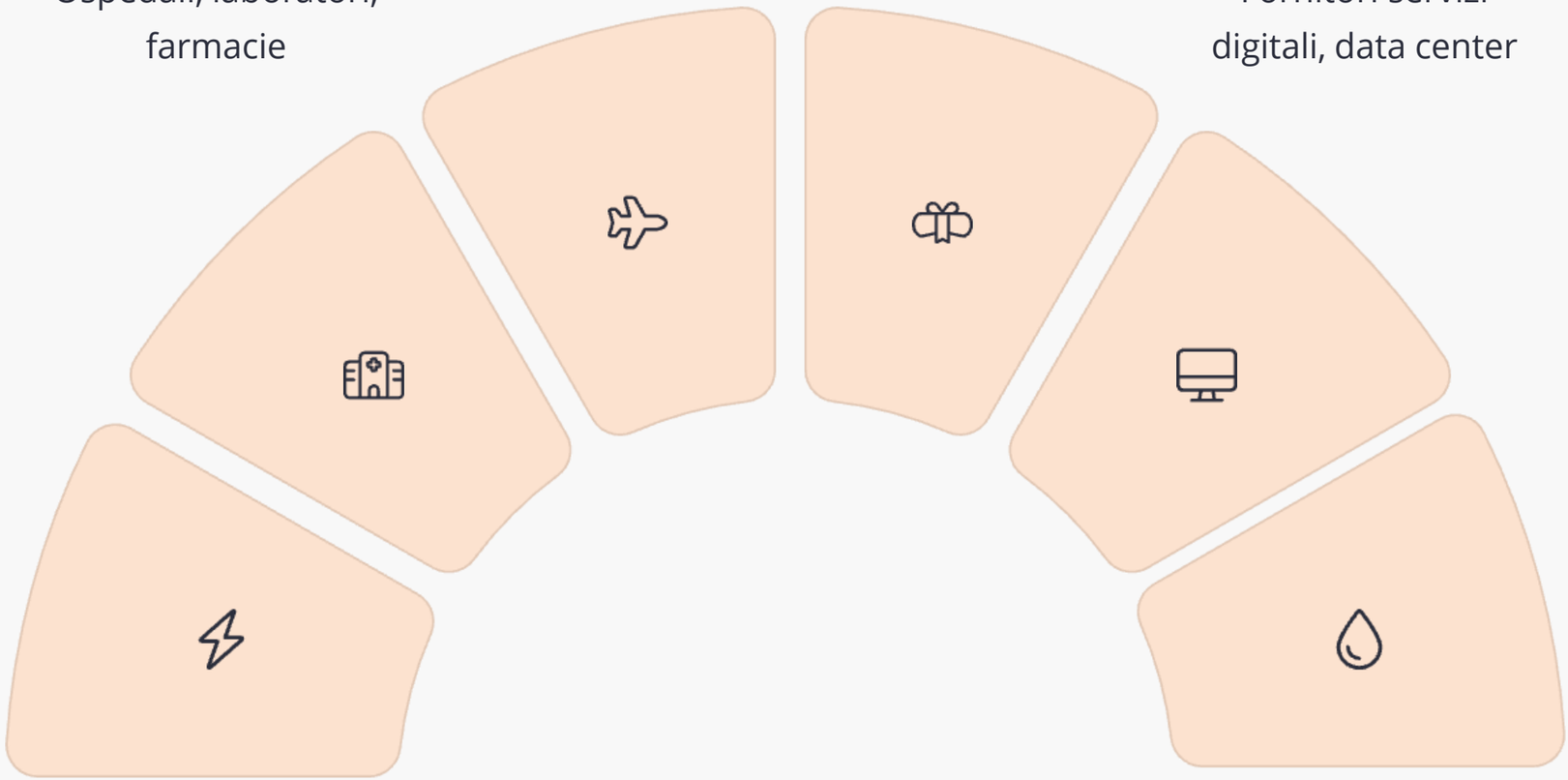
Istituti finanziari, assicurazioni

Digital

Fornitori servizi digitali, data center

Acqua

Fornitura e distribuzione



Sanzioni e controlli previsti

10M€

Sanzione massima per soggetti essenziali

O fino al 2% del fatturato globale annuo

7M€

Sanzione massima per soggetti importanti

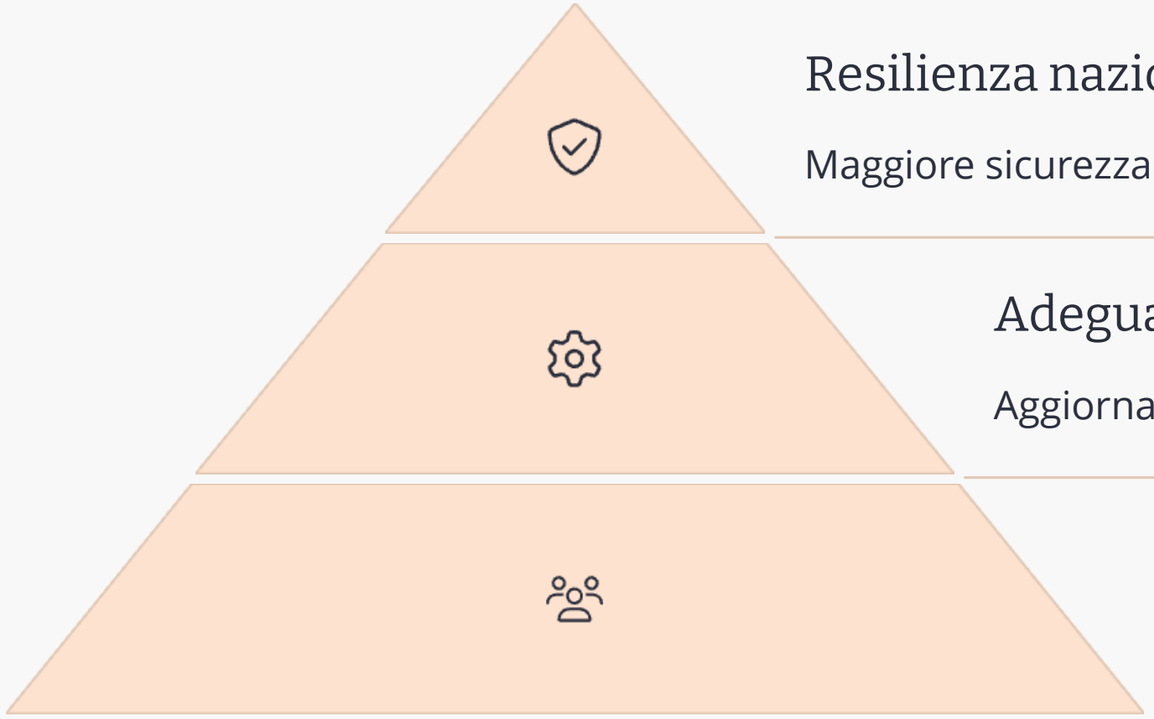
O fino all'1,4% del fatturato globale annuo

24h

Tempo per segnalazione incidenti

Notifica iniziale alle autorità competenti

Impatti, benefici e prossimi step



Resilienza nazionale

Maggiore sicurezza per l'intero sistema-paese

Adeguamento organizzativo

Aggiornamento di processi e responsabilità

Formazione continua

Sviluppo competenze per tutto il personale