Febbraio 2025

Direttiva NIS2 e D.lgs. 138/2024

Cosa cambia per la cybersecurity e resilienza aziendale

Direttiva NIS2 e D.lgs. 138/2024

Introduzione

Criteri di applicazione

Oltre i parametri dimensionali

Fornitori «sistemici»

Gruppi e società collegate

Obblighi e responsabilità

Adacta TAX & LEGAL

Direttiva NIS2 e D.lgs. 138/2024
Cosa cambia per la cybersecurity aziendale

NIS è l'acronimo di «Network and Information Security».

La **Direttiva NIS 2** (UE 2022/2555), in vigore dal 17 gennaio 2023, introduce nuove regole per rafforzare la sicurezza informatica in tutta l'Unione Europea. Unitamente al **D.Lgs. 138/2024** di recepimento nell'ordinamento italiano, viene ampliato il numero di aziende coinvolte e imposte misure più rigorose per la gestione del rischio cyber e la continuità operativa.

Adeguarsi alla **NIS 2** non è solo un obbligo legale: significa proteggere i propri asset digitali e fisici, migliorare la fiducia di clienti e partner e garantire maggiore resilienza aziendale, ridurre il rischio di attacchi informatici, evitare sanzioni e mantenere un vantaggio competitivo.

A chi si applica?

Direttiva NIS2 e D.lgs. 138/2024

Criteri di applicazione settoriali e dimensionali
(art.3, co. 1-4)

Oltre i parametri dimensionali

Gruppi e società collegate
(art.3, co.10)

Anche gli operatori fuori soglia possono, in alcuni casi, rientrare nel perimentro NIS2 **indipendentemente dalle loro dimensioni.**

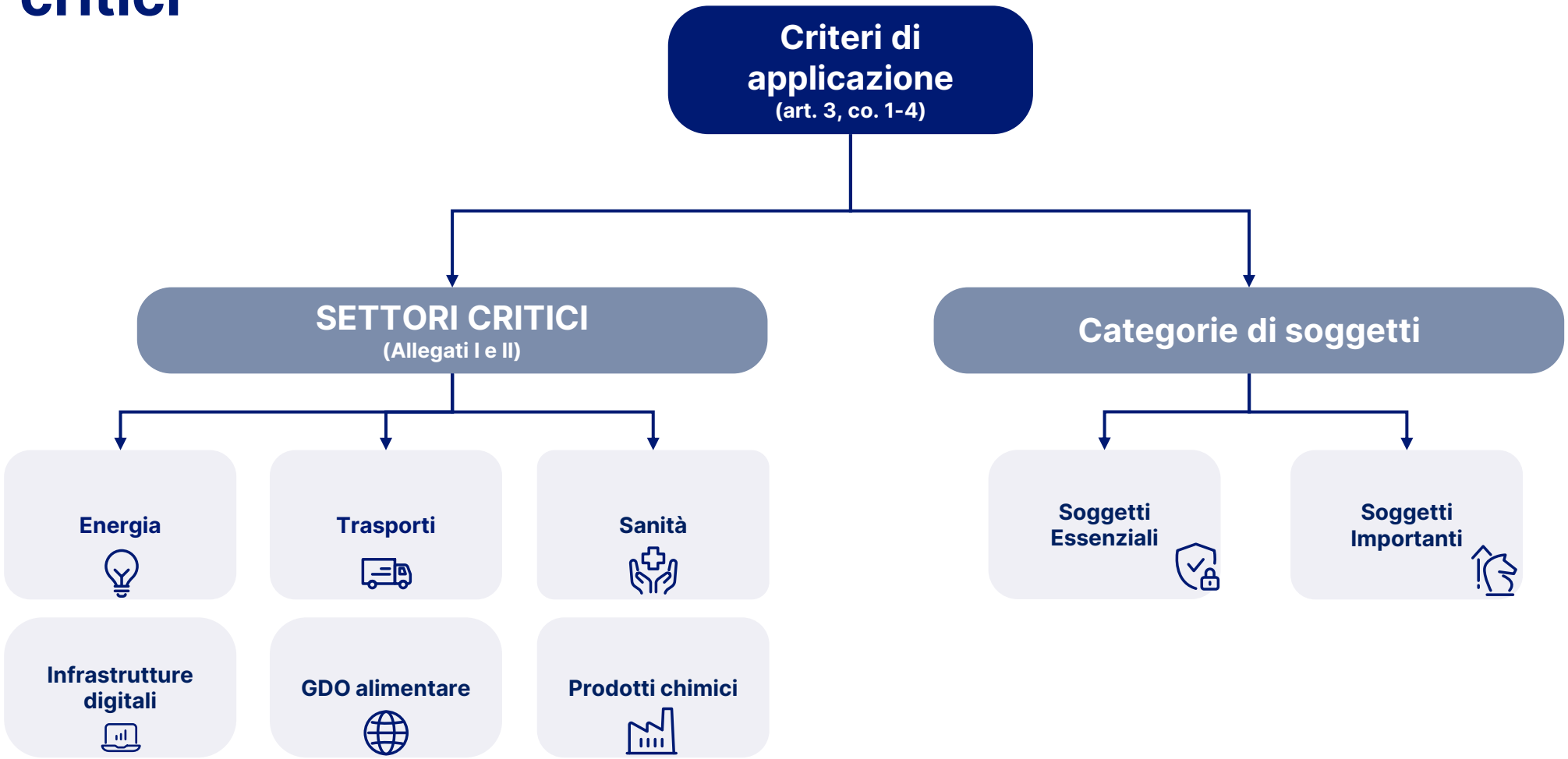
Adacta TAX & LEGAL

Direttiva NIS2 e D.lgs. 138/2024
A chi si applica?

La normativa NIS 2 fissa numerosi e complessi criteri per identificare gli enti e le imprese interessate, includendo settori **strategici** sia pubblici sia privati.

- **Settori ad alta criticità**, ovvero aziende considerate essenziali per il funzionamento socioeconomico dell'UE, tra cui energia, trasporti, sanità, infrastrutture e servizi digitali, devono adottare misure di cybersecurity e resilienza avanzate.
- **Altri settori critici**, tra cui servizi postali, fabbricazione di prodotti critici (es. macchinari, apparecchiature elettriche, dispositivi medici, automotive, ecc.), chimica e GDO alimentare, sono altresì soggetti obblighi di sicurezza informatica specifici.

Criteri di applicazione – Categorie di soggetti e settori critici



Adacta TAX & LEGAL

Criteri di applicazione – Soglie dimensionali

Uno dei punti qualificanti è il criterio di individuazione dei **soggetti "essenziali"** ed **"importanti"**. La normativa NIS2 si applica innanzitutto alle imprese che **superano le soglie** (da valutare a livello di gruppo) previste dalla **Raccomandazione 2003/361/CE in materia di microimprese, piccole e medie imprese**.

GRANDI IMPRESE	MEDIE IMPRESE	PICCOLE IMPRESE*
✓ Numero di dipendenti ≥ 250 ✓ Fatturato annuo ≥ 50 milioni di euro ✓ Bilancio annuo ≥ 43 milioni di euro	✓ Numero di dipendenti 50-249 ✓ Fatturato annuo tra 10 e 50 milioni di euro ✓ Bilancio annuo tra 10 e 43 milioni di euro	✓ Numero di dipendenti < 50 ✓ Fatturato annuo < 10 milioni di euro ✓ Bilancio annuo < 43 milioni di euro

*Le piccole imprese sono escluse dal perimetro NIS2 (salvo importanti eccezioni)

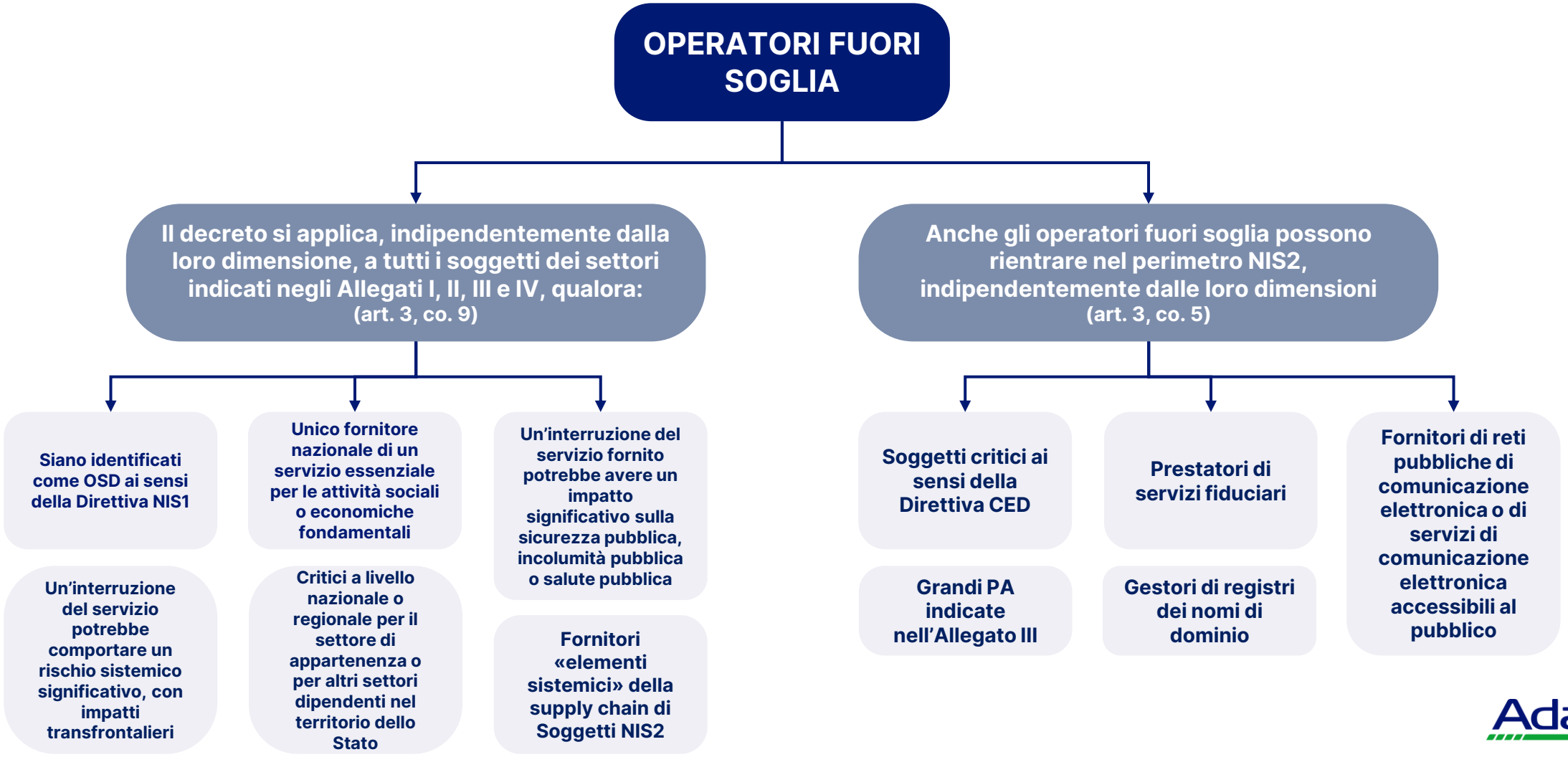
Adacta TAX & LEGAL

Soggetti «fuori-soglia»

La Normativa NIS2 intercetta - tramite previsione di specifici criteri - anche soggetti critici che ricadono fuori dai meri parametri dimensionali.

E’ pertanto necessario porre la massima attenzione a TUTTI i criteri di applicazione di cui alla Normativa NIS2.

Oltre i parametri dimensionali



Adacta TAX & LEGAL

SUPPLY CHAIN

Sul fronte della supply chain, inoltre, il regime NIS2 impone una valutazione puntuale della **dipendenza dai fornitori**, introducendo obblighi specifici sia a carico degli operatori critici sia, appunto, di quei fornitori che, seppur di dimensioni inferiori alle soglie base, rivestono un **ruolo strategico sulla resilienza complessiva di un Soggetto NIS2**.

FORNITORE «SISTEMICO»

Questo accade quando l'interruzione del servizio di un fornitore potrebbe generare **conseguenze importanti sulla filiera di un Soggetto NIS2**, incidendo sulla sua resilienza cyber e/o continuità operativa nazionale o transfrontaliera.

I fornitori «sistemici» della supply chain di un Soggetto NIS2

Chi è?

Un'impresa è un **elemento sistemico** di una **catena di approvvigionamento** quando la sua **operatività** è **cruciale** per servizi critici, con possibili **impatti** su tutta la filiera Soggetto NIS2.

Come individuarlo?

- **Unicità** del fornitore.
- **Concentrazione del rischio**, per la quota di mercato del fornitore assorbita dal Soggetto NIS2.
- Disponibilità di **fornitori sostitutivi**.
- **Impatto potenziale** dell'interruzione del fornitore sulla **continuità operativa o cybersecurity del Soggetto NIS2**.

Adacta TAX & LEGAL

GRUPPI E SOCIETÀ COLLEGATE

Le valutazioni sulle **catene di approvvigionamento** sono particolarmente rilevanti anche all'interno dei **gruppi societari**.

Una singola **controllata** o **collegata**, titolare o beneficiaria di funzioni di gruppo cruciali – in termini di gestione dei sistemi informativi oppure di attività NIS2 rilevanti – può essere assoggettata agli obblighi NIS2.

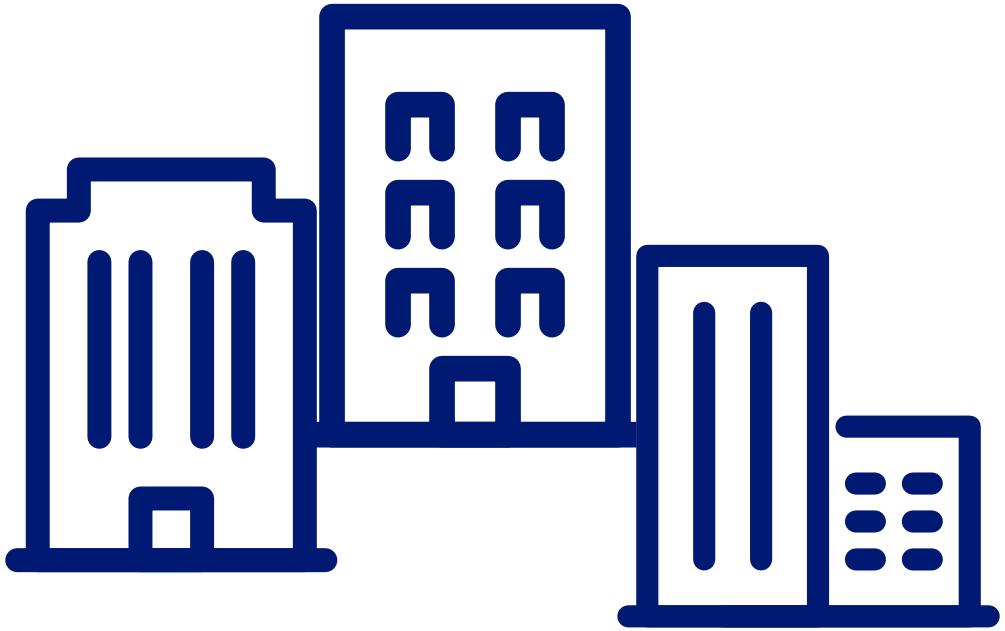
Questo vale salvo che il singolo ente non ricada nei criteri per la c.d. **Clausola di salvaguardia** (nel qual caso potrà richiedere ad ACN una deroga).

Gruppi e società collegate

Il regime NIS2 si applica alle società collegate a Soggetti NIS2 che, indipendentemente dalla loro dimensione, hanno un ruolo rilevante per le operazioni di gestione della cybersecurity o continuità operativa

- **Adottano o influenzano le decisioni sulle misure di gestione della sicurezza di un Soggetto NIS2**
- **Detengono o gestiscono sistemi informatici e di rete da cui dipende la fornitura dei servizi del Soggetto NIS2**
- **Effettuano operazioni di sicurezza informatica del Soggetto NIS2**
- **Forniscono servizi ICT o di sicurezza, anche gestiti, al Soggetto NIS2**

Gruppi e società collegate
Clausola di Salvaguardia

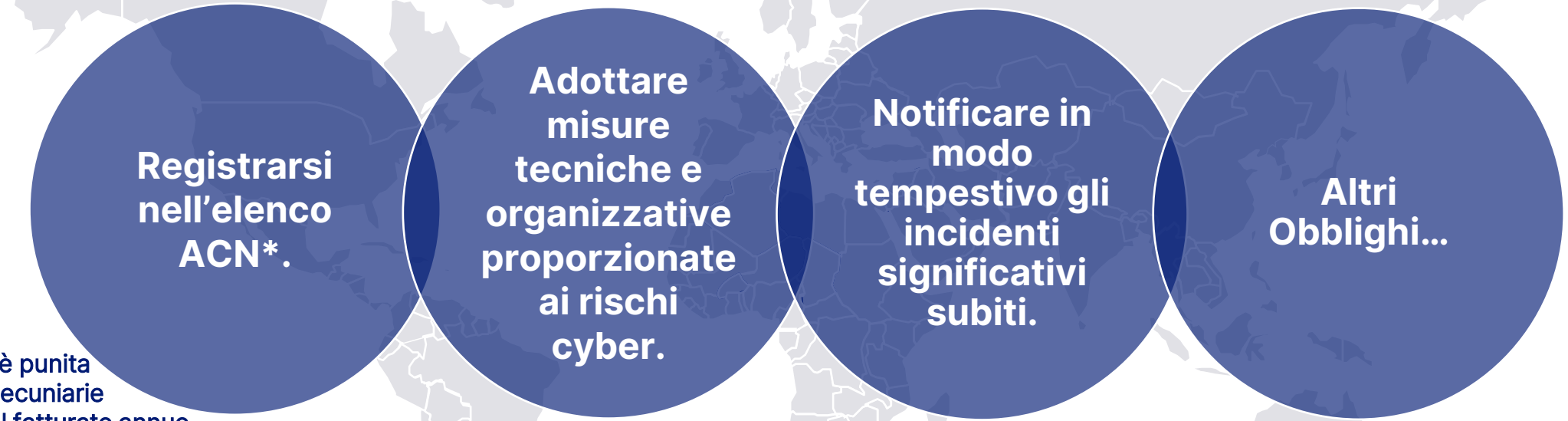


Le **società collegate** a Soggetti NIS2, che ricadono nei criteri dimensionali di gruppo, sono soggette anch'esse al Decreto, se non ricadono **congiuntamente** nei due criteri previsti dalla c.d. **Clausola di Salvaguardia** (DPCM 221/2024):

1. **Totale indipendenza informatica e di rete** della società collegata dal funzionamento dei sistemi informativi del gruppo
2. **Totale indipendenza delle attività o servizi NIS2** della società collegata da quelle/i del gruppo

Adacta TAX & LEGAL

Direttiva NIS2 e D.lgs. 138/2024
Obblighi e responsabilità dei soggetti NIS2



*La mancata registrazione è punita con sanzioni pecuniarie fino al 0,1% del fatturato annuo per i soggetti essenziali e fino al 0,07% per i soggetti importanti.

Adacta TAX & LEGAL

Autorità Nazionale per la Cybersicurezza

L'**Autorità Nazionale per la Cybersicurezza** (ACN) è l'ente competente a tutelare gli interessi nazionali nel campo della sicurezza e resilienza cibernetica.

Tra i suoi compiti principali c'è l'**attuazione della disciplina NIS2 in Italia.** La vigilanza, anche tramite monitoraggio, analisi e supporto diretti, sulle **entità sottoposte alla direttiva** è parte cruciale delle sue attività.

Inoltre, ACN promuove una cultura della **cybersicurezza**, con attività di formazione continua e programmi di sensibilizzazione, collaborando con enti pubblici e privati per garantire una preparazione adeguata contro le minacce cibernetiche.

Adacta TAX & LEGAL

La Roadmap

28.02.2025

Registrazione e censimento dei Soggetti sulla piattaforma di ACN

30.04.2025

Decisione ACN su inclusione nell'Elenco NIS2

30.06.2025

Carico elenco attività e servizi dei Soggtti NIS2

Aprile 2025 / Aprile 2026

Elaborazione e implementazione degli obblighi di base

Aprile 2026

Elaborazione e adozione degli obblighi a lungo termine

Maggio 2026 / ...

Completamento dell'implementazione degli obblighi di base

Adacta TAX & LEGAL

Governance dei rischi

Le misure di sicurezza sono basate su un approccio multirischio, mirando a proteggere i sistemi informatici e di rete e il loro ambiente fisico da incidenti. Esse devono includere i seguenti elementi

- Politiche di analisi dei rischi di cybersicurezza e di sicurezza dei sistemi informatici e gestione degli incidenti.
- Continuità operativa e sicurezza della supply chain.
- Igiene informatica e formazione in cybersicurezza, unitamente a politiche relative all'uso della crittografia e cifratura.
- Ciclo di vita dei sistemi informatici e di rete e uso di soluzioni di autenticazione robusta (a più fattori, altro).
- Sicurezza delle risorse umane, controllo dell'accesso, gestione dei beni e valutazione delle misure di gestione implementate.

Le sanzioni dell'ACN

Sanzioni amministrative pecuniarie

- ✓ per i **soggetti essenziali**, escluse le pubbliche amministrazione: fino a un massimo di **10.000.000 euro o del 2% del totale del fatturato annuo** su scala mondiale per l'esercizio precedente del soggetto;
- ✓ per i **soggetti importanti**, escluse le pubbliche amministrazione: fino a un massimo di **7.000.000 euro o del 1,4% del totale del fatturato annuo** su scala mondiale per l'esercizio precedente del soggetto;
- ✓ per le **pubbliche amministrazioni** che sono soggetti essenziali: da euro 25.000 a euro 125.000.

Sospensione temporanea degli organi direttivi

CdA e **altre persone fisiche responsabili** dell'attuazione della NIS2 **non potranno svolgere funzioni dirigenziali** all'interno dell'ente, finché l'ente non avrà adottato le misure necessarie a **porre rimedio alle carenze riscontrate dall'ACN** o finché non si sarà **conformato alle prescrizioni** indicate da ACN.

Adacta TAX & LEGAL

Adacta
TAX & LEGAL

Adacta Tax & Legal
Strada Marosticana, 6/8,
36100 Vicenza – Italia

Via Visconti di Modrone, 21,
20122 Milano – Italia

+39.0444.228000
info@adacta.it
adacta.it