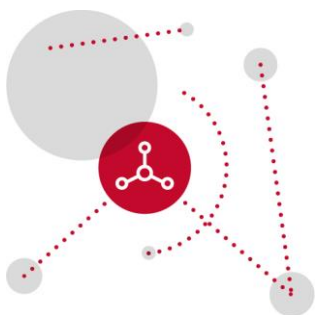


Focus Team Innovazione e Trasformazione Digitale

10 Febbraio 2026

**Focus Team Innovazione
e Trasformazione Digitale****Focus Team Leader**

Tommaso Faelli
tommaso.faelli@belex.com
Tel. +39 02 771131

**Autori**

Tommaso Faelli
tommaso.faelli@belex.com
Tel. +39 02 771131

Marco Dell'Antonia
marco.dellantonio@belex.com
Tel. +39 02 771131

Giulia Tenaglia
giulia.tenaglia@belex.com
Tel. +39 02 771131

Matteo De Angelis
matteo.deangelis@belex.com
Tel. +39 06 845511

**Cybersecurity: riapertura dei termini per la registrazione
al Portale ACN e principali adempimenti per il CdA****1. Ambito di applicazione NIS2 e termini di notifica all'ACN**

La Normativa NIS2 (Direttiva UE 2022/2555, D. lgs. 138/2024 e Determine ACN) si applica alle società:

- (i) stabilite sul territorio italiano e sottoposte alla giurisdizione italiana;
- (ii) con almeno 50 (cinquanta) occupati e un fatturato annuo o un totale di bilancio annuo superiore a EUR 10 milioni;
- (iii) fornitrici di uno o più servizi indicati negli Allegati I e II del Decreto di Recepimento.

Le attività comprese negli allegati potrebbero apparire di nicchia se interpretate come riferibili all'oggetto sociale o all'attività prevalente dell'impresa. Tuttavia, la Normativa NIS2 e le FAQ pubblicate sul sito web dell'ACN attraggono nel campo di applicazione le attività in questione anche quando marginali rispetto all'attività sociale e prestate solamente come servizio *intercompany* alle altre società del gruppo (**si pensi per esempio a certi servizi IT infragruppo, vedi paragrafo 3**).

Le società soggette alla Normativa NIS hanno avuto la prima finestra di registrazione sul Portale dell'Agenzia per la Cybersicurezza Nazionale (ACN) tra gennaio e febbraio 2025.

Per il 2026 i termini per la registrazione sono aperti **dal 1° gennaio al 28 febbraio 2026**. Inoltre, i soggetti già iscritti potranno aggiornare le informazioni caricate nello stesso periodo.

Di seguito riportiamo:

- una tabella con gli adempimenti previsti per i soggetti NIS che si registreranno nel 2026;
- i punti chiave sulla responsabilità degli organi di gestione in materia di cybersicurezza.

2. Gli adempimenti NIS2 e le scadenze per il 2026

Adempimenti	Riferimento normativo	Note operative
Registrazione del Soggetto NIS sul Portale ACN	Art. 7 del D. Lgs. 138/2024 Determinazione dell'ACN n. 333017/2025	La registrazione è possibile dal 1° gennaio al 28 febbraio 2026.
Designazione di un punto di contatto	Art. 7 del D. Lgs. 138/2024 Art. 4 della Determinazione dell'ACN n. 333017/2025	Nel corso della registrazione sul Portale ACN deve essere indicato un punto di contatto. Il punto di contatto può essere un rappresentante legale del Soggetto NIS, un procuratore generale del Soggetto NIS iscritto presso il registro delle imprese oppure un dipendente delegato dal rappresentante legale del Soggetto NIS. È possibile designare un punto di contatto di gruppo nel caso di più società del gruppo soggette alla Direttiva NIS2. Il punto di contatto si occupa di curare l'attuazione delle disposizioni della Normativa NIS per conto della Società. In particolare, il punto di contatto effettua, per conto del Soggetto NIS, la registrazione sul Portale ACN e interloquisce con l'ACN.
Obblighi successivi alla comunicazione dell'inserimento nell'elenco dei soggetti NIS		
Designazione del sostituto del punto di contatto	Art. 7 del D. Lgs. 138/2024 Art. 5 della Determinazione dell'ACN n. 333017/2025	Il sostituto del punto di contatto deve essere registrato sul Portale ACN dal 15 aprile al 31 maggio 2026. Il sostituto punto di contatto supporta il punto di contatto nell'esercizio delle proprie funzioni, può interloquire direttamente con l'ACN e può effettuare sul portale ACN le medesime azioni del punto di contatto.
Indicazione dei membri degli organi amministrativi e direttivi della Società	Artt. 7, 23, 38 del D.lgs. 138/2024 Art. 17 della Determinazione di ACN n. 333017/2025	I membri degli organi amministrativi e direttivi devono essere indicati sul Portale ACN specificandone il ruolo e i recapiti dal 15 aprile al 31 maggio 2026. I membri degli organi amministrativi e direttivi (i) approvano l'implementazione delle misure di gestione

		dei rischi per la sicurezza; <i>(ii)</i> sovrintendono all'implementazione di tutti gli obblighi da adempiere tramite il Portale ACN; <i>(iii)</i> sono responsabili delle violazioni di cui al Decreto di Recepimento. In particolare, la violazione degli obblighi di cui al Decreto di Recepimento grava sull'amministratore delegato e su tutti i membri del consiglio di amministrazione. Infatti, l'ACN – a seguito della violazione e della mancata ottemperanza alle diffide della stessa ACN – può disporre nei confronti di questi soggetti misure interdittive che prevedono il divieto temporaneo di svolgere funzioni dirigenziali. La responsabilità permane in capo all'amministratore delegato e ai membri del consiglio di amministrazione a prescindere da eventuali deleghe ad altri soggetti che operano all'interno dell'organizzazione societaria.
Designazione del referente CSIRT	Art. 7 della Determinazione di ACN n. 333017/2025	<p>Ad oggi l'ACN non ha fornito indicazioni sulle tempistiche per la designazione sul Portale ACN del referente CSIRT nel 2026. È ragionevole aspettarsi che la designazione del referente CSIRT possa avvenire dal 15 aprile al 31 maggio 2026, finestra nella quale i soggetti NIS che sono stati inseriti nell'elenco dei soggetti NIS dell'ACN completano la registrazione sul Portale ACN.</p> <p>Il referente CSIRT ha il compito di interloquire con il CSIRT Italia a cui notificare gli incidenti significativi. È possibile designare uno o più sostituti del referente CSIRT.</p> <p>Il referente CSIRT deve possedere <i>(i)</i> competenze di base in materia di sicurezza informatica e di gestione di incidenti informatici, nonché <i>(ii)</i> una conoscenza approfondita dei sistemi informativi e di rete del Soggetto NIS per conto del quale operano. Inoltre, il referente CSIRT può essere esterno all'organizzazione del Soggetto NIS.</p>
Governance, gestione dei rischi di cibersicurezza e segnalazione degli	Artt. 23, 24, 25 del D.lgs. 138/2024	Al fine di rendere operativi i presidi previsti dalla Normativa NIS2, il Soggetto NIS dovrà adottare nel corso del 2026 policy, piani operativi e protocolli, in particolare: <i>(i)</i>

incidenti informatici	<p>Determinazione di ACN n. 164179 con Allegati 1, 2, 3, 4</p> <p>Allegato del Regolamento di esecuzione (UE) 2024/2690 della Direttiva NIS2 per i soggetti pertinenti¹</p>	<p>organigramma societario per definire ruoli e responsabilità sulla cybersecurity; (ii) mappatura dei sistemi informatici aziendali; (iii) policy di sicurezza dei sistemi informativi e di rete; (iv) policy di gestione dei rischi; (v) policy di gestione e notifica degli incidenti informatici; (vi) piani di continuità operativa e di ripristino in caso di incidenti informatici; (vii) policy per la sicurezza della catena di approvvigionamento; (viii) protocolli per la sicurezza dell'acquisizione di servizi TIC o prodotti TIC; (ix) piani di igiene informatica di base e di formazione in materia di sicurezza, in particolare per i membri degli organi amministrativi e direttivi.</p>
-----------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

3. Il concetto di “servizi gestiti”

Il punto 9 dell'Allegato I del Decreto di Recepimento indica tra i servizi forniti dai soggetti NIS anche i cd. “servizi gestiti” che l'art. 2, c. 1, let. iii) del Decreto di Recepimento definisce: “*servizi relativi all'installazione, alla gestione, al funzionamento o alla manutenzione di prodotti, reti, infrastrutture, applicazioni TIC o di qualsiasi altro sistema informativo e di rete, tramite assistenza o amministrazione attiva effettuata nei locali dei clienti o a distanza*”.

Questi servizi possono riferirsi tanto a componentistiche hardware quanto ad elementi software (anche distintamente) e, in particolare, le attività di installazione, gestione, funzionamento e manutenzione devono essere svolte mediante assistenza o amministrazione attiva, vale a dire con un ruolo attivo:

- (i) a distanza, per cui il fornitore con la propria strumentazione si collega alla rete del cliente; oppure
- (ii) tramite il personale e la strumentazione del fornitore presso i locali del cliente.

Infatti, la FAQ n. A 1.9.2 pubblicata sul sito web dell'ACN esclude dalla categoria dei servizi gestiti le attività di installazione, gestione,

¹ I soggetti pertinenti sono: “i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network, nonché i prestatori di servizi fiduciari” (cfr. art. 1 del Regolamento di esecuzione (UE) 2024/2690 della Direttiva NIS2).

funzionamento o manutenzione svolte dal soggetto NIS senza un ruolo attivo di quest'ultimo, vale a dire:

- a) tramite il proprio personale presso i locali del cliente, ma con la strumentazione del cliente;
- b) tramite istruzioni fornite verbalmente (in presenza o al telefono) o per iscritto (es. via e-mail).

4. Focus sulla responsabilità degli organi di gestione

A. La Direttiva NIS2 e l'organo di gestione

La Direttiva NIS2 stabilisce che l'organo di gestione di un Soggetto NIS (quindi il consiglio di amministrazione, se previsto) deve approvare le misure di gestione dei rischi informatici e vigilare sulla loro attuazione, e può essere ritenuto responsabile per violazioni degli obblighi (art. 20, par. 1 Direttiva NIS2).

Come ultima istanza, se le violazioni persistono, l'ACN può disporre o chiedere ad altre autorità (secondo il diritto nazionale) l'imposizione del divieto temporaneo di esercitare funzioni dirigenziali per chi svolge funzioni al livello di amministratore delegato o rappresentante legale (art. 32, par. 5, lett. b Direttiva NIS2). Inoltre, la Direttiva NIS2 impone agli Stati membri di prevedere la responsabilità delle persone fisiche che hanno potere di rappresentanza, decisione o controllo (art. 32, par. 6 Direttiva NIS2).

B. Le regole italiane: quando e perché possono essere interdetti i consiglieri

Il Decreto di Recepimento chiarisce due aspetti.

Primo, gli organi di amministrazione e direttivi devono approvare e sorvegliare le misure di gestione del rischio e sono responsabili delle violazioni (art. 23, comma 1, lettere a) – c) Decreto di Recepimento).

Secondo, in caso di violazioni, l'ACN segue un percorso graduale: misure di esecuzione (avvertimenti, istruzioni, ingiunzioni, ecc.) e, in mancanza di adeguamento, una diffida a conformarsi entro un termine (artt. 34 e 37 Decreto di Recepimento).

Se l'inadempimento continua anche dopo la diffida, l'ACN può sospendere certificazioni o autorizzazioni; e soprattutto applicare il divieto temporaneo di svolgere funzioni dirigenziali “nei confronti delle persone fisiche (...) ivi inclusi gli organi di amministrazione e gli organi direttivi (...) nonché di quelle che svolgono funzioni dirigenziali a livello di amministratore delegato o rappresentante legale” (art. 38, commi 5 – 6 Decreto di Recepimento).

Dunque, la misura interdittiva temporanea può riguardare, oltre che l'amministratore delegato, anche i consiglieri di amministrazione. Questo risulta:

- sia dall'espresso tenore dell'art. 38, il quale prevede la misura interdittiva sia per l'amministratore delegato sia per le persone fisiche appartenenti agli organi di amministrazione: concetto evidentemente distinto rispetto a quello di amministratore delegato e riferibile ai consiglieri di amministrazione;
- sia dalla circostanza che gli obblighi di decisione e sorveglianza, la cui violazione è sanzionata con la misura interdittiva, spettano sia agli organi di amministrazione sia agli organi direttivi: quindi a tutte le persone fisiche munite di un ruolo di rappresentanza o decisione.

C. Garanzie e proporzionalità

L'interdizione personale è peraltro una *extrema ratio*, limitata al tempo necessario per ripristinare la conformità (art. 32, par. 5 Direttiva NIS2). Il Decreto di Recepimento richiede che le misure siano motivate, proporzionate e adottate nel rispetto dei diritti di difesa, valutando gravità, durata, recidiva, danni, dolo/colpa e collaborazione (artt. 34, 37 e 38 Decreto di Recepimento). È uno strumento per fare rientrare il soggetto NIS in una situazione di conformità, applicato in via eccezionale e per il tempo strettamente necessario.

Dunque, l'ampiezza delle responsabilità personali previste dalla Normativa NIS è controbilanciata dall'approccio graduale nell'applicazione delle sanzioni. In definitiva, i consiglieri di amministrazione risultano passibili delle misure interdittive personali solamente se e nella misura in cui la loro eventuale inerzia persista nonostante le interazioni con l'ACN.

D. Indicazioni operative ACN

La determinazione dell'ACN n. 333017/2025 ("Determinazione") conferma la responsabilità degli organi di amministrazione e direttivi (artt. 4 – 6 Determinazione). In particolare, in risposta al quesito sull'art. 7, comma 4, lett. c) del Decreto di Recepimento (obbligo di indicazione di tutte le persone fisiche responsabili per la decisione e attuazione delle misure di sicurezza e di rappresentanza del Soggetto NIS), l'ACN ha chiarito che nell'aggiornamento annuale devono essere elencati i componenti degli organi di amministrazione e degli organi direttivi, cioè le "persone fisiche responsabili" ex art. 38, comma 5, richiamando l'art. 23:

"In altri termini si tratta delle persone fisiche che compongono gli organi di amministrazione e gli organi direttivi dei soggetti essenziali e dei soggetti importanti di cui all'articolo 23 del decreto NIS.

*Pertanto, ai fini dell'aggiornamento annuale è richiesta la sola elencazione dei **componenti del Consiglio di amministrazione** dell'organizzazione, o strutture*

*analoghe tenuto conto della natura giuridica e alla struttura organizzativa dell'organizzazione. Essi, infatti, ai sensi dell'articolo 23, sovrintendono all'implementazione degli obblighi di cui al decreto NIS e **sono responsabili delle eventuali violazioni***".

E. Circolare Assonime n. 23/2025 e FAQ sul sito web dell'ACN

Sul tema della responsabilità degli organi amministrativi e direttivi in materia di cybersicurezza è intervenuta anche Assonime.

Con la Circolare n. 23/2025 Assonime si pone la questione se il riferimento agli "organi amministrativi e direttivi" contenuta nel comma 6 dell'art. 38 del Decreto di Recepimento possa comportare una responsabilità concorrente (con conseguente applicazione della misura interdittiva nei confronti di tutti i componenti del consiglio di amministrazione). Assonime risponde al quesito, sulla base dei criteri fissati dall'art. 3 della legge n. 689/1981, rilevando che *"non esiste una responsabilità dell'organo in quanto tale e che anche in tal caso occorrerà individuare le persone fisiche che hanno commesso le violazioni, sulla base della specifica ripartizione delle funzioni in concreto attribuite e dei conseguenti obblighi gravanti su ciascuno dei componenti del consiglio"*.

Secondo l'interpretazione di Assonime, il riparto dei ruoli e delle responsabilità all'interno dell'organo amministrativo sono quelle previste dagli artt. 2381 e 2392 c.c. (quindi, sostanzialmente, responsabilità legate alle deleghe, salva l'eventuale colpevole inerzia degli altri consiglieri).

Su questo punto si è espressa anche l'ACN con la FAQ ODA n. 9, affermando che la disciplina della responsabilità degli amministratori prevista dagli artt. 2381 e 2392 c.c. si applica solamente alle attività di attuazione. La segregazione delle responsabilità non si applicherebbe invece – restando in capo a tutti i componenti dell'organo amministrativo – agli obblighi di indirizzo e pianificazione strategica, come:

1. approvare le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica;
2. sovrintendere all'implementazione degli obblighi attuativi della Normativa NIS2;
3. seguire una formazione in materia di sicurezza informatica;
4. promuovere l'offerta periodica di formazione specifica ai dipendenti.



Focus Team Innovazione e Trasformazione digitale

Il *Focus Team* è una costellazione di competenze in diversi ambiti di attività con focus su innovazione e trasformazione digitale.

Tommaso Faelli

IP-IT-Privacy

Alessandro De Nicola

Legal Risk, Compliance & Investigations

Marco Adda

Fiscale

Maurizio Pappalardo

Antitrust

Giulia Bianchi Frangipane

Societario

Vittorio Pomarici

Lavoro

Enrico Chieppa

Litigation & Dispute Resolution

Giulia Tenaglia

IP-IT-Privacy

Gianpaolo Ciervo

Bancario

Matteo Viani

Fiscale

Fabrizio Colonna

Financial Regulatory