NT+ Diritto
Norme & Tributi Plus

Il Sole 24 ORE

Il Commento Società

NIS e cybersecurity, nuova ipotesi di responsabilità oggettiva dell'organo amministrativo

Le deliberazioni e le linee guida ACN ed il rapporto con le certificazioni basate su standard volontari uniformi

*di Luca Tufarelli, Gaia Leoncini**
04 Novembre 2025

La responsabilità degli organi di vertice secondo le disposizioni del D.lgs. 138/2024

Il Decreto Legislativo n. 138/2024 (Decreto), di recepimento della Direttiva (UE) 2022/2555 (cd. "**Direttiva NIS2**") attribuisce agli "***organi di amministrazione***" e agli "***organi direttivi***" dei **soggetti NIS** (non ci soffermeremo nella individuazione di tali soggetti che sono da ricomprendere tra quelli essenziali ed importanti definiti negli artt. 6 e 7 del D.lgs 138/2024) una forma di **responsabilità oggettiva** rispetto degli obblighi in materia di **cybersecurity**. La parola **"*organi direttivi*"** ha generato inizialmente **vari errori e confusioni** sulla esatta individuazione delle persone fisiche che detengano il potere di direzione e rappresentanza di soggetti collettivi (associazioni, fondazioni, comitati, società, enti, etc etc.).
Sul punto non aiuta né la confusa definizione del testo di cui agli *artt. 23 e 38 del Decreto* né tantomeno l'ultima Deliberazione n. 333017 della ACN (*Autorità nazionale per la cybersicurezza istituita con il D.L. 14 giugno 2021, n. 82, a tutela degli interessi nazionali nel cyberspazio*) in vigore dallo scorso 30 settembre 2025. L'unico raggio di luce lo offrono le **FAQ** pubblicate sul **Sito dell'ACN** che identificano i ***"soggetti responsabili"*** - da indicare da parte delle organizzazioni essenziali ed importanti ai sensi *dell'art. 7 del Decreto* in sede di **registrazione** presso l'elenco tenuto da ACN - esclusivamente nelle **persone fisiche** *"....componenti del CdA o strutture analoghe tenuto conto della natura giuridica e della struttura organizzativa della organizzazione ...."*. Precisando poi che *"....non è invece attesa l'elencazione .... di altre figure apicali sotto ordinate al CdA"*. E non potrebbe essere diversamente. Una ricostruzione di diritto non può infatti prescindere dalla **nozione di "*organo*"** che l' esegesi delle fonti impone di attribuire a quelle persone fisiche che detengano il potere di amministrazione e rappresentanza dei soggetti collettivi e degli enti sia in forma singola che collegiale (esempio tipico i componenti del Consiglio di amministrazione).
Stabilito il perimetro sulle persone fisiche responsabili passiamo ad analizzare le norme introdotte dal Decreto con riferimento agli ***"organi amministrativi"*** che coincidono ai fini degli scopi del presente scritto con quelli "***direttivi***".
L'art. 23 del Decreto prevede in sintesi una **nuova ipotesi di responsabilità oggettiva dell'organo amministrativo** per le violazioni e le sanzioni connesse alla **mancata gestione dei rischi di cybersicurezza.**
A tal fine la norma stabilisce che **l'organo amministrativo:**
i) deve **approvare le modalità di implementazione** delle misure di gestione dei rischi per la **sicurezza informatica** adottate ai sensi dell'articolo 24;
ii) deve **sovraintendere all'implementazione** degli obblighi del Decreto;
iii) è **responsabile delle violazioni** del Decreto. La norma va quindi letta **in correlazione all'art. 24 ed all'art. 38** per stabilirne l'effettiva portata.
Infatti, se da un lato ***l'art. 23*** sembrerebbe **limitare la responsabilità** professionale alla fase di **implementazione** e **governo** del piano di sicurezza una volta rilevati i rischi, dall'altro lato sia ***l'art. 24*** che ***l'art. 38*** pongono la valutazione dei rischi alla base di tutte le scelte e, quindi, ne attribuiscono **il governo anche all'organo amministrativo** cui è demandata la valutazione della **proporzionalità** delle misure adottate al grado di **esposizione al rischio**.
L'art. 24 se letto come direttiva procedurale sul percorso da seguire nell'implementazione delle procedure presuppone **una analisi dei rischi** il cui contesto è comunque un parametro che l'organo amministrativo deve considerare per valutare **l'adeguatezza della misura** stessa sul punto vedi comma 1.
L'art. 38, a conferma, attribuisce agli **organi amministrativi la responsabilità personale** sanzionando con pene pecuniare rilevanti sia **l'organizzazione NIS che i componenti dell'organo** per la mancata vigilanza e la mancata adozione di misure di sicurezza adeguate ai rischi . A ciò si aggiunge il **potere interdittivo dell'ACN** che può disporre in capo ai componenti dell'organo amministrativo **l'incapacità a svolgere funzioni dirigenziali** all'interno

dell'organizzazione che rappresentano, sospensione che ha efficacia fino a quando non vengano adottate dal soggetto NIS misure di sicurezza proporzionate all'effettivo livello di esposizione al rischio.
Insomma, si tratta di una **responsabilità personale** che consiglia grande attenzione sia nel delegare parti delle attività da eseguire sia nel processo di valutazione dei rischi. **Il governo di tutto il sistema di gestione della sicurezza** è infatti **in capo all'organo amministrativo**. Pertanto, prima di pensare a come delegare fasi di processo, è bene che sia chiara la centralità della responsabilità di ogni componente dell'organo amministrativo nella governance della sicurezza informatica.
Vedremo come le c.d. ***"norme armonizzate"*** (tra cui le norme c.d. ***ISO/UNI/IEC***) che regolano la materia dei sistemi di gestione della sicurezza e che si basano tutte su un **controllo preventivo di analisi dei rischi**, rivestano un ruolo importante seppur all'interno del percorso valutativo disegnato dal legislatore e dalla ACN.

Il "piano di sicurezza" da approvare ai sensi dell'art. 24 del Decreto alla luce dei provvedimenti della ACN

L'art. 24 prescrive la necessità di utilizzare un **approccio multirischio** nell'analisi dei rischi indicando un elenco di ambiti da considerare come **obbiettivi minimi** da raggiungere con le misure e le politiche di sicurezza adottate. Il risultato di questa analisi definisce il governo e la **strategia di implementazione** delle misure da adottare per quello che possiamo definire il **"*piano di sicurezza*" informatica aziendale** da sottoporre **all'approvazione dell'organo amministrativo.**
L'art. 31 del Decreto attribuisce **all'ACN** il potere di emanare provvedimenti che stabiliscano, tra l'altro, ***"termini, modalità, specifiche e tempi graduali di implementazione"*** degli obblighi sanciti dal Decreto nonché di adottare Linee Guida vincolanti per l'attuazione concreta di questi obblighi. Al di là dei tempi fissati dal Decreto per **la fine di gennaio 2026** per l'obbligo di **notifica degli incidenti** e a **fine ottobre 2026** per quelli relativi alla **implementazione** del piano di sicurezza, la ACN al momento è intervenuta con tre provvedimenti principali; le Determinazioni n. 38565 del 2024 e le nn.164179 e 333017 del 2025.
Per quello che qui interessa, la Determinazione n. 164179 del 14 aprile 2025, ha indicato le **modalità di implementazione** del piano di sicurezza e in particolare definito il percorso di **analisi dei rischi per la successiva adozione delle misure di sicurezza tecniche, operative e organizzative** (così dette "*misure di base*") indicate nella stessa Determinazione. Le misure di sicurezza di base sono stabilite nell'allegato 1 per i **soggetti importanti** e nell'allegato 2 per i **soggetti essenziali** e riprendono la nomenclatura del ***Framework Nazionale per la Cybersecurity e la Data Protection*** (***FNCS***) [1].
La Determina ACN adotta la metodologia del Framework Nazionale, secondo cui i **soggetti NIS** devono
(i) valutare i propri **rischi**,
(ii) verificare che ciascuna misura di sicurezza di base indicata sia stata **effettivamente implementata** e secondo quali **modalità**
(iii) valutare il livello di **maturità dei processi** e delle procedure nonché **l'efficacia delle misure** adottate in base al grado di esposizione al rischio.
La Determina ha pertanto **rimappato l'analisi dei rischi prevista dal FNCS**, organizzando le misure di sicurezza in procedure operative, politiche di sicurezza e ambiti metodologici che costituiscono le aree di riferimento del piano di sicurezza da sottoporre all'approvazione dell'organo amministrativo.
Le modalità di attuazione delle misure sono state ulteriormente dettagliate dall'ACN con le Linee guida NIS2 , attualmente nella versione di settembre 2025. Le *Linee Guida* stabiliscono che per l'attestazione dell'effettiva implementazione del piano di sicurezza con le relative misure, è necessario che **l'organo amministrativo approvi formalmente l'assetto documentale** posto alla base del piano di sicurezza in attuazione degli obblighi di indirizzo, supervisione e approvazione delle misure tecniche, organizzative e procedurali necessarie a garantire un **livello adeguato di sicurezza delle reti e dei sistemi informativi**.
Le linee guida *nell'Appendice C* elencano nello specifico i documenti che l'organo amministrativo sarà formalmente chiamato ad approvare dopo aver effettuato le analisi e la valutazione dei rischi. Tale obbligo di approvazione evidenzia come la **governance della sicurezza informatica** non possa prescindere da un quadro documentale formalmente **validato dagli organi di vertice** secondo il percorso tracciato dalla Determinazione e dalle Linee Guida.

Le interazioni con le certificazioni di sicurezza

Le certificazioni dei sistemi di gestione della sicurezza basate su norme armonizzate quale per esempio la **certificazione ISO 27001**, possono costituire un utile strumento di attestazione della **conformità dei piani di sicurezza** approvati dagli organi amministrativi alle misure tecniche e organizzative richieste dal Decreto come integrate dal provvedimento della ACN.

Vale ricordare che gli **organismi di certificazione** vengono accreditati dopo il vaglio eseguito sulla base del *Regolamento CE 765/2008* dagli **Organismi Nazionali di Accreditamento** - organismi che certificano che un determinato organismo di certificazione soddisfa i criteri stabiliti da norme armonizzate e, ove appropriato, ogni altro requisito supplementare, compresi quelli definiti nei rilevanti programmi settoriali, per svolgere una specifica attività di valutazione della conformità. Cfr. art. 2 del Regolamento UE n. 765/2008 - nominati dal Governo dello stato membro dell'Unione. In Italia tale organismo è l'associazione senza fini di lucro **Accredia** nominata dal Governo ed operante sotto la supervisione del Ministero delle Imprese e del Made in Italy. A tale Associazione è assegnato il compito di attestare la **competenza e l'imparzialità degli organismi e dei laboratori** che **certificano la conformità** dei beni, dei processi e dei sistemi di gestione alle norme. Gli Organismi Nazionali di Accreditamento rivestono un ruolo riguardo alla **verifica di conformità anche nel settore della Cybersicurezza** come indicato nel successivo Regolamento (UE) 2019/881 riguardante il **ruolo dell'ENISA** (*L'agenzia europea per la cybersicurezza*) e la gestione e certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione.

In qualche modo il richiamo a questi organismi è anche stabilito nella *Direttiva NIS2* che riconosce il **valore degli standard ISO/IEC 27000**, quale riferimento utile per la **definizione di misure tecniche e organizzative adeguate** .

Non si comprende come mai né il *Decreto* né la normativa di *soft law* emanata dall'ACN riconoscano tali standard volontari quale prova o presunzione di conformità agli obblighi derivanti dalla NIS2.

Accredia è invece intervenuta riconoscendo il **valore della certificazione 27001** come attestazione di **conformità alla normativa**, con l'emanazione della **UNI/CEI 174:2025**, ossia una prassi di riferimento che definisce i requisiti per un sistema di gestione per la cybersicurezza e la sicurezza delle informazioni armonizzati ai requisiti della norma ISO/IEC 27001 e agli obiettivi indicati dal quadro di riferimento The **NIST Cybersecurity Framework (CSF) 2.0** (framework su cui è basato il Framework Nazionale).

Il **NIST CSF 2.0 e la ISO/IEC 27001** condividono infatti numerosi obiettivi comuni, trattandosi entrambi di strumenti di riferimento internazionali utilizzati per la **gestione della sicurezza delle informazioni e del rischio cyber**, pur presentando differenze significative nella struttura e nell'approccio.

Alla luce di ciò, dotarsi di una certificazione basata sugli standard volontari uniformi rappresenta pertanto una validazione esterna che conferma la solidità tecnica del sistema di sicurezza aziendale, pur non esaurendo i requisiti e gli adempimenti richiesti dal Decreto e dalla ACN, in quanto **non tutti i controlli previsti dalla ISO/IEC 27001 trovano una completa corrispondenza all'interno del NIST CSF**.

Con riferimento all'approvazione formale dell'assetto documentale su cui si fonda il piano di sicurezza, la **certificazione secondo la norma ISO/IEC 27001 nella versione 2024**, in linea con *l'art. 23 del Decreto*, richiede che le politiche di sicurezza delle informazioni aziendali siano approvate dalla direzione (Cfr. norma ISO, Controlli Appendice A, 5.1). Tuttavia, gli **standard ISO si limitano a richiedere l'approvazione delle politiche generali**, senza estendere tale obbligo all'intero corpus documentale posto alla base del sistema di gestione e validato dal certificatore nel corso dell'audit di certificazione. Audit che, se positivo, consente di vedersi attribuire il certificato di conformità.

La normativa nazionale e i **provvedimenti dell'ACN** impongono invece che il piano della sicurezza sia **approvato con uno specifico provvedimento dell'organo amministrativo** secondo le formalità stabilite dalla legge. Quindi con un atto riconducibile per definizione ai soggetti che lo hanno emesso ed al momento storico in cui lo stesso è stato approvato. Pertanto, qualora la Società sia dotata di un correlato sistema di gestione certificato secondo la norma armonizzata ISO/IEC 27001, anche l'assetto documentale sottostante alla certificazione del Sistema di Gestione della Sicurezza deve essere formalmente approvato dall'organo amministrativo in modo da garantirne la **piena opponibilità a terzi ed in particolare alle Autorità competenti in sede di controllo**.

Conclusioni

Salvo proroghe dell'ultima ora, sempre possibili, il **Consiglio di amministrazione** dovrà approvare **entro il 31 gennaio 2026** la procedura di gestione e notifica degli **incidenti di sicurezza**, mentre entro la **fine di ottobre 2026** dovrà provvedere all'**approvazione delle ulteriori procedure** individuate dalla *Determinazione ACN n. 164179 del 14 aprile 2025*, che insieme compongono il **Piano di sicurezza aziendale**.

Le procedure sottoposte **all'approvazione del Consiglio di amministrazione** rappresentano **l'esito delle analisi dei rischi** condotte sulla base del **Framework Nazionale di Cybersecurity,** successivamente **rimappate** secondo la metodologia e gli ambiti operativi **definiti dall'ACN** nella già citate Determinazioni. Esse costituiscono, pertanto, il nucleo operativo del sistema di gestione della sicurezza informatica, da cui discende la possibilità di dimostrare la **conformità** organizzativa e la **tracciabilità** delle decisioni assunte dagli organi di vertice.

L'assenza di un assetto documentale formalmente approvato equivale a una mancata assunzione di responsabilità da parte dell'organo amministrativo, configurando un **deficit di governance** che può comportare conseguenze significative non solo sotto il profilo sanzionatorio, ma anche in termini di **responsabilità gestionale e reputazionale dell'organizzazione.**

In definitiva, il Decreto e i provvedimenti dell'ACN attribuiscono agli **organi di amministrazione** dei soggetti essenziali e importanti una **responsabilità diretta e personale** nella definizione, supervisione e approvazione del **Piano di sicurezza.** Ne deriva un **modello di governance consapevole e documentata della cybersicurezza**, in cui la sicurezza informatica non costituisce più una funzione meramente tecnica, ma un **elemento strutturale** della **responsabilità strategica e fiduciaria** dell'organo di vertice.

Se un appunto va fatto al legislatore ed alla ACN è proprio il fatto che non abbiano mai richiamato nei loro provvedimenti il rapporto che ci dovrebbe essere con le **certificazioni dei sistemi di gestione della sicurezza** basate su **norme armonizzate nazionali ed internazionali**. Questo nonostante l'espresso invito in tal senso formulato dalla legislazione europea sul ruolo degli organismi nazionali di accreditamento e dei soggetti certificatori accreditati. Come detto, le stesse normative che attribuiscono all'**ENISA** la formulazione di schemi da applicare per le certificazioni relative alla cibersicurezza nella società dell'informazione prevedono un percorso che deve **coinvolgere le Autorità Nazionali di Accreditamento** proprio al fine di attribuire alle **Autorità Nazionali per la Cybersicurezza** il controllo e la vigilanza piuttosto che la normazione tecnica di processo.

_____

**Avv.ti Luca Tufarelli e Gaia Leoncini – Ristuccia Tufarelli & Partners*

[1] *Il Framework nell'attuale versione 2.1 è visionabile all'indirizzo https://www.cybersecurityframework.it/ e come si può notare riferendosi agli Allegati A e B delle Linee Guida ACN costituisce la base delle valutazioni di rischio per l'adozione delle procedure stabilite nell'Allegato C.*

Il Sole 24 ORE aderisce a The Trust Project

P.I. 00777910159 © Copyright Il Sole 24 Ore Tutti i diritti riservati
| Accessibilità | TDM Disclaimer
ISSN 2499-1589 - Norme & Tributi Plus Diritto [https://ntplusdiritto.ilsole24ore.com]