TopHic | dig deeper

Giugno 2025

Cyber Insights: sicurezza, compliance, terze parti

Parere dell'esperto

Terze parti e gestione del rischio cyber

di ***Roberto Antoniotti***

Head of Technology and Innovation - Bernoni Grant Thornton

Nel contesto odierno, caratterizzato da una crescente interconnessione digitale e da filiere produttive sempre più distribuite a livello globale, la gestione del rischio cyber legato alle terze parti è diventata un elemento imprescindibile delle strategie di sicurezza delle organizzazioni. La stima secondo cui il 48% delle violazioni di dati nel 2024 sia stato causato da vulnerabilità derivanti da accessi o relazioni con fornitori esterni conferma come questi attori rappresentino un punto d'ingresso privilegiato per i cybercriminali. Di fronte a questo scenario, non è più sufficiente affidarsi a verifiche di conformità sporadiche o a valutazioni statiche dei partner: è necessario adottare soluzioni tecnologiche evolute e processi strutturati, capaci di garantire una gestione...

continua all'interno

Overview

Cybersecurity oggi: da scelta a necessità per le imprese

di ***Francesco Carraro***

Manager - Bernoni Grant Thornton

A fronte di una digitalizzazione sempre più pervasiva, la cybersecurity non è più un'opzione: è diventata una necessità. L'espansione delle tecnologie e dei servizi digitali comporta infatti l'aumento esponenziale della superficie di attacco per i criminali informatici e il tema più grave è che non sempre gli utilizzatori ne sono pienamente consapevoli. Secondo il più recente Rapporto CLUSIT, nel 2024 sono stati registrati 3.541 attacchi cyber gravi a livello globale, il numero più alto mai censito, con una crescita del 27% rispetto all'anno precedente . In Italia, il quadro è particolarmente allarmante: il nostro Paese ha subito il 10% degli attacchi globali, pur rappresentando solo l'1,8% del PIL mondiale. Con 357 attacchi gravi noti nel 2024, l'Italia è...

continua all'interno

Approfondimento

NIS2: priorità strategica per le aziende

di ***Mattia Campagner***

Manager – Bernoni Grant Thornton

La Direttiva NIS2 rappresenta una delle novità più rilevanti e discusse, non solo per l'ampiezza del suo impatto ma anche per il ruolo strategico che attribuisce alla governance della cybersecurity. Dopo aver tracciato una prima panoramica nel paragrafo precedente, è utile entrare nel merito dei principali contenuti della Direttiva, delle categorie di soggetti interessati, degli obblighi previsti e delle scadenze operative già definite a livello nazionale. La Direttiva (UE) 2022/2555, meglio nota come NIS2, è entrata in vigore il 16 gennaio 2023 e si pone come evoluzione della precedente Direttiva NIS (2016/1148), con l'obiettivo di rafforzare e armonizzare la resilienza digitale in tutta...

continua all'interno

Supplemento Notizie flash n° 107 del 25 febbraio 1984

Grant Thornton

Overview

Cybersecurity oggi: da scelta a necessità per le imprese

di ***Francesco Carraro***
Manager - Bernoni Grant Thornton

A fronte di una digitalizzazione sempre più pervasiva, la cybersecurity non è più un'opzione: è diventata una necessità. L'espansione delle tecnologie e dei servizi digitali comporta infatti l'aumento esponenziale della superficie di attacco per i criminali informatici e il tema più grave è che non sempre gli utilizzatori ne sono pienamente consapevoli. Secondo il più recente Rapporto CLUSIT, nel 2024 sono stati registrati 3.541 attacchi cyber gravi a livello globale, il numero più alto mai censito, con una crescita del 27% rispetto all'anno precedente[1]. In Italia, il quadro è particolarmente allarmante: il nostro Paese ha subito il 10% degli attacchi globali, pur rappresentando solo l'1,8% del PIL mondiale. Con 357 attacchi gravi noti nel 2024, l'Italia è stabilmente "nel mirino" dei cybercriminali[2]. Il cybercrime è responsabile di circa l'86% degli attacchi informatici a livello globale, un fenomeno in costante crescita. Tra i principali fattori che alimentano questa tendenza vi è la diffusione di strumenti "*as-a-Service*" a basso costo nel *dark web*, che rendono accessibili attività illecite anche a soggetti con competenze tecniche limitate[3].

La governance della cybersecurity rappresenta l'insieme coordinato di politiche, standard, assetti organizzativi e meccanismi di conformità volti a garantire un presidio rigoroso della sicurezza digitale. Ambiti come energia, sanità, finanza, telecomunicazioni e trasporti sono infatti bersagli ricorrenti di minacce informatiche sempre più complesse e persistenti. Inoltre, a essere colpiti non sono solo i grandi gruppi o le infrastrutture critiche, ma anche e soprattutto le piccole e medie imprese, spesso meno strutturate e quindi più vulnerabili. Un modello di governance efficace consente di creare un ambiente digitale protetto, tutelare informazioni sensibili, assicurare la continuità operativa dei servizi essenziali e contribuire alla stabilità economica. Proprio in virtù del suo impatto sistemico, la cybersecurity viene oggi sempre più riconosciuta come una priorità: governi e autorità regolatorie hanno cominciato da alcuni anni a promuovere l'adozione di normative e standard internazionali, che fungono da riferimento per lo sviluppo di strategie di sicurezza mature e sostenibili. Proprio su questi temi ci siamo confrontati a Milano, dal 14 al 16 maggio, in occasione dell'incontro che ha riunito i team cybersecurity delle member firm del network internazionale Grant Thornton. L'evento ha rappresentato un'importante opportunità di dialogo e di condivisione delle prospettive ed esperienze operative di ciascun invitato, focalizzata sulle principali sfide attuali in materia di sicurezza informatica.

Tra i temi più dibattuti, hanno trovato particolare rilevanza la Direttiva NIS2 (*Network Information Security*) e lo standard ISO/IEC 27001:2022, a conferma della loro centralità nella definizione di modelli di governance cyber efficaci e scalabili.
La prima Direttiva NIS (2016/1148) ha definito un quadro normativo a livello europeo, pensato per migliorare il coordinamento sovranazionale nella gestione della sicurezza delle reti e dei sistemi informativi, con l'obiettivo di proteggere i servizi essenziali per il funzionamento dell'economia e della società dell'UE[4].
In seguito alla rapida evoluzione dell'ecosistema digitale, la Commissione Europea ha avviato un processo di revisione che ha portato all'adozione della Direttiva NIS2, entrata in vigore a gennaio 2023. Gli Stati membri erano tenuti a recepire la nuova direttiva nei rispettivi ordinamenti nazionali entro il 17 ottobre 2024[5]. La NIS2 ha l'obiettivo di uniformare e rafforzare maggiormente la cybersecurity all'interno dell'Unione Europea, introducendo obblighi più stringenti in materia di gestione del rischio e notifica degli incidenti ed estendendoli a un numero maggiore di soggetti pubblici e privati (la NIS riguardava circa 300 aziende italiane, la NIS2 ne coinvolge oltre diecimila).
Inoltre, la Direttiva stabilisce regole per migliorare la cooperazione tra Stati membri, promuovere la condivisione di informazioni e garantire un'applicazione più efficace delle misure di protezione a livello nazionale ed europeo[6].
Parallelamente, molte aziende scelgono di adottare volontariamente standard internazionali come la ISO/IEC 27001:2022, che definisce un modello per la gestione della sicurezza delle informazioni (ISMS). Questo approccio consente di mappare i rischi, pianificare contromisure, monitorare l'efficacia dei controlli e perseguire un miglioramento continuo.
La norma ISO/IEC 27002:2022, complementare alla 27001, fornisce indicazioni operative dettagliate per l'implementazione dei controlli di sicurezza. L'integrazione di questi standard all'interno dei processi aziendali è spesso vista come una best practice, in grado di rafforzare la postura di sicurezza, migliorare la fiducia degli stakeholder e facilitare la compliance a normative come NIS2 e GDPR.

[1] Clusit, Rapporto sulla Cybersecurity in Italia e nel mondo 2025, p. 9.
[2] Ibid, pp. 30–31.
[3] Ibid, pp. 13–14.
[4] Commissione Europea, Domande e risposte sulla direttiva NIS - Rafforzare la sicurezza delle reti e dei sistemi informativi nell'UE, n.d.
[5] Agenzia per la Cybersicurezza Nazionale (ACN), Direttiva NIS, n.d.
[6] Commissione Europea, NIS2 Directive, n.d.

Il parere dell'esperto

Terze parti e gestione del rischio cyber

di ***Roberto Antoniotti***
Head of Technology and Innovation - Bernoni Grant Thornton

Nel contesto odierno, caratterizzato da una crescente interconnessione digitale e da filiere produttive sempre più distribuite a livello globale, la gestione del rischio cyber legato alle terze parti è diventata un elemento imprescindibile delle strategie di sicurezza delle organizzazioni. La stima secondo cui il 48% delle violazioni di dati nel 2024 sia stato causato da vulnerabilità derivanti da accessi o relazioni con fornitori esterni conferma come questi attori rappresentino un punto d'ingresso privilegiato per i cybercriminali. Di fronte a questo scenario, non è più sufficiente affidarsi a verifiche di conformità sporadiche o a valutazioni statiche dei partner: è necessario adottare soluzioni tecnologiche evolute e processi strutturati, capaci di garantire una gestione dinamica, continua e proattiva dell'intero ecosistema di terze parti.

Le organizzazioni più mature in ambito cyber hanno già integrato nelle proprie strategie strumenti avanzati che permettono di ottenere visibilità in tempo reale sul livello di rischio dei propri fornitori e partner. Tuttavia, queste piattaforme da sole non bastano a gestire la complessità crescente di una superficie d'attacco in continua espansione, che coinvolge ambienti *cloud*, dispositivi IoT/OT, sistemi *legacy* e applicazioni di terze parti.

Per questo motivo, Grant Thornton propone un approccio olistico e integrato, capace di coniugare le più moderne tecnologie di monitoraggio e *detection* con servizi di governance, advisory e risposta operativa.

Al centro di questa proposta si colloca *Cybersonar*, una piattaforma proprietaria che unisce funzionalità di *Threat Intelligence* e *Attack Surface Management*, consentendo il monitoraggio continuo della superficie d'attacco esterna e l'identificazione tempestiva di vulnerabilità, configurazioni errate e minacce emergenti, non solo per l'organizzazione ma anche per le sue terze parti critiche. *Cybersonar* permette alle aziende di anticipare gli attacchi, rafforzare la resilienza dell'intero ecosistema digitale e garantire la conformità a normative quali la NIS2 e il regolamento DORA, sempre più rilevanti per molteplici settori.

Questa piattaforma si integra perfettamente con altre soluzioni tecnologiche di punta come *Cyberhunter*, il sistema SIEM & SOAR proprietario che abilita l'automazione dei processi di *detection* e response, e *Defprobe*, soluzione NDR progettata per il rilevamento di anomalie e minacce su reti aziendali, *cloud* e ambienti IoT/OT. A completare l'ecosistema, Grant Thornton offre strumenti innovativi di brand protection predittiva, rimozione di siti e contenuti falsi, *search riservate* nel *dark e deep web*, oltre a chatbot AI personalizzabili per esigenze di sicurezza specifiche.

Tuttavia, la tecnologia da sola non basta: per garantire una protezione completa, Grant Thornton affianca alle piattaforme proprietarie un portafoglio completo di servizi professionali. In ambito *Cybersecurity Governance*, le aziende possono contare su attività di *Cybersecurity Advisory*, definizione di strategie e modelli di governo della sicurezza (*Cybersecurity Strategies & Governance*), supporto CISO *as-a-Service*, gestione di processi di compliance verso standard e leggi come ISO 27001, NIS2, DORA e GDPR, nonché sviluppo di *Security Policies* e procedure personalizzate. Particolare attenzione è rivolta alla fase di *Security by Design*, affinché la sicurezza sia integrata fin dalle prime fasi di sviluppo di prodotti, applicazioni e servizi. Sul fronte tecnico, Grant Thornton eroga servizi di *Cyber Defence* come *vulnerability assessment*, *penetration testing* su reti e applicazioni web, *secure code review*, attività forensi su ambienti digitali, mobili e IoT/OT, *threat modelling*, *cyber threat intelligence* mirata e *assessment* della postura di sicurezza in ambienti *cloud* complessi.

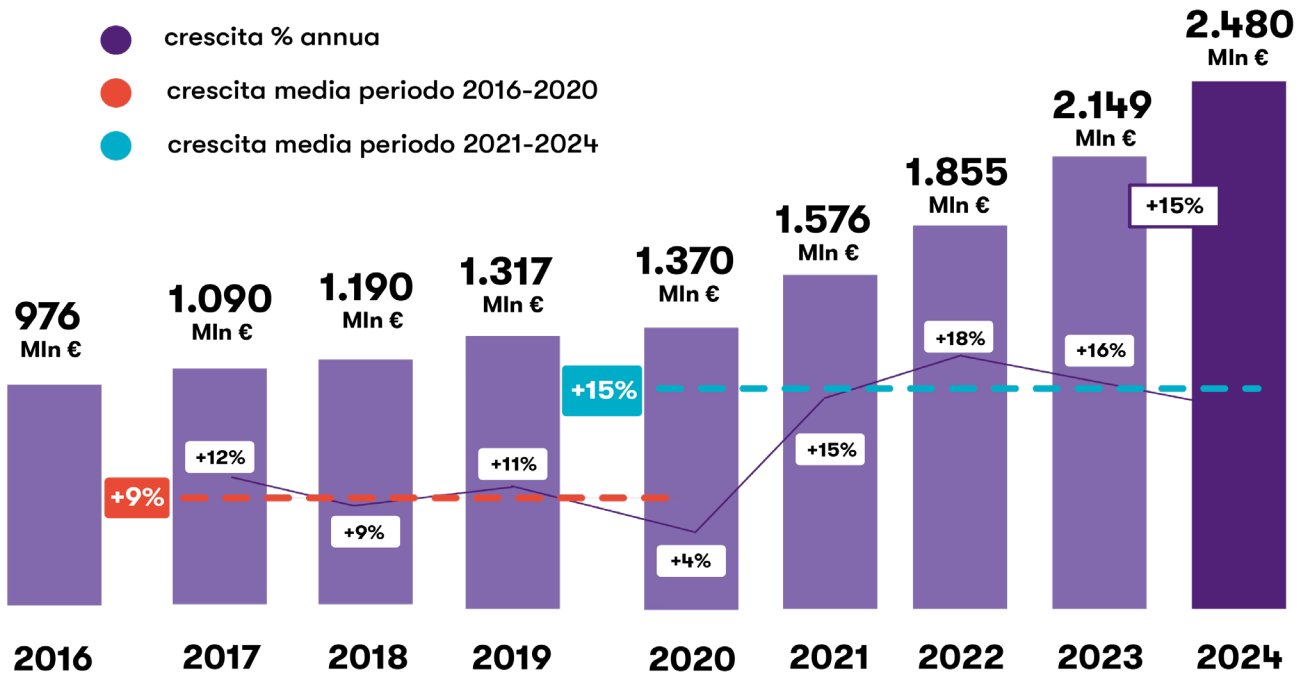
In caso di incidente, le aziende sono supportate da team specializzati di *Incident Response & Forensics* in grado di intervenire rapidamente per contenere, analizzare e risolvere anche eventi sofisticati e su larga scala.
Tutte queste capacità confluiscono in un *Security Operations Centre* (SOC) all'avanguardia, dotato di funzioni di *Managed Detection and Response* (MDR) e *Network Detection and Response* (NDR), per una sorveglianza continua degli ambienti IT/OT, la gestione automatizzata degli alert e la risposta tempestiva agli incidenti. A supporto della protezione dei dati e degli accessi sono inoltre disponibili soluzioni di *Identity and Access Management* (IAM, IGA, PAM), *Data Loss Prevention* (DLP), *Network Access Control* (NAC) e *Email Security Gateway*, fondamentali per ridurre la superficie d'attacco interna e prevenire la perdita o l'esfiltrazione di informazioni sensibili. Infine, per mitigare uno dei rischi più rilevanti, il fattore umano, Grant Thornton propone programmi strutturati di *Cyber Security Awareness* personalizzati, per sensibilizzare e formare il personale su comportamenti sicuri, *phishing simulation*, gestione delle credenziali e risposta agli incidenti.
L'esperienza maturata con numerosi clienti ci conferma che la vera sfida non è solo tecnica, ma anche di governance: la sicurezza informatica deve uscire dall'ambito strettamente IT per diventare un obiettivo di leadership, gestione e governo del rischio, cultura aziendale e *awareness*. In Italia, come evidenziato dal Rapporto CLUSIT 2025, cresce la consapevolezza, ma il gap rispetto ai livelli di maturità di altri Paesi europei resta ancora significativo.

Le aziende italiane stanno iniziando a spostare il focus dagli strumenti tecnologici verso la governance, investendo in modelli organizzativi, formazione e valutazione dei rischi. Questo cambiamento è necessario per stare al passo con il contesto normativo europeo che è in continua evoluzione. La Direttiva NIS2 rappresenta, oggi, uno dei più importanti temi di sicurezza e conformità per tutte le organizzazioni che operano in settori strategici all'interno dell'Unione Europea. Tuttavia, i dati più recenti a nostra disposizione dimostrano che la piena conformità alla NIS2 è ancora un traguardo lontano per molte imprese italiane: infatti, solo il 61% di quelle che hanno avviato un'iniziativa strutturata risulta in linea con i requisiti[7].
Troppo spesso riscontriamo in azienda modelli frammentati, ruoli poco chiari e una sottovalutazione dell'impatto della *supply chain*: aspetti che la NIS2 rende oggi prioritari. In questa fase, molte organizzazioni stanno avviando attività di *assessment* e *gap analysis*, spesso affiancate da percorsi di certificazione ISO/IEC 27001:2022 per strutturare processi efficaci e misurabili. Grant Thornton, grazie alla propria esperienza multidisciplinare e alla presenza capillare sul territorio, ha già supportato con successo alcune aziende italiane nell'avvio del percorso di adeguamento alla NIS2. In particolare, i nostri team hanno condotto assessment approfonditi su vari livelli organizzativi, dalla governance alla *supply chain*, identificando con precisione i *gap* rispetto ai requisiti normativi e proponendo piani di azione concreti, sostenibili e calibrati sul contesto specifico di ciascuna impresa.

Questi interventi si sono successivamente tradotti in roadmap operative che hanno permesso ai clienti di arrivare preparati e di anticipare le scadenze regolatorie, aumentare la propria resilienza informatica e rafforzare la fiducia degli stakeholder interni ed esterni.
Un ulteriore riconoscimento del nostro impegno e della nostra competenza nel settore è rappresentato dall'ottenimento della certificazione ISO/IEC 27001:2022, che attesta l'eccellenza del nostro sistema di gestione della sicurezza delle informazioni. Questo risultato non solo consolida la nostra leadership nel campo della cybersecurity, ma rappresenta anche una garanzia concreta per i nostri collaboratori: lavorare con un partner certificato significa affidarsi a professionisti che operano secondo i più alti standard internazionali. Inoltre, essere certificati ISO/IEC 27001:2022 ci consente di trasferire ai nostri clienti metodi collaudati, una governance strutturata e strumenti già testati, accelerando così il percorso di conformità (non solo verso la NIS2, ma anche verso altre recenti normative come DORA nel settore finanziario).
Il nostro obiettivo non è solo la compliance, ma la costruzione di un sistema di cybersecurity solido, capace di generare valore e proteggere il business nel lungo periodo. In un panorama normativo in rapida evoluzione, Grant Thornton si propone come partner affidabile per accompagnare le aziende italiane nel passaggio da un approccio reattivo a una visione strategica e proattiva della sicurezza informatica. Adeguarsi alla NIS2 non è solo un obbligo: è una scelta di responsabilità, che rafforza la resilienza operativa e la fiducia degli stakeholder.

Dal punto di vista del mercato, il settore della cybersecurity sta vivendo una fase di espansione senza precedenti. Il mercato globale è stato stimato a 245,62 miliardi di dollari nel 2024 e si prevede che raggiungerà i 500,70 miliardi di dollari entro il 2030, con un tasso di crescita annuale composto (CAGR) del 12,9%[8].

Anche in Italia il trend è molto positivo: nel 2024, il mercato nazionale ha toccato i 2,48 miliardi di euro, registrando un incremento del 15% rispetto al 2023. Tra i settori più dinamici si segnalano logistica, trasporti e servizi, che, favoriti dall'attuazione della Direttiva NIS2, hanno registrato incrementi superiori alla media, rispettivamente del 25% e del 24%[9].



Campione Survey CISO 2024: 131 Grandi Organizzazioni

Questi numeri testimoniano una trasformazione strutturale nella percezione e nella gestione del rischio digitale, alimentata non solo dalle nuove normative, ma anche da una maggiore consapevolezza dell'importanza strategica della sicurezza informatica. Le aziende che sapranno investire tempestivamente in soluzioni strutturate, integrate e orientate alla governance saranno in una posizione di vantaggio competitivo, potendo contare su maggiore resilienza operativa, miglior posizionamento di mercato e una più alta credibilità nei confronti di clienti, investitori e partner.

[7] ANGI – Associazione Nazionale Giovani Innovatori. Osservatorio sulla Cybersecurity: solo il 61% delle imprese che hanno intrapreso un cammino strutturato verso la NIS2 risulta conforme, 2024.
[8] Grand View Research, Cyber Security Market Report, 2024.
[9] Osservatorio Cybersecurity & Data Protection – Politecnico di Milano, Il mercato della cybersecurity in Italia: cresce del 15% nel 2024, 2024.

Approfondimento

NIS2: priorità strategica per le aziende

di ***Mattia Campagner***
Manager – Bernoni Grant Thornton

La Direttiva NIS2 rappresenta una delle novità più rilevanti e discusse, non solo per l'ampiezza del suo impatto ma anche per il ruolo strategico che attribuisce alla governance della cybersecurity. Dopo aver tracciato una prima panoramica nel paragrafo precedente, è utile entrare nel merito dei principali contenuti della Direttiva, delle categorie di soggetti interessati, degli obblighi previsti e delle scadenze operative già definite a livello nazionale.

La Direttiva (UE) 2022/2555, meglio nota come NIS2, è entrata in vigore il 16 gennaio 2023 e si pone come evoluzione della precedente Direttiva NIS (2016/1148), con l'obiettivo di rafforzare e armonizzare la resilienza digitale in tutta l'Unione Europea. Rispetto alla versione precedente, la NIS2 amplia sensibilmente l'ambito di applicazione, includendo un maggior numero di settori e imponendo obblighi più stringenti in materia di gestione del rischio, notifica degli incidenti e responsabilità della governance aziendale.

Per quanto riguarda l'ambito di applicazione, l'obbligo di conformità riguarda principalmente le organizzazioni che rientrano nella categoria delle medie e grandi imprese, che superano talune soglie dimensionali previste per tale classificazione, in conformità alla Raccomandazione 2003/361/CE della Commissione Europea.

In base a tale definizione, una media impresa è caratterizzata da meno di 250 addetti e da un fatturato annuo che non supera i 50 milioni di euro, oppure da un totale di bilancio annuo inferiore a 43 milioni di euro. Le imprese di dimensioni minori, ovvero piccole e microimprese, generalmente con meno di 50 dipendenti e un fatturato o bilancio annuo non superiore a 10 milioni di euro, sono in linea di massima escluse, salvo nel caso in cui operino in settori considerati strategici o svolgano funzioni particolarmente rilevanti per la sicurezza nazionale o la continuità di servizi essenziali. Inoltre, la nuova Direttiva NIS2 include 18 settori complessivi, di cui 11 considerati altamente critici (rispetto agli 8 previsti dalla precedente normativa) e 7 settori aggiuntivi classificati come critici. All'interno di questo perimetro rientrano oltre 80 categorie di soggetti, suddivisi in due macro-gruppi: entità essenziali ed entità importanti, a seconda della natura e del peso strategico delle attività svolte.

Settore	Dettaglio	Grandi imprese	Medie imprese	Piccole e micro imprese
Settori altamente critici				
Energia	19 tipologie di soggetto	Essenziali	Importanti *	Fuori ambito **
Trasporti	10 tipologie di soggetto			
Settore bancario	DORA Lex specialis			
Infrastrutture dei mercati finanziari				
Settore sanitario	5 tipologie di soggetto			
Acqua potabile	1 tipologia di soggetto			
Acque reflue	1 tipologia di soggetto			
Infrastrutture digitali	9 tipologie di soggetto			
Gestione dei servizi TIC (b2b)	2 tipologie di soggetto		Importanti *	Fuori ambito **
Spazio	1 tipologia di soggetto			

Figura 1 – Suddivisione dei settori altamente critici in entità essenziali e importanti [10]

Settori critici			
Servizi postali e di corriere	1 tipologia di soggetto	Importanti *	Fuori ambito **
Gestione dei rifiuti	1 tipologia di soggetto		
Fabbricazione, produzione e distribuzione di sostanze chimiche	1 tipologia di soggetto		
Produzione, trasformazione e distribuzione di alimenti	1 tipologia di soggetto		
Fabbricazione	6 tipologie di soggetto		
Fornitori di servizi digitali	4 tipologie di soggetto		
Spazio	2 tipologie di soggetto	Importanti *	Fuori ambito **

Figura 2 – Elenco dei settori critici [11]

Ulteriori tipologie di soggetti		
Pubblica Amministrazione centrale	4 categorie di PA	Essenziali
Pubblica Amministrazione regionale e locale	11 categorie di PA	Importanti *
Ulteriori tipologie di soggetti	4 tipologie di soggetti	Identificazione dell'Autorità

Figura 3 – Suddivisione di ulteriori tipologie di soggetti in entità essenziali e importanti. [12]

Per quanto riguarda gli obblighi operativi, la Direttiva prevede l'adozione di misure di gestione del rischio adeguate e documentate, l'implementazione di procedure per la notifica tempestiva degli incidenti, da trasmettere all'autorità nazionale entro 24 ore dalla scoperta (rispetto alle 72 ore previste dalla precedente normativa), l'introduzione di meccanismi di controllo sulla sicurezza della *supply chain*, che impongono alle organizzazioni di valutare e monitorare i rischi legati ai propri fornitori e partner esterni, in particolare quelli che gestiscono servizi IT, infrastrutture o dati sensibili, la definizione di piani di continuità operativa e gestione delle crisi, la responsabilizzazione del top management, che potrà essere direttamente sanzionato in caso di gravi inadempienze.

Un altro elemento distintivo della Direttiva NIS2 è l'introduzione di un regime sanzionatorio rafforzato.

Nel dettaglio, le entità essenziali possono essere sanzionate fino a 10 milioni di euro o al 2% del fatturato mondiale annuo totale (qualunque sia il maggiore tra i due importi), mentre per le entità importanti il limite massimo è fissato a 7 milioni di euro o all'1,4% del fatturato.
Accanto alle sanzioni economiche, la direttiva introduce anche forme di responsabilità diretta per i vertici aziendali. In caso di inadempienza significativa, i dirigenti possono essere soggetti a misure specifiche da parte dell'autorità competente, comprese la revoca temporanea delle funzioni decisionali in materia di sicurezza e obblighi di formazione. Questo implica che la governance della cybersecurity non può più essere delegata interamente a strutture operative o tecniche: è il Consiglio di Amministrazione, insieme al top management, a dover garantire il presidio strategico e il rispetto delle regole. L'approccio sanzionatorio previsto dalla NIS2, dunque, non si limita a colpire l'organizzazione nel suo complesso, ma coinvolge direttamente i decisori, nella logica di una maggiore *accountability* e trasparenza nella gestione del rischio informatico.

Per quanto riguarda l'Italia, la NIS2 è stata recepita con il Decreto Legislativo 138/2024. Il decreto attribuisce all'Agenzia per la Cybersicurezza Nazionale (ACN) un ruolo centrale nella supervisione e nel coordinamento, definisce le modalità di identificazione dei soggetti obbligati e stabilisce la piattaforma digitale di riferimento per la gestione delle comunicazioni e delle notifiche. Le principali scadenze operative per i soggetti italiani sono:

Prima fase attuativa
(ottobre 2024 - aprile 2024)

- **Entro febbraio 2025:** censimento e registrazione dei soggetti
- **Entro marzo 2025:** adozione dell'elenco dei soggetti NIS
- **Entro aprile 2025:** notifica ai soggetti NIS
- **Entro aprile 2025:** elaborazione e adozione obblighi di base

Seconda fase attuativa
(aprile 2025 - aprile 2026)

- **A partire da gennaio 2026:** obbligo di notifica di base
- **Entro aprile 2026:** elaborazione e adozione del modello di categorizzazione delle attività e dei servizi
- **Entro aprile 2026:** elaborazione e adozione degli obblighi a lungo termine
- **Entro settembre 2026:** completa implementazione delle misure di sicurezza di base

Terza fase attuativa
(da aprile 2026)

- **Da metà aprile 2026:** categorizzazione delle attività e dei servizi; implementazione degli obblighi a lungo termine.

Con la NIS2, l'Unione Europea compie un salto di qualità nella costruzione di un sistema di cybersicurezza solido, integrato e orientato alla prevenzione. Per le aziende coinvolte, si tratta di una sfida complessa ma necessaria, che richiede investimenti, competenze e un approccio strutturato. Ma soprattutto, si tratta di un'opportunità concreta per rafforzare la propria resilienza, la fiducia degli stakeholder e la competitività sul mercato.

[10] Fonte: Agenzia per la Cybersicurezza Nazionale (ACN), Ambito di applicazione NIS2, n.d.
[11] Ibid.
[12] Ibid.

We can help you protect your future

Grant Thornton