SCLA
STUDIO LEGALE

IL “CONFLITTO DI INTERESSI” NEGLI APPALTI PUBBLICI

Avv. Martina Vancini

La Direttiva UE 2022/2555, meglio nota come NIS2, impone standard di cybersecurity uniformi in tutti i 27 Stati membri. In Italia, il recepimento della stessa è avvenuto con il D. Lgs. 138/2024, entrato in vigore il 16 ottobre 2024.

Il panorama delle minacce si è notevolmente aggravato: se la NIS1 nasceva in un’era dove il ransomware era ancora un fenomeno emergente, oggi ci troviamo davanti ad attacchi capaci di paralizzare intere filiere produttive. La Direttiva NIS2 nasce con l’obiettivo di fare in modo che tutte le realtà coinvolte siano in grado di mantenere la continuità operativa di servizi critici anche in caso di attacco informatico.

La nuova direttiva estende quindi il campo di applicazione a 18 settori ridefinendo, al contempo, i criteri dimensionali per includere medie imprese e, in alcuni casi specifici, anche microimprese.

Viene infatti operata una distinzione tra entità essenziali (EE) ed entità importanti (EI). Le entità essenziali operano nei settori altamente critici (energia, trasporti, sanità, infrastrutture digitali, acqua, settore bancario, mercati finanziari e spazio) e, per queste organizzazioni, l’ACN può disporre ispezioni in loco senza preavviso e richiedere audit straordinari. Le entità importanti, invece, pur operando in settori critici (servizi postali, gestione rifiuti, industria alimentare, manifattura, ricerca) godono di un regime leggermente meno stringente ma

non per questo trascurabile. La differenza si riflette anche sulle sanzioni: per le EE le multe possono arrivare fino a 10 milioni di euro o al 2% del fatturato mondiale annuo; per le EI, invece, il tetto scende a 7 milioni di euro o all'1,4% del fatturato.

Le grandi imprese (con oltre 250 dipendenti o con un fatturato superiore ai 50 milioni di euro) e le medie imprese (con oltre 50 dipendenti o con un fatturato superiore ai 10 milioni di euro), appartenenti ai settori sopra indicati, devono rispettare quanto previsto dalla NIS2. Le piccole imprese (con 10–49 dipendenti) e le microimprese (sotto i 10 dipendenti) devono rispettare la NIS2 solo se "unici fornitori" di servizi essenziali in uno Stato membro o se un'interruzione dei loro servizi avrebbe impatti significativi su sicurezza pubblica, salute o economia.

L'obiettivo della NIS2 è tripartito:

(i) introdurre obblighi tecnici dettagliati, riducendo al minimo i margini di discrezionalità nazionali;

(ii) introdurre la responsabilità diretta degli organi di amministrazione: non basta delegare la cybersecurity al reparto IT ma sono i consigli di amministrazione che devono approvare le misure di sicurezza, garantire le risorse necessarie e sottoporsi a formazione specifica;

(iii) imporre una valutazione sistemica della vulnerabilità, estendendo gli obblighi di security ai rapporti con fornitori e subfornitori: non è più sufficiente proteggere il proprio perimetro, bisogna governare il rischio cyber lungo l'intera catena del valore.

L'art. 24 del D. Lgs. 138/2024 costituisce il cuore degli obblighi in materia di gestione del rischio dei soggetti NIS. I soggetti essenziali e importanti sono infatti chiamati ad adottare misure tecniche, operative e organizzative adeguate e proporzionate alla gestione dei rischi posti alla sicurezza dei sistemi informativi e di rete che utilizzano nelle loro attività o nella fornitura dei loro servizi.

Vediamo ora le novità di dicembre 2025 introdotte con la Determinazione del Direttore Generale n. 379907 del 18 dicembre 2025 che ha sostituito la precedente Determinazione ACN n. 164179 del 14 aprile 2025. L'ACN fornisce indicazioni operative dettagliate per strutturare un processo efficace di incident management articolato in cinque macro-fasi interconnesse.

PREPARAZIONE: la fase di preparazione precede il verificarsi dell'incidente e costituisce la base per una risposta efficace. Include tre sottofasi:
(i) il governo, ovvero la definizione delle politiche di sicurezza e l'assegnazione di ruoli e responsabilità;
(ii) l'identificazione, ovvero l'inventario dei sistemi informativi e di rete e l'individuazione di minacce e vulnerabilità;
(iii) la protezione, ovvero l'individuazione delle misure tecniche (backup, log, controllo accessi) e organizzative (procedure, formazione).

RILEVAMENTO: la fase di rilevamento è finalizzata a individuare e analizzare gli eventi rilevanti per la sicurezza informatica, con l'obiettivo di individuare tempestivamente il verificarsi di un incidente e limitarne l'impatto e l'estensione.

RISPOSTA: la fase di risposta rappresenta il cuore del processo e si articola in quattro sottofasi:
(i) la segnalazione, riguardante la notifica dell'incidente alle autorità competenti e la comunicazione alle parti interessate;
(ii) l'investigazione, la quale mira a comprendere l'origine e la portata dell'incidente;
(iii) il contenimento, che ha l'obiettivo di limitare la diffusione dell'incidente e prevenire ulteriori danni;
(iv) l'eradicazione, che consiste nella rimozione della minaccia dai sistemi compromessi.

RIPRISTINO: è finalizzata a riportare i sistemi informativi allo stato antecedente all'incidente, assicurandosi che tutto funzioni regolarmente.

MIGLIORAMENTO: riguarda la fase post incidente ed è finalizzata a potenziare la capacità di gestione degli stessi, individuando eventuali carenze.

La procedura di notifica, prevista dall'art. 25 del D. Lgs. 138/2024, prevede tempistiche stringenti: entro 24 ore dalla scoperta dell'incidente deve essere inviata una pre-notifica al CSIRT che segnali l'incidente, entro 72 ore deve essere inviata una notifica completa con valutazione iniziale della gravità e dell'impatto. Infine, entro un mese dalla notifica, deve essere inviata una relazione finale che descriva dettagliatamente l'incidente, le misure di attenuazione adottate e l'impatto subito.

Alla luce di ciò, è necessario, per alcune realtà, iniziare fin da subito ad operare in conformità al nuovo quadro normativo.

Il presente articolo non intende fornire un parere legale e, per l'effetto, non può essere considerato sostitutivo di una consulenza legale specifica.

Clicca qui per scaricare l’articolo in PDF