



CLYDE&Co

Successful risk navigation

Misure di sicurezza di base
NIS2: il settore aeronautico
italiano è pronto al
decollo?

ITA

Misure di sicurezza di base NIS2: il settore aeronautico italiano è pronto al decollo?

Con l'avvicinarsi dei termini per l'adozione delle misure di sicurezza di base NIS2, gli operatori del settore aeronautico e il loro management sono chiamati a verificare che la governance, i presidi di cybersicurezza e la gestione del rischio lungo la supply chain siano effettivamente pronti e in grado di sostenere il vaglio delle autorità, dei partner commerciali e del mercato.

In sintesi:

- Scadenze imminenti: per i soggetti cui è stata comunicata l'iscrizione nell'elenco NIS da aprile 2025, l'obbligo di implementazione delle misure di sicurezza di base scade a partire da ottobre 2026; per gli iscritti del 2026, dal 31 luglio 2027.
- Responsabilità del management: gli organi di amministrazione e direttivi devono approvare e sovrintendere l'attuazione delle misure, con possibili responsabilità anche personali in caso di inadempimento.
- Conformità da dimostrare: governance, gestione del rischio, protezione dei sistemi e risposta agli incidenti devono essere adeguatamente documentate e verificabili.
- Sicurezza della supply chain: nel settore aeronautico il rischio cyber va governato lungo l'intera supply chain, integrandolo con safety, security e continuità operativa.
- Impatto strategico: la conformità alla normativa NIS2 non è solo un obbligo di legge, ma un fattore di affidabilità, continuità del servizio e competitività sul mercato.

La cybersicurezza rappresenta da tempo una priorità per l'aviazione. La continuità delle operazioni di volo e dei servizi aeroportuali dipende da sistemi digitali fortemente interconnessi, quali sistemi di navigazione e controllo del traffico aereo, piattaforme operative dei vettori, infrastrutture aeroportuali, servizi di assistenza a terra, manutenzione, gestione dei passeggeri e dei bagagli e reti di fornitori tecnologici. In questo contesto, un incidente informatico può produrre effetti che superano il perimetro della singola organizzazione, incidendo sulla regolarità, sulla continuità e sulla resilienza delle operazioni.

L'attuazione della Direttiva NIS2, recepita in Italia con il D.lgs. n. 138/2024 (Decreto NIS2), entra ora in una fase particolarmente significativa per gli operatori aeronautici in elenco NIS. La registrazione presso l'Agenzia per la cybersicurezza nazionale (ACN), la trasmissione di informazioni e le comunicazioni previste per il 2025 e il 2026 non esauriscono il percorso di adeguamento al Decreto NIS2, ma piuttosto ne rappresentano il punto di partenza.

Il Decreto NIS2 prevede un sistema di adempimenti periodici a carico dei soggetti inclusi nel perimetro NIS2 che comprende, tra l'altro, la revisione delle informazioni societarie comunicate all'ACN, l'aggiornamento delle designazioni delle figure incaricate dei rapporti con l'ACN e della gestione degli

incidenti, la tempestiva comunicazione delle variazioni e la categorizzazione delle attività e dei servizi aziendali.

Più che un obbligo una tantum, la NIS2 è dunque un processo di costante adeguamento, soggetto a scadenze, verifiche e aggiornamenti scadenziati, rispetto al quale la capacità di programmare per tempo le attività e definire chiaramente le responsabilità è essenziale ai fini di conformità.

L'attenzione è oggi rivolta sugli aspetti sostanziali. Con la Determinazione n. 379907 del 19 dicembre 2025, l'ACN ha precisato le misure di sicurezza di base per la gestione dei rischi relativi alla sicurezza dei sistemi informativi e di rete sia per i soggetti essenziali che i soggetti importanti, funzionali anche a prevenire gli incidenti o a ridurne al minimo l'impatto.

Tali misure, che costituiscono attuazione degli articoli 23, 24 e 25 del Decreto NIS2, incidono tra l'altro sulla governance in materia di sicurezza informatica, sulla valutazione del rischio, sulla gestione e protezione dei sistemi informativi, nonché sul rilevamento, sulla risposta e sul ripristino in caso di incidenti.

L'ACN, come indicato nella medesima determinazione, ha previsto che i soggetti NIS adottino le misure di sicurezza di base entro 18 mesi dalla ricezione della comunicazione di inserimento nell'elenco NIS.

Poiché le prime comunicazioni di inserimento nell'elenco sono state trasmesse nell'aprile 2025, nel corso del mese di ottobre 2026 giunge a scadenza per i soggetti interessati (inclusi quelli del settore aeronautico) il termine per l'adozione delle misure di sicurezza di base previste. I soggetti inseriti per la prima volta nell'elenco NIS nel corso del 2026 potranno, invece, adottare tali misure entro il 31 luglio 2027.

Nel settore aeronautico, questo passaggio assume particolare rilievo: al ricorrere dei presupposti previsti dalla normativa, la disciplina NIS2 può applicarsi, tra gli altri, ai vettori aerei, ai gestori aeroportuali e agli operatori del controllo del traffico aereo, che devono porre in essere un effettivo modello di governo del rischio cyber, integrato con i processi di safety, security, continuità operativa, supply chain e protezione dei sistemi informativi.

La resilienza del settore dipende, infatti, anche dai rapporti con gli handler, le imprese di manutenzione, gli operatori logistici, i fornitori di servizi digitali e gli altri soggetti della filiera, che possono essere a loro volta inclusi nel perimetro NIS2. Il rischio cyber non può quindi essere valutato per sistemi o organizzazioni isolate, ma deve essere governato considerando le interconnessioni operative, le dipendenze contrattuali e la continuità dei servizi essenziali.

Per le funzioni legali, di compliance e di risk management, l'applicazione delle misure segna il passaggio dalla dichiarazione di conformità alla dimostrazione dell'effettiva implementazione dei presidi. Le autorità competenti potranno valutare in che modo le misure siano concretamente applicate e governate, anche attraverso l'imposizione di misure correttive e sanzioni amministrative pecuniarie.

Inoltre, la governance societaria è direttamente coinvolta: l'articolo 23 del Decreto NIS2 prevede che gli organi di amministrazione e direttivi approvino le modalità di implementazione delle misure di gestione dei rischi per la sicurezza informatica, sovrintendano all'attuazione degli obblighi previsti dal citato

Decreto e siano responsabili delle relative violazioni. Il successivo articolo 38 stabilisce, inoltre, che le persone fisiche responsabili di un soggetto essenziale, o che agiscono in qualità di suoi rappresentanti legali con poteri di rappresentanza, decisionali o di controllo, possono essere ritenute responsabili degli inadempimenti del soggetto NIS rappresentato. Inoltre, in alcuni casi, queste ultime possono essere temporaneamente interdette dallo svolgimento delle funzioni dirigenziali.

Analoghe aspettative di una effettiva implementazione delle citate misure emergeranno verosimilmente anche sul piano commerciale, poiché clienti, partner e fornitori lungo le supply chain attribuiranno sempre più rilevanza, anche in sede contrattuale, alla capacità delle organizzazioni di dimostrare l'adozione di adeguati standard di sicurezza e una gestione consapevole del rischio cyber.

L'adeguamento alla NIS2 diventa così non soltanto un requisito di conformità, ma anche un elemento di affidabilità operativa, continuità del servizio e competitività nel mercato dell'aviazione.

Autori

Paola Croci

Giorgia De Zorzi

Edoardo Mombelli

500

Partners

70+

Offices worldwide*