Shipping Italy
Il quotidiano online del trasporto marittimo

Navigazione e cyber security: dal Corpo delle Capitanerie una circolare per aumentare la sicurezza

Nicola Capuzzo · Wednesday, January 7th, 2026

Il Ministero delle Infrastrutture e dei Trasporti ridisegna le priorità della sicurezza marittima nazionale ponendo l'accento sulla minaccia sempre più concreta del rischio cibernetico. Con la pubblicazione della Circolare "Sicurezza della Navigazione, Serie Generale n. 177/2025" del 16 dicembre scorso, il Comando Generale delle Capitanerie di Porto e l'Autorità Nis per il Settore Trasporti hanno definito il nuovo perimetro normativo vincolante. Il provvedimento si rivolge alle navi battenti bandiera italiana, alle società di gestione Ism e agli impianti portuali, imponendo un aggiornamento delle misure di difesa digitale coerente con gli indirizzi dell'Imo e armonizzato con il quadro europeo della Direttiva Nis2, recepita in Italia con il Decreto Legislativo 138/2024.

La convergenza tra tecnologie informatiche e operative ha reso le moderne unità navali e i terminal portuali dipendenti da sistemi interconnessi come Ecdis, Ais e interfacce di accesso remoto. Se da un lato questa evoluzione ha ottimizzato l'efficienza logistica, dall'altro ha ampliato la superficie esposta ad attacchi che, compromettendo i "Computer Based System", potrebbero minacciare non solo la continuità operativa, ma la stessa sicurezza della navigazione e l'integrità ambientale. Da qui la necessità di un intervento normativo.

La Circolare 177/2025 segna quindi il passaggio da un approccio volontario a uno strutturale e obbligatorio. Il focus del provvedimento risiede nella necessità per le compagnie di integrare organicamente la gestione del rischio cyber all'interno dei propri Safety Management System e dei piani di security. Non si tratta più solo di installare barriere tecnologiche, ma di formalizzare procedure aziendali che coprano l'intero ciclo di vita della minaccia: dalla prevenzione e rilevazione dell'intrusione, fino alla pianificazione delle risposte e delle strategie di recupero post-incidente per garantire la resilienza dei sistemi critici, quali propulsione, governo, generazione elettrica e gestione del carico.

In questo contesto il capitale umano rappresenta un pilastro fondamentale, per questo il ministero ha stabilito che l'adeguamento tecnologico debba andare di pari passo con un percorso di formazione qualificante per tutte le figure chiave, dagli equipaggi ai Company e Port Facility Security Officer, fino ai tecnici It/Ot. Una preparazione che dovrà peraltro essere costantemente aggiornata affinché possa riconoscere le tecniche di attacco più sofisticate e reagire con tempestività.

Il legislatore si spinge fino alle frontiere tecnologiche future, includendo disposizioni che riguardano i sistemi autonomi e i servizi integrati nave-terra, anticipando le vulnerabilità di un settore in rapida automazione. Inoltre, la gestione delle emergenze viene saldata agli obblighi di notifica previsti dalla normativa Nis2, imponendo agli operatori di segnalare tempestivamente gli incidenti significativi al Csirt Italia, consolidando così la cooperazione tra settore marittimo e difesa cibernetica nazionale.

Come sottolineato congiuntamente dal Comando Generale e dall'Autorità Nis, la cybersicurezza diviene una componente imprescindibile della sicurezza marittima complessiva. Per consentire agli operatori di adeguarsi a questi standard elevati, l'entrata in vigore definitiva delle nuove disposizioni è stata fissata al 1° novembre 2026.

This entry was posted on Wednesday, January 7th, 2026 at 5:11 pm and is filed under Navi, Politica&Associazioni
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.