

Federlogistica: la Cyber security vada alle AdSP

19 Febbraio 2022



Luigi Merlo

ROMA – “Il **vero e unico faro** per programmare e gestire i processi di innovazione tecnologica nei porti sono le **Autorità di Sistema Portuale**; e non è certo un caso che nel mondo importanti scali marittimi, come Barcellona o San Diego, proprio per la loro centralità e per le funzioni di regia complessiva, siano stati oggetto di **cyber attack** e per questo siano stati dotati di risorse, anche professionali, che consentano loro di gestire i processi di **digitalizzazione** e affrontare i **cyber risk**, anche per l’intera comunità portuale che governano”.

Secondo **Luigi Merlo**, presidente di **Federlogistica-Confrtrasporto**, “è venuto il momento di affrontare, con serietà e concretezza e quindi nella gestione delle risorse del PNRR, le tematiche relative all’innovazione tecnologica e alla digitalizzazione, dalle quali dipende la sicurezza così come l’efficienza e la competitività dei porti, ma anche dell’intera catena logistica.

I tempi sono stretti: **il 2022 sarà l’anno chiave con l’entrata in vigore della Direttiva Europea Nis 2 sulla sicurezza delle reti e dei sistemi informativi**; Direttiva che **estenderà il raggio di azione** in molti settori delicati tra i quali i trasporti e i porti, **amplierà gli obblighi** non solo alle grandi imprese ma anche a quelle medie e **prevederà sanzioni elevate** per chi non si adegua”.

“Il sistema logistico e portuale italiano non può farsi trovare impreparato. Le risorse del PNRR per la digitalizzazione devono quindi essere impiegate per aiutare le

imprese ma anche le Autorità di Sistema Portuale a strutturarsi. È il caso di ricordare che le stesse AdSP si trovano a far fronte a carichi di lavoro rilevanti per la progettazione e l'implementazione delle opere da realizzare; e proprio in questo scenario devono poter contare su sistemi inviolabili, introducendo da subito la figura del **cyber manager**".

Per il presidente di Federlogistica-Conftrasporto, il rischio di **attacchi hacker**, come quelli subiti da molti porti nel mondo, non è un'ipotesi aleatoria, è invece "terribilmente concreto". E solo un percorso di digitalizzazione che sfoci rapidamente in **Cyber Security Assessment** e quindi nell'impiego dei relativi piani di gestione del rischio cyber "può consentire un salto di qualità non più rinviabile".