OGGETTO*:* Modifica della Struttura Organizzativa dell'AdSP del Mar Ionio. Sezione ICT – Cybersecurity – Transizione Digitale [ICT].

Si premette che l'Autorità di Sistema Portuale (AdSP) del Mar Ionio opera in un contesto istituzionale, economico e tecnologico caratterizzato da una crescente complessità organizzativa e da una progressiva digitalizzazione dei processi amministrativi, logistici e operativi, che coinvolgono una pluralità di soggetti pubblici e privati, a livello nazionale e internazionale.

Il sistema portuale costituisce un'infrastruttura strategica per il Paese, essenziale per la continuità delle catene di approvvigionamento, per la sicurezza nazionale e per lo sviluppo economico. In tale ambito, l'affidabilità, la disponibilità e la sicurezza dei sistemi informativi rappresentano requisiti imprescindibili per il corretto svolgimento delle funzioni istituzionali dell'AdSP.

Negli ultimi anni, la Pubblica Amministrazione in generale, e le AdSP in particolare, sono state interessate da un processo di profonda trasformazione digitale, promosso dal legislatore nazionale e dall'Unione Europea, che ha imposto:

- l'adozione di piattaforme digitali interoperabili;
- la dematerializzazione dei procedimenti amministrativi;
- l'integrazione dei sistemi informativi con quelli di altre amministrazioni e operatori economici;
- l'innalzamento degli standard di sicurezza informatica e di protezione dei dati.

Tale processo è disciplinato, in particolare, dal Codice dell'Amministrazione Digitale (d.lgs. n. 82/2005), che individua nel Responsabile per la Transizione Digitale (RTD) la figura deputata a garantire la coerenza, il coordinamento e l'attuazione delle politiche di innovazione digitale all'interno dell'Ente, nonché dal Piano Triennale per l'Informatica nella Pubblica Amministrazione, che assegna alla sicurezza informatica un ruolo centrale e trasversale.

Parallelamente, il contesto delle minacce informatiche ha registrato un'evoluzione significativa, con un aumento esponenziale di attacchi cyber rivolti alle pubbliche amministrazioni e, in particolare, alle infrastrutture critiche e strategiche, tra cui rientrano a pieno titolo i sistemi portuali. Tali minacce non si limitano alla sottrazione di dati, ma possono compromettere la continuità operativa dei servizi, la sicurezza fisica delle infrastrutture e la fiducia degli operatori economici e istituzionali.

In risposta a tale scenario, il quadro normativo nazionale ed europeo ha rafforzato gli obblighi in materia di cybersicurezza, attraverso:

- il Regolamento (UE) 2016/679 (GDPR) e la normativa nazionale di adeguamento;
- la Direttiva (UE) 2016/1148 (NIS) e la successiva evoluzione del quadro normativo in materia di sicurezza delle reti e dei sistemi informativi;
- l'istituzione dell'Agenzia per la Cybersicurezza Nazionale (ACN) e le relative linee di indirizzo per le pubbliche amministrazioni.

In tale contesto, la distinzione tradizionale tra funzioni di pianificazione digitale, gestione tecnica dei sistemi e presidio della sicurezza informatica risulta sempre meno efficace, in quanto i processi di

digitalizzazione e le misure di sicurezza devono essere progettati, attuati e monitorati in modo integrato e coerente.

Per le Autorità di Sistema Portuale, tale esigenza è ulteriormente accentuata dalla gestione di sistemi informativi complessi e interconnessi, quali, a titolo esemplificativo:

- Port Community System (PCS);
- sistemi di controllo degli accessi e della security portuale;
- piattaforme di interoperabilità con Agenzia delle Dogane, Capitanerie di Porto, operatori logistici e terminalisti;
- infrastrutture ICT a supporto dei servizi essenziali e delle funzioni istituzionali.

Alla luce di quanto sopra, emerge la necessità di un modello organizzativo che assicuri un presidio unitario, continuativo e altamente specializzato della transizione digitale, della gestione dei sistemi informativi e della cybersicurezza, evitando frammentazioni organizzative che potrebbero generare inefficienze, rischi operativi e criticità sotto il profilo della responsabilità amministrativa.

L'attuale struttura organizzativa dell'AdSP del Mar Ionio, prevede due sezioni separate di cui una, sezione ICT, incardinata all'interno della Direzione Affari Generali ed Internazionali, è composta da due unità tra cui l'Amministratore di Sistema ed un ingegnere informatico; mentre l'altra, in staff alle dirette dipendenze del Segretario Generale, in cui è inquadrato il RTD.

Sebbene incardinati in sezioni distinte, le tre figure collaborano quotidianamente essendo coinvolti in una pluralità di progetti di digitalizzazione complessa che richiedono l'implementazione di figure professionali diverse e complementari.

In tale contesto, emerge l'esigenza di un assetto organizzativo coerente, integrato e funzionale alla governance unitaria dei processi digitali e della sicurezza informatica.

All'interno della sezione dovranno, quindi, convergere le tre figure attualmente in forza all'AdSPMI e cioè:

- Il RTD, ing. Luciano Manelli, con compiti che includono, tra l'altro:
  - la pianificazione e l'attuazione delle politiche di digitalizzazione;
  - la razionalizzazione e l'integrazione dei sistemi informativi;
  - la promozione della sicurezza informatica quale elemento strutturale dei processi digitali;
  - il raccordo con le altre strutture organizzative e con i soggetti istituzionali esterni (AgID, ACN, altre PA);
- l'Amministratore di Sistema, p.i. Gianfranco Fornaro, con funzioni operative e tecniche, tra cui:
  - la gestione, configurazione e manutenzione delle infrastrutture ICT;
  - l'amministrazione dei sistemi, delle reti e delle piattaforme applicative;
  - l'implementazione delle misure di sicurezza logica e fisica;
  - il supporto tecnico all'attuazione delle strategie digitali e di sicurezza definite a livello direzionale.
- l'ing. Cosimo Lemma, che presta la sua collaborazione, tra l'altro:
  - nell'analisi e gestione del rischio informatico;
  - nella definizione e verifica delle misure di sicurezza;

- nel monitoraggio degli incidenti e della risposta agli eventi di sicurezza;
- nel supportare l'adeguamento continuo dell'Ente alle normative e alle best practice in materia di cybersicurezza.

La trasformazione digitale e la sicurezza informatica costituiscono ambiti strettamente interconnessi e non scindibili. L'inquadramento delle tre unità nella stessa sezione organizzativa consentirà, tra l'altro:

- una governance unitaria dei processi digitali;
- un allineamento costante tra strategia, progettazione e gestione operativa;
- una riduzione dei rischi derivanti da frammentazioni organizzative.

Inoltre, la collocazione congiunta delle suddette figure favorisce:

- la traduzione immediata delle direttive strategiche del RTD in azioni tecniche concrete;
- una maggiore efficacia nell'implementazione delle misure di sicurezza;
- un presidio continuo dei sistemi informativi critici per le funzioni portuali.

In un contesto portuale, caratterizzato da infrastrutture critiche e servizi essenziali, l'integrazione organizzativa tra competenze digitali e di sicurezza:

- rafforza la capacità di prevenzione e risposta agli incidenti informatici;
- migliora la resilienza dei sistemi e la continuità operativa;
- assicura una gestione coordinata delle emergenze cyber.

Da ultimo, si consideri che, sebbene la riorganizzazione proposta miri a razionalizzare il funzionamento della sezione, da un'analisi svolta sulle attività in corso, è emerso che l'attuale dotazione organica non è sufficiente a rispondere efficacemente al carico di lavoro connesso alle predette funzioni. Appare, quindi, necessario assegnare un dipendente della *Sezione Relazioni Internazionali, Comunicazione e Sviluppo* alla *nuova Sezione ICT* al fine di fornire il necessario supporto amministrativo al suindicato personale impegnato come RUP e/o DEC.

Dall'esito della mappatura delle competenze dei dipendenti dell'AdSP Mar Ionio, effettuata al fine di dare piena attuazione all'obiettivo trasversale in materia di anticorruzione e trasparenza per l'anno 2025, risulta come il dipendente Nicola Gelao, attualmente incardinato nella Direzione AGE, sezione Relazioni internazionali, comunicazione e sviluppo, sia in possesso di competenze informatiche e gestionali che possono essere complementari alle attività di transizione digitale.

Si ritiene, pertanto, opportuno – al fine di agevolare la collaborazione tra il personale della sezione ICT, il Responsabile della Transizione Digitale ed il dirigente della Direzione Affari Generali e Internazionali così da conseguire la migliore sinergia assegnare l'ing. Nicola Gelao, alla nuova sezione ICT.

Infine, nell'ottica di razionalizzare le risorse e semplificare i flussi decisionali, l'inquadramento nella medesima Sezione potrà contribuire a:

- evitare duplicazioni di competenze e sovrapposizioni funzionali;
- semplificare i processi decisionali e i flussi informativi;
- consentire un uso più efficiente delle risorse umane e tecnologiche.

Alla luce delle considerazioni sopra esposte, si ritiene motivato e funzionale creare un'unica sezione, all'interno della Direzione Affari Generali ed Internazionali, da denominare ICT – Cybersecurity – Transizione Digitale, il cui acronimo potrà continuare ad essere, quindi, ICT, al fine di garantire:

- coerenza strategica e operativa;
- maggiore efficacia nella gestione dei sistemi informativi;
- un più elevato livello di sicurezza e resilienza dell'Ente.

La Dirigente Affari Generali ed Internazionali
dott.ssa Laura Cimaglia (*)

LAURA CIMAGLIA
31.12.2025
10:42:39
GMT+01:00

Il S.G. f.f.
dott.ssa Raffaella Ladiana (*)

RAFFAELLA LADIANA
31.12.2025 10:52:54
GMT+01:00

(*) Documento informatico firmato digitalmente ai sensi del d.lgs. n. 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa.