Autorità di Sistema Portuale
del Mar Ionio

Decreto del Presidente
Direzione competente: SG

Oggetto: Direttiva MIT del 06.05.2025, n. 102. Obiettivo strategico: "Adozione di una strategia di governance strutturale della cybersecurity". Obiettivo operativo: "Adozione o aggiornamento degli atti di regolamentazione dell'uso dei sistemi informativi e di individuazione e gestione delle misure di sicurezza informatica in attuazione delle disposizioni recate dal decreto legislativo 4 settembre 2024, n. 138 e delle connesse direttive della Agenzia nazionale per la Cybersicurezza Nazionale". Relazione del Responsabile per la Transizione Digitale ai sensi dell'art.17 del D.lgs. 7 marzo 2005 n. 82, giusta Decreto del Presidente n. 19 del 03-02-2022.

IL PRESIDENTE

Avv. Giovanni Francesco Gugliotti, nominato Presidente dell'Autorità di Sistema Portuale del Mar Ionio con Decreto del Ministro delle Infrastrutture e dei Trasporti n. 282 del 12 novembre 2025;

su proposta del Segretario Generale f.f., dott.ssa Raffaella Ladiana;

Premesso che

- l'AdSPMI ha da tempo avviato un processo di innovazione tecnologica e digitale ed un percorso di razionalizzazione e semplificazione organizzativa, volti all'adozione di strumenti applicativi che permettano all'Amministrazione di adempiere alle prescrizioni normative di carattere nazionale ed europeo, e di soddisfare la crescente domanda dei servizi portuali dell'area mediterranea attraverso l'iniziativa progettuale dello Smart Taranto Digital Port;
- in tale ottica, l'Ente, con decreto n. 132 del 06.12.2023, ha aderito alla Convenzione di concessione stipulata, ai sensi degli artt. 164, 165, 179 co. 3 e art. 183 co. 15 del d.lgs. 50/2016, dal Dipartimento per la Trasformazione Digitale della Presidenza del Consiglio dei Ministri con il Polo Strategico Nazionale S.p.A. (PSN), che offre servizi cloud qualificati alle Pubbliche Amministrazioni per la loro transizione digitale, migrando i principali servizi online. In seguito, in data 07.12.2023, è stato sottoscritto il contratto d'utenza, discendente dall'adesione dell'AdSPMI alla suddetta Convenzione;
- al fine di elevare il livello di cybersecurity dell'infrastruttura interna, l'Ente ha chiesto l'ammissione a finanziamento – previa candidatura all'avviso pubblico n. 08/2024 – per gli interventi di potenziamento della resilienza cyber, a valere sul Piano Nazionale di Ripresa e

Resilienza, Missione 1 – Componente 1 – Investimento 1.5 "Cybersecurity" M1C1I1.5, presentando il Progetto denominato "POTENZIAMENTO DELLA RESILIENZA CYBER DEL PORTO DI TARANTO";

- in seguito all'ammissione a finanziamento, con Decreto n. 23 del 25.02.2025, l'AdSPMI ha aderito all'Accordo Quadro per la fornitura di prodotti per la sicurezza perimetrale, protezione degli endpoint e anti-APT ed erogazione di servizi connessi – lotto 1 – per le Pubbliche Amministrazioni (Cybersecurity 2) ai sensi dell'art. 54 co. 3 del D.Lgs. n. 50/2016;

Considerato che

- con nota MIT n. 778/2023/Naz/0 del 06.12.2023, inerente all'attuazione del d.lgs. n. 65/2018 (di recepimento in Italia della direttiva (UE) 2016/1148, "Direttiva NIS"), l'AdSPMI è stata individuata quale Operatore di Servizi Essenziali del Settore Trasporti – Sotto-settore: Trasporto per le vie d'acqua e in seguito all'entrata in vigore del d.lgs. n. 138/2024, l'Ente ha ricevuto in data 13.04.2025 comunicazione ai sensi dell'art. 7, comma 3, lettera a (al protocollo AdSP n. 9027 del 14.04.2025) di inserimento nell'elenco NIS quale soggetto essenziale di cui all'Allegato I del decreto legislativo medesimo, "Settori di alta criticità" ("Trasporti - Trasporto per vie d'acqua - Organi di gestione dei porti);
- conseguentemente, l'AdSP MI, ha provveduto:
  a) a designare entro il 28.02.2025 (in sede di registrazione sulla piattaforma digitale dell'ACN) il proprio punto di contatto (Ing. Luciano Manelli, inquadrato, come Responsabile per la Transizione al Digitale nello Staff del Segretario Generale/Presidente);
  b) a fornire entro il 31.05.2025 l'indicazione di un sostituto del punto di contatto (Dott.ssa Laura Cimaglia, Dirigente della Direzione AGE); nonché
  c) a individuare l'ing. Cosimo Lemma, impiegato nella Direzione AGE – Sezione ICT, quale referente CSIRT.

Considerato, inoltre, che per l'adempimento degli obblighi di base del suddetto decreto, i soggetti NIS sono tenuti ad adottare le misure di sicurezza di base e a notificare al CSIRT Italia gli incidenti significativi di base stabiliti dalla determinazione ACN n. 164179 del 14.04.2025.

Preso atto della relazione del Responsabile della Transizione Digitale dell'AdSP MI, alla quale sono allegati i seguenti documenti strategici che adempiono alla normativa vigente e definiscono

la regolamentazione dell'uso dei sistemi informativi e di individuazione e gestione delle misure di sicurezza informatica:

a) Piano strategico per la cybersecurity;
b) Politica di risposta agli incidenti e ripristino, articolata in:
   - Politica di risposta agli incidenti e ripristino – ALL1 Procedura di incident handling and response su perimetro cloud del Polo Strategico Nazionale
   - Politica di risposta agli incidenti e ripristino – ALL2 Piano di isolamento asset su perimetro cloud del Polo Strategico Nazionale
   - Politica di risposta agli incidenti e ripristino - ALL3 Procedura di incident handling and response su perimetro infrastruttura on-premise;
c) Politica di affidabilità delle Risorse Umane, formazione del personale e consapevolezza;
d) Politica di gestione degli asset;
e) Politica di gestione dei rischi della catena di approvvigionamento;
f) Politica di gestione del rischio, conformità ed audit di sicurezza;
g) Politica di gestione delle identità e degli accessi;
h) Politica di gestione delle vulnerabilità;
i) Politica di sicurezza dei dati;
j) Politica dei ruoli e responsabilità sulla sicurezza dei sistemi informativi e di rete;
k) Politica sulla sicurezza delle reti e delle comunicazioni;
l) Politica sulla sicurezza fisica.

Ritenuto che, in attuazione dell'obiettivo strategico generale dei presidenti delle Autorità di sistema portuale, da conseguire per l'anno 2025, (punto n. 4) della Direttiva MIT del 06.05.2025, n. 102) occorre l'"*Adozione di una strategia di governance strutturale della cybersecurity*", da attuare, tra l'altro, attraverso il seguente obiettivo operativo: "*Adozione o aggiornamento degli atti di regolamentazione dell'uso dei sistemi informativi e di individuazione e gestione delle misure di sicurezza informatica in attuazione delle disposizioni recate dal decreto legislativo 4 settembre 2024, n. 138 e delle connesse direttive della Agenzia nazionale per la cybersicurezza nazionale*";

tutto ciò premesso, considerato e ritenuto,

Letta e applicata la L. 84 del 1994, rubricata *"Riordino della legislazione in materia portuale"* e s.m.i. e, in particolare, l'art. 9 della stessa;

Sentito il Segretario Generale f.f., nominato con decreto n. 38/2025 del 03.06.2025;

DECRETA

1. le premesse fanno parte integrante e sostanziale del presente provvedimento;
2. di definire la seguente mission strategica per la cybersecurity: "*Garantire un ecosistema portuale digitale sicuro, resiliente e integrato, attraverso l'adozione di soluzioni tecnologiche avanzate, la promozione di una cultura condivisa della sicurezza informatica e il rafforzamento della cooperazione tra attori pubblici e privati, al fine di sostenere l'innovazione, la sostenibilità e l'attrattività internazionale del sistema portuale*";
3. di prendere atto ed approvare la relazione del Responsabile per la Transizione Digitale allegata al presente provvedimento e, conseguentemente, adottare ed approvare i seguenti documenti strategico-regolamentari:
   a) Piano strategico per la cybersecurity;
   b) Politica di risposta agli incidenti e ripristino, articolata in:
      - Politica di risposta agli incidenti e ripristino – ALL1 Procedura di incident handling and response su perimetro cloud del Polo Strategico Nazionale
      - Politica di risposta agli incidenti e ripristino – ALL2 Piano di isolamento asset su perimetro cloud del Polo Strategico Nazionale
      - Politica di risposta agli incidenti e ripristino - ALL3 Procedura di incident handling and response su perimetro infrastruttura on-premise;
   c) Politica di affidabilità delle Risorse Umane, formazione del personale e consapevolezza;
   d) Politica di gestione degli asset;
   e) Politica di gestione dei rischi della catena di approvvigionamento;
   f) Politica di gestione del rischio, conformità ed audit di sicurezza;
   g) Politica di gestione delle identità e degli accessi;
   h) Politica di gestione delle vulnerabilità;
   i) Politica di sicurezza dei dati;
   j) Politica dei ruoli e responsabilità sulla sicurezza dei sistemi informativi e di rete;

k) Politica sulla sicurezza delle reti e delle comunicazioni;

l) Politica sulla sicurezza fisica.

4. il Piano, le procedure e le politiche potranno essere rivisitati ed eventualmente ampliati annualmente, in funzione degli aggiornamenti normativi e dell'evoluzione tecnologica, mantenendole aggiornate alle più recenti metodologie di gestione del rischio informatico, per contrastare in modo sempre più efficace le minacce emergenti oltre a quelle note;
5. il Piano e le procedure di *incident handling and response* saranno efficaci con decorrenza dalla data di registrazione del presente provvedimento;
6. di dare atto che con l'approvazione delle politiche prende avvio il procedimento di adeguamento dell'Ente agli obblighi a lungo termine e che il completamento dell'implementazione dei suddetti obblighi avverrà entro diciotto mesi ex art. 42, comma 1, lettera c del d.lgs. 138/2024 dalla ricezione della notifica di inserimento nell'elenco dei soggetti NIS (13.04.2025).

Il presente Decreto è notificato agli interessati a/m posta elettronica e sarà registrato e condiviso con gli uffici competenti, nonché pubblicato secondo le disposizioni normative in materia di Anticorruzione e Trasparenza.

Il Segretario Generale f.f.
Dott.ssa Raffaella Ladiana (*)

Il Presidente
Avv. Giovanni Francesco Gugliotti (*)

(*) 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.