Autorità di Sistema Portuale
del Mare Adriatico Orientale
Porti di Trieste e Monfalcone

Linee Guida per la gestione della comunicazione, dei rapporti con Istituzioni e Fornitori di Servizi digitali in tema di Sicurezza Cibernetica

Autorità di Sistema Portuale del Mare Adriatico Orientale

Sommario

PREMESSA

La *sicurezza informatica o cibernetica* (c.d. *cybersecurity*) rappresenta una priorità strategica per le infrastrutture critiche come i porti, che svolgono un ruolo fondamentale nell'economia nazionale e internazionale.

Gli attacchi alle infrastrutture critiche cibernetiche, oltre a compromettere le funzionalità operative, possono avere ripercussioni gravi a livello economico, sociale e di percezione del buon andamento della pubblica amministrazione.

Tali attacchi, inoltre, sono spesso utilizzati come strumenti propagandistici per diffondere insicurezza e sfiducia nei confronti dell'operato delle Istituzioni.

In questo contesto, l'Autorità di Sistema Portuale del Mare Adriatico Orientale intende adottare una policy interna in grado di definire i principi e le linee guida per la gestione della comunicazione interna ed esterna degli eventi legati alla *cybersecurity*.

Il presente documento è pensato per promuovere innanzitutto la massima riservatezza nella gestione delle informazioni, conformemente ai principi generali (art. 3) del Codice di Comportamento dell'Autorità di Sistema Portuale del Mare Adriatico Orientale, secondo cui i "*dipendenti dell'Autorità non usano a fini privati le informazioni di cui dispongono per ragioni d'ufficio, evitano situazioni e comportamenti che possano ostacolare il corretto adempimento dei compiti o nuocere agli interessi o all'immagine dell'Autorità*".

La sua attuazione sarà, inoltre, supportata da un efficiente e sicuro sistema di procedure e linee guida per la comunicazione interna e per la gestione dei rapporti con le altre Istituzioni competenti in tema di comunicazione sulla *sicurezza cibernetica*, nonché da strumenti contrattuali volti a regolare i rapporti con i fornitori di servizi digitali assicurando un coordinamento efficace tra tutti i soggetti coinvolti.

1. Obiettivi del documento

Con tale documento, l'Autorità di Sistema Portuale del Mare Adriatico Orientale mira a garantire un alto standard di difesa attraverso:

- Riservatezza e Controllo delle Comunicazioni, con l'obiettivo di ridurre al massimo la diffusione di informazioni sensibili riguardanti attacchi cibernetici, per garantire la tutela della riservatezza dei sistemi di difesa e ridurre al massimo l'obiettivo di risonanza mediatica dell'informazione ricercata da chi esegue l'attacco;
- Attenzione alle modalità di comunicazione interna ed esterna, garantendo che ogni dichiarazione ufficiale sia gestita in modo centralizzato dai vertici dell'Autorità di Sistema Portuale del Mare Adriatico Orientale.
- Coordinamento e Collaborazione con la promozione di un approccio integrato e collaborativo nella gestione degli incidenti informatici, coinvolgendo tutti i soggetti interni ed esterni rilevanti, comprese le società controllate, le partecipate, i fornitori e le Istituzioni competenti.
- Tutela Legale e Contrattuale con l'adozione di misure contrattuali volte a proteggere l'Autorità di Sistema Portuale del Mare Adriatico Orientale da eventuali divulgazioni non autorizzate, garantendo l'adesione alla policy da parte di tutti i dipendenti, partner e fornitori.

2. Divieto di Comunicazioni esterne non autorizzate

In un'ottica di tutela dell'interesse della Pubblica Amministrazione, nessun dipendente, compresi i soggetti coinvolti nel sistema di sicurezza informatica, è autorizzato a rilasciare dichiarazioni pubbliche o condividere informazioni relative a temi collegati ai sistemi di sicurezza cibernetica adottati dall'Autorità di Sistema Portuale e, in particolare:

- informazioni su attacchi cibernetici in corso o già avvenuti;
- modelli, protocolli o strumenti interni di difesa informatica e più in generale qualsiasi informazione da cui possa derivare un rischio per la sicurezza del sistema portuale.

Ogni comunicazione ufficiale relativa a eventi di sicurezza cibernetica deve essere gestita, in collaborazione con l'*Area Relazioni Esterne*, esclusivamente dai vertici dell'Autorità di Sistema Portuale del Mare Adriatico Orientale, che potranno, se ritenuto necessario, ricorrere a dichiarazioni rilasciate preferibilmente in forma scritta. Con il fine di ridurre l'effetto di risonanza, tali comunicazioni dovranno essere rilasciate solo in circostanze eccezionali, al termine dell'attacco, se ritenuto strettamente necessario per la tutela dell'Amministrazione e del sistema portuale.

3. Gestione delle Comunicazioni interne

A livello interno, la circolazione delle informazioni relative alla sicurezza cibernetica è strettamente regolamentata e riservata ai seguenti soggetti:

- Responsabile dell'*Area Sicurezza Informatica*: incaricato di monitorare e gestire gli eventi di cybersecurity, informando tempestivamente i vertici dell'Autorità di Sistema Portuale del Mare Adriatico Orientale sull'evoluzione degli attacchi, sulle misure adottate e sulle conseguenze rilevate.

- *Responsabile della sicurezza portuale/Port Security Officer:* ha il compito di mantenere un canale di comunicazione riservato con i corpi istituzionali competenti (es. Capitaneria di Porto, Polizia Marittima) e di coordinarsi con il Responsabile dell'*Area Sicurezza Informatica* per garantire un'azione sinergica.
- *Punto di contatto NIS:* designato ai sensi del D. Lgs. 138/2024 art. 7, comma 1, lettera c). Può eventualmente coincidere con uno degli altri soggetti elencati.
- Responsabile dell'*Area Relazioni Esterne*
- Presidente/Commissario Straordinario
- Segretario Generale/Segretario Generale facente funzioni

Ogni comunicazione interna dovrà avvenire tramite canali sicuri e riservati, nel rispetto delle normative vigenti sulla protezione dei dati.

4. Rapporti con Corpi Istituzionali competenti in materia di sicurezza e di sicurezza informatica

Delle presenti Linee Guida sarà data comunicazione, per conoscenza, ai Corpi Istituzionali competenti in materia di sicurezza, quali la Capitaneria di Porto e la Polizia di Frontiera Marittima, per garantire un coordinamento efficace.

Lo scambio di informazioni con tali Corpi Istituzionali, a cura del *Responsabile della sicurezza portuale/Port Security Officer*, dovrà avvenire in modo riservato e nel rispetto delle procedure stabilite, e comunque dopo l'autorizzazione da parte del Presidente/Commissario Straordinario e/o del Segretario Generale/Segretario Generale facente funzioni.

Le comunicazioni ai Corpi Istituzionali competenti in materia di sicurezza informatica avverranno secondo quanto definito dalla normativa vigente (D. Lgs. 65/2018, 105/2019 e 138/2024 e ss.mm.ii.).

5. Coinvolgimento di Società controllate, partecipate e rapporti con i fornitori

La presente policy deve essere formalmente trasmessa, a cura del Responsabile dell'*Area Sicurezza Informatica*, e sottoscritta per presa visione da tutte le società controllate dall'Autorità di Sistema Portuale del Mare Adriatico Orientale.

Per le società partecipate, invece, l'Autorità di Sistema Portuale del Mare Adriatico Orientale promuove l'adozione di analoghe linee guida interne da adottare formalmente all'interno dei propri ordinamenti regolamentari, nel rispetto delle specifiche competenze.

Il Responsabile dell'*Area Sicurezza Informatica* si adopererà, a tutti i livelli necessari, affinché i fornitori di servizi digitali all'Autorità di Sistema Portuale del Mare Adriatico:

- Sottoscrivano nei nuovi contratti apposite clausole contrattuali e/o accordi di riservatezza (NDA) che vietino la divulgazione di informazioni relative al sistema di sicurezza informatica

dell'Autorità di Sistema Portuale del Mare Adriatico Orientale, inclusi dettagli sugli attacchi, sulla loro natura e sulle conseguenze.

- Sottoscrivano specifiche clausole contrattuali integrative dei contratti già attualmente in vigore.
- Rispettino le clausole contrattuali specifiche relative alla sicurezza informatica, redatte per garantire un elevato livello di protezione.
- Sottoscrivano, per presa visione e accettazione, le seguenti linee guida, con l'obbligo di rispettarne i principi e le direttive.

6. Sanzioni e Tutela legale

L'Autorità di Sistema Portuale del Mare Adriatico Orientale adotterà tutte le misure legali necessarie per tutelarsi contro la diffusione di informazioni non autorizzate o false relative a eventi di cybersecurity.

I dipendenti dell'Autorità di Sistema Portuale del Mare Adriatico Orientale, così come previsto dall'art. 13, comma 3, del Codice di Comportamento "*rispettano il segreto d'ufficio e mantengono riservate le notizie e le informazioni apprese nell'ambito dell'attività svolta*" con la conseguenza che una eventuale violazione di tale articolo "*è fonte di responsabilità disciplinare accertata all'esito del procedimento disciplinare, nel rispetto dei principi di gradualità e proporzionalità delle sanzioni*" (cfr. art. 22, comma 1, del Codice di Comportamento)

7. Entrata in vigore e pubblicazione sul sito istituzionale dell'Autorità di Sistema Portuale del Mare Adriatico Orientale

La presente policy, è pubblicata sul sito istituzionale dell'Autorità di Sistema Portuale del Mare Adriatico Orientale per garantire la massima trasparenza. Eventuali aggiornamenti o modifiche saranno tempestivamente comunicati e resi disponibili.

La presente policy entra in vigore a partire dalla data di pubblicazione e rimarrà valida fino a successive modifiche, che verranno pubblicate sul sito istituzionale dell'Autorità di Sistema Portuale del Mare Adriatico Orientale.

Trieste, data della firma digitale

VITTORIO
TORBIANELLI
26.02.2025
09:36:15 CET

Il Commissario Straordinario
Vittorio Alberto Torbianelli