m_inf.A651153.REGISTRO UFFICIALE.U.0171227.16-12-2025.h.07:56

*Roma, data del protocollo informatico*

Ministero delle infrastrutture e dei trasporti
Comando generale
del Corpo delle Capitanerie di porto
Guardia costiera
---
Reparto VI
Sicurezza della Navigazione e Marittima

Ministero delle infrastrutture e dei trasporti
Organo Centrale di Sicurezza
Autorità NIS Settore Trasporti

Circolare Titolo: Sicurezza della Navigazione
Serie Generale n. 177/2025

*Argomento:* *Maritime Cyber Risk***.** Aggiornamento delle misure di sicurezza per le navi nazionali, le società di gestione ISM (Company ISM) e i gestori di impianti portuali.

*Riferimento: Circolare Titolo: Sicurezza della Navigazione - Serie Generale n. 155/2019, recante "Cyber risk management".*

Negli ultimi anni, il settore dei trasporti marittimi ha attraversato, e sta attraversando, una profonda trasformazione, caratterizzata da un crescente impiego di tecnologie digitali e di sistemi automatizzati destinati alla gestione della navigazione, della logistica e delle operazioni portuali; tale evoluzione, pur apportando significativi benefici in termini di efficienza operativa e competitività, ha contestualmente ampliato la superficie di esposizione a minacce informatiche, introducendo nuove vulnerabilità a carico dell'intera filiera marittima.

L'adozione diffusa di sistemi digitali quali *Electronic Chart Display and Information System* (ECDIS), *Automatic Identification System* (AIS), *Global Maritime Distress and Safety System* (GMDSS), nonché delle piattaforme informatiche a supporto delle operazioni portuali, ha infatti incrementato l'efficacia dei processi, ma ha parallelamente creato nuove opportunità di sfruttamento da parte di attori malevoli.

Alla luce di tali considerazioni, la gestione della sicurezza informatica costituisce oggi un elemento imprescindibile per la protezione dei dati, dei sistemi e delle infrastrutture critiche, nonché un fattore determinante per la tutela della sicurezza marittima (nelle accezioni di *safety* e s*ecurity).*

Essa deve quindi essere considerata non più come un elemento accessorio della gestione marittima, bensì una componente strategica della sicurezza nazionale, economica e ambientale e, pertanto, una regolamentazione della *cybersecurity* è condizione imprescindibile per assicurare la resilienza del settore dei trasporti marittimi, oggi esposto a minacce informatiche sempre più sofisticate e persistenti.

Alla luce dei più recenti sviluppi tecnologici, dell'esperienza maturata nell'applicazione delle disposizioni vigenti e delle nuove linee guida IMO nel frattempo pubblicate, questa Amministrazione di bandiera, Autorità Competente e Punto di Contatto Nazionale per l'attuazione, il controllo e l'informazione sull'applicazione delle misure di sicurezza marittima[1], ha ravvisato la necessità di aggiornare i contenuti della Circolare in riferimento.

A tal fine, con il condiviso parere del Gruppo di lavoro per la sicurezza della navigazione istituito presso questo Reparto – ampliato alla partecipazione di: Autorità NIS – Settore Trasporti, Agenzia per la Cybersicurezza Nazionale, Assiterminal, Assoporti, Assocostieri, Uniport, Assologistica, ALIS e Confetra – sono state predisposte le allegate istruzioni. Le stesse sono state presentate al Comitato Interministeriale per la sicurezza dei trasporti marittimi e dei porti (CISM) nella seduta plenaria del 29 ottobre 2025 e successivamente illustrate nel corso del 100° meeting del *Committee for Maritime Security*, tenutosi presso EMSA il 9 dicembre u.s., con l'obiettivo di condividere il percorso intrapreso dall'Italia per la piena attuazione degli indirizzi IMO e per contribuire all'allineamento del quadro di sicurezza marittima alla Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 (NIS2), relativa a misure per un livello comune elevato di cybersicurezza nell'Unione, recepita con D.Lgs. 4 settembre 2024, n. 138.

Quanto sopra, fermo restando le ulteriori disposizioni che saranno impartite dalla Autorità Nazionale Competente NIS (ACN) alle Società/Organi di gestione dei porti che rientrano nell'Allegato I "Settori ad alta criticità", punto c), "Trasporto per vie d'acqua", del sopracitato D. Lgs. 4 settembre 2024, n.138.

La presente Circolare, salvo diversa indicazione contenuta nell'annesso, entra in vigore il **1° novembre 2026** e, a decorrere dalla medesima data, abroga la Circolare richiamata in riferimento.

La Circolare viene inviata ai soggetti cui compete la puntuale implementazione delle misure in essa contenute ed è pubblicata sul sito istituzionale del Corpo delle Capitanerie di porto – Guardia Costiera, Sezione "Sicurezza della Navigazione", ai fini di pubblicità legale ai sensi dell'articolo 32 della Legge 18 giugno 2009, n. 69.

IL CAPO REPARTO VI
Contrammiraglio (CP)
Francesco CIMMINO
(documento sottoscritto con firma digitale, ai sensi del D.lvo 82/2005 n.21)

*Firmato Digitalmente da/Signed by:*
**FRANCESCO CIMMINO**

*In Data/On Date:*
**lunedì 15 dicembre 2025 19:44:05**

IL CAPO DELL'ORGANO
CENTRALE DI SICUREZZA
Direttore Generale
Dott. Costantino FIORILLO
(documento sottoscritto con firma digitale, ai sensi del D.lvo 82/2005 n.21)

Firmato digitalmente da
**Costantino Fiorillo**
CN = Costantino Fiorillo
C = IT

[1] *Reg. n. 725/2004, artt. 4 e 9 e Dir. 2005/65/CE, art. 12, entrambe del Parlamento Europeo e del Consiglio.*

| INDIRIZZI PER COMPETENZA |
|---|
| ➢ **DIREZIONI MARITTIME – TUTTE**<br>➢ **CAPITANERIE DI PORTO - TUTTE**<br>➢ **UFFICI CIRCONDARIALI MARITTIMI – TUTTI** (*p.p. Uffici marittimi dipendenti*) |
| ➢ **MINISTERO DELLE INFRASTRUTTURE E DEI TRASPORTI**<br>Gabinetto del Sig. Ministro<br>segr.capogabinetto@mit.gov.it<br><br>Dipartimento per i trasporti e la navigazione<br>dip.trasporti@pec.mit.gov.it<br><br>Direzione generale per il mare, il trasporto marittimo e per vie d'acqua interne<br>dg.tm@pec.mit.gov.it<br><br>Direzione generale per i porti, la logistica e l'intermodalità<br>dg.sli@pec.mit.gov.it |
| ➢ **AUTORITÀ NIS – SETTORE TRASPORTI**<br>autorita.nis@mit.gov.it autorita.nis@pec.mit.gov.it |
| ➢ **ASSITERMINAL**<br>info@assiterminal.it |
| ➢ **ASSOPORTI**<br>assoporti@pec.assoporti.it |
| ➢ **ASSOCOSTIERI**<br>assocostieri@assocostieri.it |
| ➢ **UNIPORT**<br>uniport@pec.associazione-uniport.org |
| ➢ **ASSOLOGISTICA**<br>roma@assologistica.it |
| ➢ **ALIS**<br>info@alis.it |
| ➢ **CONFETRA**<br>confetra@confetra.com confetra@legalmail.it |
| ➢ **CONFITARMA**<br>confitarma@pec.it direzione@confitarma.it |
| ➢ **ASSARMATORI**<br>segreteria@assarmatori.eu |
| ➢ **COMPAGNIE NON ASSOCIATE** *(via e-mail, a cura del Reparto VI - Ufficio 2)* |
| **INDIRIZZI PER CONOSCENZA** |
| ➢ **MARICOGECAP**:<br>- Reparto II<br>- Reparto III<br>- Reparto VII<br>- Ufficio dell'Assistente del Comandante generale<br>- Ufficio dell'Assistente del Vice Comandante generale |
| ➢ **STATO MAGGIORE MARINA** |
| ➢ **AGENZIA PER LA CYBERSICUREZZA NAZIONALE**<br>autorita.nis@acn.gov.it |
| ➢ **RINA SERVICES S.p.A.**<br>rina.maricogecap@legalmail.it rina.services.spa@legalmail.it |
| ➢ **BUREAU VERITAS SA**<br>bvmarine_offshore@legalmail.it bvitalia@legalmail.it |
| ➢ **DNV AS**<br>dnvitalia@legalmail.it detnorskeveritasitalia@legalmail.it |
| ➢ **LLOYD'S REGISTER GROUP LTD**<br>lritalia@legalmail.it |
| ➢ **AMERICAN BUREAU OF SHIPPING**<br>absitaly@pcert.postecert.it |
| ➢ Accademia Navale Livorno - Gruppo Insegnamento CP<br>➢ Mariscuola Taranto - Gruppo Insegnamento NP<br>➢ Mariscuola La Maddalena - Gruppo Insegnamento NP<br>➢ Direzione Marittima di Genova - Centro di Formazione Specialistico "CA (CP) Antonio De Rubertis"<br>➢ Direzione Marittima di Livorno - Centro di Formazione Specialistico "M.A.V.M. Capitano di Porto Bruno Gregoretti" |

*Ministero delle infrastrutture e dei trasporti*

---

Comando generale del Corpo delle Capitanerie di porto

Guardia costiera

Reparto VI - Sicurezza della Navigazione e Marittima

---

Organo Centrale di Sicurezza

Autorità NIS – Settore Trasporti

# Circolare Titolo: Sicurezza della Navigazione Serie Generale n.177/2025

## *Maritime Cyber Risk*.

## Aggiornamento delle misure di sicurezza per le navi nazionali, le società di gestione ISM (*Company*) e i gestori di impianti portuali (*port facility*)

# INDICE

**1. Introduzione pag. 3**
**2. Contesto pag. 4**
**2.1 Applicazione pag. 4**
**2.2 Definizioni chiave pag. 5**
**2.3 Documentazione del CBS pag. 6**
**2.4 Categorie dei sistemi CBS pag. 6**
**2.5 Tipi di minacce informatiche pag. 6**
**2.6 Attori delle minacce pag. 7**
**3. Sicurezza informatica pag. 8**
**4. Il rischio pag.10**
**5. Gestione del rischio informatico pag.12**
**5.1 Company/navi pag.13**
**5.2 Procedure del Sistema di gestione della sicurezza (SMS) e del Piano di sicurezza della nave (SSP) pag.17**
**5.3 MASS pag.18**
**5.4 Facility/Port facility pag.19**
**5.5 Cyber risk Assessment pag.23**
**6. Porti pag.25**
**7. Responsabilità e Formazione pag.25**
**8. Drill ed exercise pag.28**
**9. Audit interni pag.28**
**10. Segnalazioni pag.29**
**11. Ispezioni di controllo dello Stato di approdo pag.29**
**12. Norme di riferimento pag.30**

**Allegato A pag.31**

## 1. Introduzione

La gestione del rischio, nel mondo dello shipping, è stata tradizionalmente e prevalentemente focalizzata su operazioni tradizionali, ma la sempre maggiore dipendenza dei sistemi di bordo dalla digitalizzazione, dall'integrazione fra equipaggiamenti, dall'automazione e dai sistemi basati sulla rete di trasmissione dati ha, però, evidenziato una crescente necessità per la gestione dei rischi informatici anche nel settore marittimo.

Le vulnerabilità create dall'accesso, interconnessione o messa in rete di questi sistemi e i relativi, concreti rischi informatici evidenziano la necessità di un approccio strutturato e sistematico alla gestione del rischio cyber.

Tale approccio deve essere coerente con gli indirizzi adottati in sede IMO, come riportato nella MSC-FAL.1/Circ.3/Rev.3[1] e nelle Unified Requirements IACS per la cyber resilience (UR E26)[2], nonché integrato con i più recenti sviluppi del quadro normativo unionale e nazionale in materia di cybersicurezza.

In tale contesto, particolare attenzione deve essere rivolta ai sistemi e alle funzioni tecniche critiche, la cui compromissione potrebbe incidere direttamente sulla sicurezza della nave, delle persone e dell'ambiente, tra cui, a titolo non esaustivo:

- ✓ Sistemi del ponte di comando;
- ✓ Sistemi di governo;
- ✓ Sistemi di rilevazione ed estinzione incendio;
- ✓ Watertight integrity e flooding detection;
- ✓ Luce (normale/emergenza, low location, luci di navigazione etc.);
- ✓ Emergency shutdown;
- ✓ Sistemi di generazione e distribuzione dell'energia elettrica;
- ✓ Sistemi di comunicazione interna;
- ✓ Sistemi di movimentazione e gestione del carico, del bunkeraggio, della lubrificazione, della zavorra ecc;
- ✓ Sistemi di propulsione, gestione del carburante e dei macchinari e controllo della potenza;
- ✓ Sistemi di security, controllo degli accessi e sorveglianza;
- ✓ Sistemi di gestione e assistenza ai passeggeri;
- ✓ Sistemi amministrativi di gestione e di benessere dell'equipaggio;
- ✓ Reti pubbliche rivolte ai passeggeri;
- ✓ Sistemi amministrativi e di benessere dell'equipaggio;
- ✓ Interfaccia nave-porto; e
- ✓ Sistemi integrati nave-terra (es. comunicazione e sistemi di controllo remoto per MASS).

Parallelamente, in coerenza con un approccio basato sul rischio e con i principi di gestione della cybersicurezza riconosciuti a livello internazionale ed europeo, la protezione dei suddetti sistemi deve essere supportata da un adeguato assetto organizzativo, procedurale e gestionale, che comprenda, in particolare:

- ✓ **Governance e responsabilità**: definizione chiara di ruoli, responsabilità e procedure in materia di *cybersecurity*, integrate nel Safety Management System (SMS) della compagnia, in linea con l'ISM Code;
- ✓ **Identificazione dei rischi**: mappatura dei sistemi critici di bordo e a terra (OT e IT), delle interdipendenze tra essi e delle potenziali minacce e vulnerabilità informatiche;

[1] *MSC-FAL.1/Circ.3/Rev.3 4 April 2025 – Guidelines on maritime cyber risk management*
[2] *Guidelines for cyber resilience of ships*

- ✓ **Protezione dei sistemi**: adozione di misure tecniche e organizzative adeguate, tra cui il controllo degli accessi, la gestione delle credenziali, la segmentazione delle reti, l'aggiornamento e la gestione sicura del software e dell'hardware;
- ✓ **Gestione delle interconnessioni e della *supply chain***: valutazione dei rischi derivanti dall'integrazione tra sistemi di bordo, sistemi di terra e fornitori esterni, inclusi manutentori, *service provider* e produttori di apparecchiature;
- ✓ **Consapevolezza e formazione del personale**: programmi di *training* e sensibilizzazione dell'equipaggio e del personale di terra, al fine di ridurre il rischio umano, riconosciuto come uno dei principali vettori di attacco;
- ✓ **Rilevamento degli incidenti**: capacità di individuare tempestivamente eventi anomali o attacchi informatici, attraverso procedure di monitoraggio e segnalazione;
- ✓ **Risposta e mitigazione**: predisposizione di piani di risposta agli incidenti *cyber*, volti a limitare l'impatto operativo, garantire la continuità delle operazioni e preservare la *safety* e la *security* della nave;
- ✓ **Ripristino e resilienza**: misure per il recupero sicuro dei sistemi e dei dati, incluse procedure di backup e *disaster recovery*, al fine di ripristinare rapidamente le funzionalità essenziali.

Alla luce di quanto sopra, la cybersicurezza deve essere considerata parte integrante della gestione complessiva della sicurezza marittima e non un elemento accessorio, richiedendo un approccio coordinato e coerente tra navi, società di gestione e impianti portuali, in linea con il quadro normativo internazionale, unionale e nazionale di riferimento.

## 2. Contesto

Le tecnologie informatiche, quindi, sono diventate essenziali per il funzionamento e la gestione di numerosi sistemi critici per la sicurezza della navigazione - nell'accezione più ampia del termine - e la protezione dell'ambiente marino. Appare, altresì, necessario incentivare ulteriormente lo scambio strutturato di informazioni e best practices tra Autorità competenti, Enti gestori e infrastrutture portuali, anche mediante l'utilizzo di piattaforme dedicate o attraverso l'organizzazione di tavoli tecnici periodici, al fine di potenziare in maniera coordinata il sistema di cybersecurity dell'intero comparto. Le misure previste dalla presente circolare sono applicate secondo criteri di proporzionalità rispetto alla natura, dimensione e complessità della Company, della nave e della Port Facility, nonché alla tipologia e criticità dei sistemi informatici e cyber-fisici (CBS). Pertanto, per i soggetti NIS e per i soggetti non NIS, eventuali richieste di adattamento o semplificazione motivate da ridotta complessità organizzativa o tecnologica devono essere sottoposte al Comando Generale - VI Reparto e all'Autorità NIS - Settore Trasporti che valutano la coerenza con i requisiti minimi di sicurezza e con le normative vigenti.

### 2.1 Applicazione

La presente circolare è destinata, principalmente, a tutte le organizzazioni del settore marittimo (navi, società di gestione/*Company* e impianti portuali/*Facility*) a cui si applica la normativa internazionale, unionale, nazionale in materia di security, Direttiva UE 2022/2555 e Decreto Legislativo n° 138/2024 (d'ora in poi NIS 2) e sono redatte per supportare l'adozione di buone pratiche per la gestione della sicurezza e della protezione nel settore informatico.

A tal fine, l'approccio delineato nel presente allegato è coerente con i principali modelli e standard di riferimento riconosciuti a livello nazionale e internazionale in materia di gestione del rischio *cyber*, quali, a titolo esemplificativo e non esaustivo, il NIST Cybersecurity Framework, la norma ISO/IEC 27001, nonché il Framework Nazionale per la Cybersecurity e la Data Protection e la UNI/PdR 174:2025, quale prassi di riferimento a supporto dei soggetti NIS, anche certificati ISO/IEC 27001.

2.2 Definizioni chiave

a. Sistemi basati su computer (Computer Based System - CBS): Si intende un dispositivo elettronico programmabile, o un insieme interoperabile di dispositivi elettronici programmabili, organizzati per raggiungere uno o più scopi specifici, quali la raccolta, l'elaborazione, la conservazione, l'utilizzo, la condivisione, la diffusione o la dismissione di informazioni. I CBS a bordo comprendono sia sistemi IT (Information Technology) che OT (Operational Technology). Un CBS può consistere in una combinazione di sottosistemi collegati tramite una rete. I CBS di bordo possono essere connessi, direttamente o tramite mezzi di comunicazione pubblici (ad esempio Internet), ai CBS a terra, ai CBS di altre navi e/o ad altre infrastrutture.
b. Incidente informatico (Cyber incident o cyberattacco): Si intende un evento o una sequenza di eventi che comportano, o possono comportare, conseguenze negative per un CBS o per le informazioni che esso elabora, archivia o trasmette, e che possono richiedere un'azione di risposta volta a mitigarne le conseguenze. Più in generale l'evidenza di eventi che comportano la perdita di riservatezza o di integrità di dati digitali di sua proprietà, o sui quali esercita il controllo, anche parziale, nonché della violazione dei livelli di servizio attesi dalle proprie attività deve essere considerata incidente informatico ai fini dell'attivazione delle misure di gestione e risposta.
c. Gestione del rischio informatico (Cyber risk management): processo di identificazione, analisi, valutazione e comunicazione di un rischio connesso al cyberspazio, nonché di accettazione, eliminazione, trasferimento o trattamento del medesimo fino a un livello ritenuto accettabile, tenendo conto dei costi e dei benefici delle azioni intraprese dalle parti interessate.
d. Tecnologia dell'informazione (IT - Information Technology): Si riferisce ai CBS orientati all'uso dei dati come informazione, comprendendo software, hardware e tecnologie di comunicazione (ad esempio, informazioni commerciali o dati relativi all'equipaggio, come stipendi, certificazioni, ecc.).
e. Tecnologia operativa (OT - Operational Technology): Si riferisce ai CBS orientati all'uso dei dati per controllare o monitorare processi fisici (ad esempio, i livelli di temperatura dell'olio del motore principale, che vengono inviati alla sala di controllo).
f. Sicurezza informatica: l'insieme delle attività necessarie per proteggere la rete e i sistemi informativi, gli utenti di tali sistemi e altre persone interessate dalle minacce informatiche, così come definito dall'articolo 2, punto 1), del regolamento (UE) 2019/881.

g. Resilienza: caratteristica che fornisce all'equipaggio, alle navi e agli impianti portuali le capacità per affrontare efficacemente gli incidenti informatici che si verificano sui sistemi informatici di bordo, che contribuiscono a far funzionare e mantenere la nave in condizioni di sicurezza.

h. Cyber Company Officer (CyCO) - Cyber Security Officer (CySO) - Cyber Port Facilities Security Officer (CyPFSO): soggetti individuati dalla *Company*/responsabile dell'impianto portuale - anche nell'ambito dell'assetto organizzativo aziendale/personale di bordo esistente - quali responsabili della funzione di Protezione *Cyber Security*.

Per tutte le altre definizioni, si rimanda alla MSC-FAL.1/Circ.3/Rev.3, all' IACS UR E26/27 ed ai documenti dell'Agenzia per la cybersicurezza nazionale ACN[3] denominati:

- La tassonomia cyber dell'ACN;
- Guida alla notifica degli incidenti al CSIRT Italia;
- Glossario - ACN -;
- Misure di sicurezza di base per i soggetti importanti/essenziali.

2.3 Documentazione del CBS

Per le navi nuove, con impostazione chiglia a far data dalla emissione della presente circolare, a valle dell'identificazione dei sistemi che rientrano nella definizione di CBS, la relativa documentazione tecnica deve essere fornita alla *Company* ed alla *Facility* dal fornitore, secondo le previsioni della UR E27 "*Cyber resilience of on-board systems and equipment*", nella sua versione aggiornata.

Per le navi esistenti, la conformità - secondo criteri proporzionati e coerenti con le reali caratteristiche dei sistemi OT installati - è verificata e dichiarata dall'Organismo nave.

2.4 Categorie di sistemi CBS

Le categorie di sistemi CBS - come anche identificato nella IACS UR E22 - possono essere di tre tipi (I, II e III):

I. Sistemi il cui guasto non comporta situazioni di pericolo per l'incolumità delle persone, per la sicurezza della *Company/Facility*, della nave/impianto portuale ovvero una minaccia per l'ambiente;

II. Sistemi il cui guasto potrebbe eventualmente portare a situazioni di pericolo per l'incolumità delle persone, per la sicurezza della *Company/Facility*, della nave/impianto portuale ovvero una minaccia per l'ambiente;

III. Sistemi il cui guasto potrebbe portare ad una immediata situazione di pericolo per l'incolumità delle persone, per la sicurezza della *Company/Facility*, della nave/impianto portuale ovvero una minaccia per l'ambiente.

2.5 Tipi di attacchi informatici

In generale, esistono due categorie di attacchi informatici che possono colpire la *Company/Facility* e le navi/impianti portuali:

1. Attacchi non mirati, in cui i sistemi e i dati di una *Company/Facility* o di una nave/impianto portuale sono uno dei tanti potenziali obiettivi. Esempi e tecniche che possono essere utilizzati includono:

[3] Disponibili sul portale www.acn.gov.it

- ✓ i software dannosi (cd. *Malware*);
- ✓ la creazione di un sito Web falso o la compromissione di un sito web autentico per sfruttare visitatori ignari (cd. *Water holing*);
- ✓ Ricerca casuale di vulnerabilità che potrebbero essere sfruttate su Internet (*Scanning*);
- ✓ dirottamento URL o URL falso; si basa su errori quali errori di battitura commessi dagli utenti di Internet durante l'immissione dell'indirizzo di un sito web in un browser. Se un utente inserisse accidentalmente un indirizzo di sito web errato, potrebbe essere indirizzato a un sito web alternativo e spesso dannoso (*Typosquatting*);

2. Attacchi mirati, in cui l'obiettivo previsto o uno di più obiettivi possibili sono i sistemi e i dati di una *Company/Facility* e di una nave/impianto portuale.
   Esempi e tecniche, non esaustive, che possono essere utilizzate includono:
   - ✓ potenziali aggressori informatici per manipolare personale interno all'ambiente lavorativo, affinché infrangano le procedure di sicurezza, normalmente, ma non esclusivamente, attraverso l'interazione tramite i social media (*social engineering*);
   - ✓ attacco attraverso la prova di molte password, con l'obiettivo di identificare quella corretta (*brute force*);
   - ✓ utilizzo di credenziali e password precedentemente compromesse o specifiche di uso comune, per tentare l'accesso non autorizzato a un sistema ovvero ad una applicazione (*credential stuffing*);
   - ✓ un attacco che prende il controllo di più computer e/o server (*denial of service*);
   - ✓ invio di e-mail a un gran numero di potenziali obiettivi, chiedendo particolari informazioni sensibili o riservate. L'e-mail può anche contenere un allegato dannoso o richiedere a una persona di visitare un sito web falso utilizzando un collegamento ipertestuale incluso nell'e-mail (*phishing*);
   - ✓ invio di e-mail personali, spesso contenenti software dannoso o collegamenti che scaricano automaticamente software dannoso (*Spear-phishing*);
   - ✓ attacco ad una *Company/Facility* o ad una nave/impianto portuale, con la compromissione del sistema o dell'equipaggiamento, software o servizi di supporto (*subverting the supply chain*).

   Altri metodi di attacco informatico si stanno evolvendo; ad esempio: sostituirsi ad un dipendente di una determinata società (Es. spedizioni) per ottenere informazioni da utilizzare per un ulteriore attacco. Il numero potenziale e la sofisticazione degli strumenti e delle tecniche utilizzati negli attacchi informatici continueranno ad evolversi, legati anche all'ingegno delle organizzazioni e degli individui che li sviluppano.

2.6 Attori delle minacce

Organizzazioni e individui possono costituire una minaccia intenzionale o anche involontaria alla sicurezza dell'equipaggio, dell'ambiente, della nave, della *Company* o della *Facility*. Di seguito si riportano, in modo non esaustivo, alcuni esempi di autori di minacce e le loro possibili motivazioni e obiettivi.

Diverso può essere il grado di competenze e la capacità di risorse nel condurre l'attività al fine di minacciare potenzialmente la sicurezza:

| Attori | Motivazione |
|---|---|
| Attori accidentali | Nessun movente doloso con danni involontari causati per mancanza di conoscenza o disattenzione (es. USB infette nei sistemi IT o OT). |
| Attivisti o dipendenti scontenti | ▪ vendetta<br>▪ interruzione delle operazioni<br>▪ l'attenzione dei media<br>▪ danno reputazionale |
| Criminali | ▪ guadagno finanziario<br>▪ spionaggio commerciale<br>▪ spionaggio industriale |
| Opportunisti | ▪ la sfida<br>▪ guadagno di reputazione<br>▪ guadagno finanziario |
| Organizzazioni sponsorizzate o terroristi | ▪ guadagno politico/ideologico, ad esempio disgregazione (in)controllata delle economie e delle infrastrutture nazionali critiche<br>▪ spionaggio<br>▪ guadagno finanziario<br>▪ spionaggio commerciale<br>▪ spionaggio industriale<br>▪ guadagno commerciale |

## 3. Sicurezza informatica

Le misure di sicurezza per i sistemi essenziali non devono influire negativamente sulla disponibilità dei sistemi. L'implementazione delle misure di protezione non deve causare la perdita delle funzioni di sicurezza, di controllo e monitoraggio o la perdita di altre caratteristiche che potrebbero avere conseguenze sulla affidabilità del sistema. Il sistema deve essere adeguatamente progettato per consentire alla *Company/Facility* e alla nave/impianto portuale di continuare le operazioni garantendo, al contempo, la riservatezza, l'integrità e la disponibilità dei dati necessari per la sicurezza dei suoi sistemi, con particolare riferimento a quelli essenziali e di emergenza e comunque necessari per la sicurezza della nave, delle persone e del carico. Ai fini della presente circolare, per *sistemi essenziali* e *sistemi di emergenza* si intendono i sistemi IT/OT la cui compromissione può avere impatti significativi sulla sicurezza della navigazione, sulla protezione dell'ambiente marino, sulla continuità operativa della nave o della Port Facility. In coerenza con gli standard internazionali, rientrano in tali categorie i sistemi classificati come *Essential* o *Important* secondo le IACS UR E26/E27 e le pertinenti disposizioni IMO (SOLAS, MSC-FAL.1/Circ.3/rev.3).

Gli incidenti informatici possono verificarsi come risultato, ad esempio, di:

- un incidente di sicurezza informatica, che influisce sulla disponibilità e sull'integrità di OT; ad esempio, la corruzione dei dati cartografici conservati in un sistema di visualizzazione e informazione di carte elettroniche (ECDIS);
- un malfunzionamento non intenzionale del sistema verificatosi nel corso delle attività di manutenzione e aggiornamento del software, anche mediante l'utilizzo di supporti di memorizzazione esterni potenzialmente compromessi;
- perdita o manipolazione dei dati dei sensori esterni, fondamentali per il funzionamento di una nave e che potrebbero mettere a rischio la sicurezza delle persone e della nave così come la protezione dell'ambiente;
- guasto di un sistema a causa di "crash del software" e/o "bug";
- interazione dell'equipaggio con tentativi di *phishing*, che è il vettore di attacco più comune da parte di autori di minacce e che potrebbe portare alla perdita di dati sensibili o all'introduzione di malware nei sistemi di bordo.

Inoltre, nell'industria marittima una serie di caratteristiche influiscono sulla sua vulnerabilità agli incidenti informatici. Queste includono anche:

- il coinvolgimento di più soggetti, anche appartenenti alla catena di fornitura, nella gestione e manutenzione delle infrastrutture IT e OT e delle reti, con conseguente potenziale complessità nell'individuazione delle relative responsabilità;
- utilizzo di sistemi IT e OT non più supportati e/o che si basano su sistemi operativi obsoleti;
- utilizzo di sistemi OT a cui non è possibile applicare aggiornamenti dei sistemi o eseguire antivirus a causa di problemi di omologazione;
- navi che si interfacciano online con le parti di terra e altre parti della catena dei trasporti e di approvvigionamento globale;
- apparecchiature della nave monitorate e accessibili a distanza, ad esempio da parte dei produttori o dei fornitori di supporto o degli Uffici tecnici e operativi delle Società di gestione;
- la condivisione di informazioni aziendali critiche e dati sensibili dal punto di vista commerciale con fornitori di servizi a terra, compresi terminal marittimi e operatori portuali e, ove applicabile, autorità;
- la presenza e l'impiego di sistemi critici a controllo informatico che, in assenza degli aggiornamenti correttivi più recenti o di adeguate misure di protezione, possono compromettere la sicurezza della nave e la tutela dell'ambiente;
- una cultura di gestione del rischio informatico che ha ancora potenziale di miglioramento, ad esempio attraverso una formazione più mirata, l'esecuzione di esercitazioni e il chiarimento rispetto a ruoli e responsabilità;
- sistema di automazione che, spesso, è composto da più sottosistemi di numerosi fornitori che vengono integrati dai cantieri navali con ipotetica poca o non sufficiente attenzione ai problemi informatici;
- la carenza o l'inadeguatezza della formazione del personale in materia di sicurezza informatica può costituire un fattore di rischio, contribuendo all'insorgenza di incidenti cibernetici o agevolandone la realizzazione, in quanto limita la capacità di prevenire, rilevare e gestire efficacemente le minacce.

## 4. Il rischio

Per proteggere la catena di fornitura marittima globale iperconnessa, che dipende dallo scambio efficiente e affidabile di dati e dai sistemi OT che consentono operazioni efficienti, le *Company* e i gestori di impianti portuali devono gestire le operazioni in modo da contenere i rischi informatici entro limiti accettabili[4].

Un rischio informatico è una situazione in cui una minaccia sfrutta una vulnerabilità, che può avere un impatto negativo sulla confidenzialità, sull'integrità e sulla disponibilità dei dati, del sistema o della rete.

Il modello "CIA", di cui alla IAPH-Cybersecurity-Guidelines, include:

- Confidenzialità (*Confidentiality*): assicurare che solo utenti autorizzati possano accedere alle informazioni.
- Integrità (*Integrity*): garantire che i dati non vengano alterati in modo non autorizzato.
- Disponibilità (*Availability*): garantire che i sistemi e i dati siano accessibili quando necessari.

Questo modello è essenziale, seppur non copre, da solo, la sicurezza delle interazioni digitali, specialmente in contesti complessi, come reti distribuite, ambienti cloud o infrastrutture critiche (come la logistica marittima).

Per coprire queste nuove esigenze, sono stati aggiunti nuovi principi che espandono il CIA:

- Autenticazione (*Authentication*): verifica chi sei veramente. Senza autenticazione, confidenzialità e integrità non possono essere garantite.
- Non ripudiabilità (*Non-repudiation*): è la prova dell'avvenuta azione. Un utente non può negare di aver fatto qualcosa.

In particolare:

- <u>Confidenzialità</u>: garantisce che le informazioni o i sistemi siano accessibili solo agli utenti autorizzati. Nel salvaguardare la riservatezza dei propri dati, una *Company/Facility* o una nave/impianto portuale può raggruppare le informazioni in base alla sensibilità e all'accesso limitato, sia digitale che fisico. Le tattiche per garantire la riservatezza includono autorizzazioni per i file, crittografia ed elenchi di controllo degli accessi.

  Le *Company/Facility* e le navi/impianti portuali creano, elaborano, ricevono, gestiscono, archiviano e trasferiscono grandi volumi di dati, che includono ma non sono limitati a transazioni di pagamento, attività di servizio, dati, manifesti del carico e dettagli bancari. Gli autori delle minacce informatiche potrebbero utilizzare questi dati per guadagni illeciti che potrebbero avere un impatto sull'organizzazione in termini di:

  - Reputazione, rilasciando pubblicamente la prova dell'attacco o una serie di informazioni sensibili.
  - Competitività, vendendo informazioni a un concorrente.
  - Conformità normativa, nel caso in cui l'aggressore pubblichi/venda parte/tutti i dati e contengano informazioni sensibili, l'organizzazione

[4] È definito rischio "accettabile" il risultato di un processo di analisi e valutazione formalizzato, con criteri oggettivi e condivisi, secondo standard internazionali (es. ISO 31000).

potrebbe essere ritenuta colpevole di violazione delle leggi sulla privacy, come, ad esempio, con la violazione del Regolamento generale sulla protezione dei dati dell'Unione Europea (GDPR).

- Integrità: si riferisce alla conservazione delle informazioni o dell'accuratezza dei sistemi per la protezione dei dati da modifiche o cancellazioni non autorizzate. Le violazioni dell'integrità possono minare la fiducia e considerare, quindi, beni, clienti o finanze non più affidabili. *Company/Facility* e navi/impianti portuali devono utilizzare il controllo della versione o i backup di sistema per garantire che le modifiche non autorizzate ai dati possano diventare definitive.
  Un attore ostile nel dominio cibernetico potrebbe compromettere l'integrità, la disponibilità o la riservatezza delle informazioni, con potenziali impatti su:
  - Aspetti economico-finanziari, mediante alterazione di dati o processi al fine di ottenere indebiti vantaggi economici o causare perdite.
  - Adempimenti normativi e regolamentari, attraverso la manipolazione di dati o documentazione per eludere obblighi legali o presentare informazioni non veritiere.
  - Sicurezza e operatività dei sistemi, includendo la modifica o la creazione non autorizzata di credenziali, la mascheratura di attività illecite o la compromissione di funzionalità critiche.
- Disponibilità: La disponibilità è la proprietà dell'informazione e dei sistemi digitali di essere accessibili e utilizzabili al momento della richiesta da parte di un soggetto autorizzato. Le minacce informatiche mirate alla disponibilità possono causare interruzioni critiche del sistema, inclusi i sistemi operativi dei terminali, le operazioni abilitate Wi-Fi, i sistemi negli uffici e le comunicazioni abilitate alla rete, come i telefoni basati su IP. Per proteggerne la disponibilità, le *Company/Facility* e le navi/impianti portuali possono disporre di una serie di ridondanze (sistemi, comunicazioni e persino backup di dati). Minando la disponibilità dei dati o di un sistema, gli autori delle minacce informatiche possono creare impatti come:
  - mancato rispetto dell'interfaccia unica marittima nazionale (se i dati amministrativi non possono essere più scambiati).
  - Ritardare o interrompere lo scambio di dati operativi per il coordinamento del traffico, il carico o altri processi operativi.
  - Fornitura dei dati storici/statistici necessari per le indagini sui sinistri marittimi.
  - Ritardare la presentazione dei documenti richiesti (dichiarazioni, fatture…).
  - Compromettere la capacità delle parti interessate di elaborare gli ordini, tracciare il carico, ecc.
  - Effettuare un'interruzione del servizio operativo con conseguente interruzione del lavoro.
- Autenticazione: è fondamentale verificare l'identità di un utente o di un sistema prima di concedere l'accesso a risorse digitali o fisiche. Solo gli utenti verificati possono interagire con dati sensibili (es. dati personali, dati commerciali strategici) o sistemi critici (es. sistemi la cui compromissione può avere impatti rilevanti su *safety, security*, ambiente o operatività). Meccanismi di autenticazione robusti, come l'autenticazione a più fattori (MFA), certificati digitali e token hardware/software, sono essenziali per evitare accessi non autorizzati che potrebbero compromettere la disponibilità, l'integrità o la riservatezza. Una mancata autenticazione efficace può permettere a un attaccante di impersonare

utenti legittimi, aggirare i controlli di sicurezza o introdursi nei sistemi operativi, terminali o comunicazioni.

- Non ripudiabilità: garantisce che un utente o un'entità non possa negare di aver compiuto una determinata azione, come l'invio di un messaggio, l'esecuzione di una transazione o la modifica di dati. Ciò è particolarmente rilevante nella gestione delle responsabilità legali e contrattuali. L'uso di firme digitali, registri di log sicuri e sistemi di audit permette di associare in modo inequivocabile un'azione all'utente che l'ha compiuta, fornendo una prova valida in sede giudiziaria o investigativa. In ambito marittimo e portuale, la non ripudiabilità è cruciale per attribuire la responsabilità in caso di anomalie nei flussi di dati, transazioni fraudolente o accessi non autorizzati.

  La registrazione e la conservazione dei log di accesso e delle attività devono avvenire nel rispetto del Regolamento (UE) 2016/679 (GDPR), del D.Lgs. 196/2003 e s.mm.ii. e dell'articolo 4 della Legge 300/1970, adottando misure tecniche e organizzative adeguate a garantire la minimizzazione dei dati, la limitazione degli accessi, la sicurezza del trattamento e tempi di conservazione proporzionati alle finalità di sicurezza delle informazioni contenute.

## 5. Gestione del rischio informatico

Per gestione del rischio informatico si intende il processo di identificazione, analisi, valutazione e comunicazione di un rischio informatico e di accettazione, impedimento, trasferimento o mitigazione dello stesso a un livello accettabile, considerando i costi e i benefici delle azioni intraprese per le parti interessate.

La gestione del rischio informatico dovrebbe essere parte integrante della cultura della sicurezza e della protezione di una *Company/Facility*/nave/impianto portuale, favorevole al funzionamento sicuro ed efficiente degli stessi ed essere implementata a vari livelli sia a terra che a bordo.

La gestione del rischio informatico deve:

- identificare i ruoli e le responsabilità degli utenti, del personale chiave e del management;
- identificare i sistemi, le risorse e i dati che, se interrotti, potrebbero comportare rischi per le operazioni e la sicurezza della *Company/Facility* e delle navi/impianti portuali;
- implementare misure tecniche e procedurali per proteggersi da un incidente informatico, rilevare tempestivamente gli incidenti e garantire la continuità delle operazioni;
- prevedere un piano di emergenza in base al quale eseguire anche le esercitazioni.

Alcuni aspetti della gestione del rischio informatico possono includere informazioni commercialmente sensibili o riservate, ad esempio la valutazione del rischio informatico e gli inventari hardware e software associati e le mappe di rete.

Le *Company/Facility* e le navi/impianti portuali dovrebbero quindi considerare di proteggere queste informazioni in modo appropriato e, per quanto possibile, gestire le informazioni sensibili nei propri sistemi di gestione.

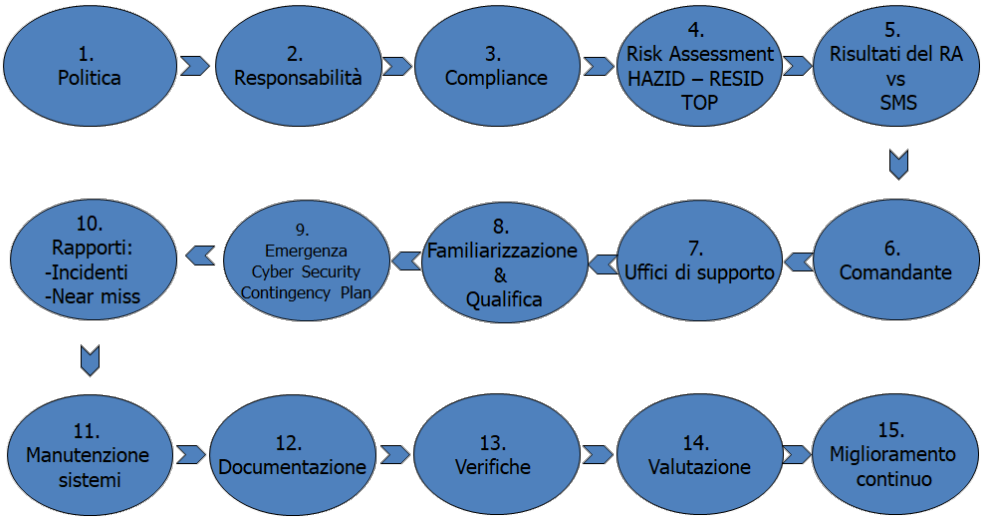
### 5.1 *Company* - Nave

Scopo

Scopo del presente paragrafo è quello di identificare il processo ISM legato alla *cyber security*, fornendo una guida che possa supportare le Società di gestione nella redazione del "*risk assessment*" (punti 4 e 5 del processo ISM), al fine di proteggere i sistemi e le informazioni dalle minacce informatiche.

Quanto sopra con l'obiettivo di adottare tutte le misure per garantire, ai sensi del codice ISM (punto 1 del preambolo), la gestione sicura della nave, la protezione dell'ambiente, la tutela dell'equipaggio e delle persone trasportate.

Processo ISM




1. POLITICA (Codice ISM punto 2.1) - La politica della *Company* deve essere aggiornata (ampliamento dei propri obiettivi di gestione ISM), con l'inserimento degli aspetti di *cyber security* e le misure necessarie ai fini della sicurezza della nave, legata anche ai rischi cyber.

   Una politica aggiornata di sicurezza e protezione dell'ambiente dovrebbe dimostrare:
   - l'impegno a gestire i rischi informatici come parte dell'approccio complessivo alla gestione della sicurezza (compresa la cultura della sicurezza) e alla tutela dell'ambiente;
   - la consapevolezza che il SMS presenta non solo aspetti di sicurezza (*safety e security*), ma anche di protezione informatica, e che, in particolare, l'accento sia posto sulla gestione dei rischi per la *safety* introdotti da OT, IT e reti;
   - la comprensione che, senza adeguate misure di protezione e controllo dei rischi tecnici e procedurali, l'OT è vulnerabile agli attacchi ed alle possibili interruzioni che possono incidere sull'impiego sicuro di dei sistemi della *Company* e della nave, sulla protezione delle persone a bordo e sulla tutela dell'ambiente.

2. RESPONSABILITA' (Codice ISM punto 3.2) - La *Company* deve designare:
   - a terra, il *Cyber Company Officer* (CyCO), quale responsabile per la gestione e protezione contro i rischi informatici che possa fornire assistenza al Comandante della nave per lo svolgimento dei suoi compiti;
   - a bordo, il *Cyber Security Officer* (CySO), che può essere il Comandante o altro membro dell'equipaggio con compiti direttivi.

3. COMPLIANCE (Codice ISM punto 1.2) - linee guida e raccomandazioni dell'IMO (punto 4.2. della MSC-FAL.1/Circ.3/Rev.2 e Rev.3), dell'Amministrazione e degli Organismi riconosciuti costituiscono una base per la creazione e l'aggiornamento del Risk Assessment (RA) e per l'aggiornamento del Sistema di gestione della sicurezza (SMS) della *Company*. Gli aggiornamenti/modifiche al SMS devono essere verificati, in sede di audit, ai sensi del punto 6 "*Manuale del safety management*" della Circolare: Serie Generale 69/2007.

4. RISK ASSESSMENT (Codice ISM punto 1.2) - il *risk assessment* (RA) dovrà individuare i rischi, le protezioni contro gli attacchi e le responsabilità, tenendo in debita considerazione la Circolare SG 83/2010 e la Rec 171 - Recommendation on incorporating cyber risk management into Safety Management Systems.
   Nello sviluppo del RA è necessario considerare i diversi sistemi operativi (*Operational Technology System* - OT) e quelli informatici (*Information Technology System* - IT) e la differenza tra gli stessi.
   Quando si esamina il CBS è necessario considerare, come già fatto cenno, la distinzione tra sistemi di tecnologia informatica (IT) e quelli di tecnologia operativa (OT). I sistemi IT indicano sistemi incentrati sull'uso di dati come informazioni, inclusi software, hardware e tecnologie di comunicazione (ad esempio, dati sull'equipaggio, come stipendi, certificati, ecc.). I sistemi OT indicano sistemi incentrati sull'uso di dati per controllare o monitorare processi fisici (ad esempio, i livelli di temperatura dell'olio del motore principale, che vengono inoltrati alla sala di controllo). Inoltre, è opportuno, considerare anche la protezione delle informazioni durante lo scambio, l'archiviazione e l'uso dei dati all'interno di questi sistemi. Le vulnerabilità nei sistemi OT possono aumentare il rischio per la sicurezza operativa delle navi. Pertanto, i sistemi OT dovrebbero essere protetti dai sistemi rivolti a Internet e dai sistemi IT con segregazione e strumenti di protezione appropriati, come, per esempio, il dispositivo hardware "diodo dati unidirezionale". Sebbene queste tecnologie e sistemi forniscano significativi guadagni di efficienza per l'industria marittima, presentano anche rischi per i sistemi e i processi critici collegati al funzionamento dei sistemi collegati alla spedizione. Questi rischi possono derivare da vulnerabilità derivanti da un funzionamento, un'integrazione, una manutenzione e/o una progettazione inadeguati dei sistemi correlati alla sicurezza informatica e da minacce informatiche intenzionali e non intenzionali. Le minacce sono presentate da azioni malevoli (ad esempio, hacking o introduzione di malware) o dalle conseguenze indesiderate di azioni benigne (ad esempio, manutenzione del software o permessi utente). Una gestione efficace del rischio informatico dovrebbe considerare entrambi i tipi di minaccia. Il rischio informatico si riferisce, quindi, ai sistemi computerizzati (CBS), che sono minacciati da una circostanza o da un evento potenziale che può comportare criticità operative, di sicurezza o di protezione legate alla navigazione o avarie derivanti da informazioni o sistemi corrotti, persi o compromessi. Inoltre, nella valutazione devono essere inclusi, almeno gli aspetti descritti al punto 3.5 della MSC-FAL.1/Circ.3/Rev.3, e riportati nell'allegato A. Un modello completo e utilizzabile come riferimento è

rappresentato dalle "Guidelines on Cyber Security Onboard Ships"[5], o dal "Framework Nazionale per la Cybersecurity e la Data Protection"[6].
I criteri di accettazione del rischio devono essere documentati; per la categorizzazione della gravità di un particolare sistema può farsi riferimento alle indicazioni fornite nel documento IACS UR E22, nella sua versione aggiornata.
Si sottolinea che la valutazione del rischio non è un'attività da eseguirsi *una tantum*, ma deve essere ripetuta, a valle di adeguate valutazioni, a intervalli regolari (si raccomanda almeno una volta l'anno), fatte salve valutazioni diverse della *Company* basate su rischio, complessità e cambiamenti significativi intervenuti. La valutazione del rischio deve essere aggiornata ogni qualvolta si presentino delle nuove minacce o a seguito di attacchi anche senza conseguenze (*near miss*).

5. RISULTATI DEL RA - I risultati del RA devono essere registrati come processi e le misure adottate rese note all'equipaggio e al personale di terra coinvolto nel processo. Qualora il RA stabilisca che determinate misure non debbano essere rese pubbliche ovvero portate a conoscenza di tutte le persone all'interno della *Company*, le misure dovranno, invece, essere parte della valutazione del rischio di security (SSA) e del piano di security della nave (SSP). A tal riguardo vedasi anche paragrafo 5.2.

6. COMANDANTE (Codice ISM punti 6.1, 6.2) - Il SMS deve riportare le procedure indirizzate al Comandante della nave ed al CySO, se persona diversa. In questo caso, la Società deve anche tenere conto che nuovi compiti di cyber non sono esclusivamente responsabilità del Comandante, ma distribuiti in considerazione degli incarichi e delle responsabilità assegnate al personale di terra ed a bordo.

7. UFFICI DI SUPPORTO - Il Comandante e il CySO devono ricevere un supporto qualificato da terra al fine di porre in essere le misure necessarie per eseguire i compiti previsti in materia di *cybersecurity*. Questo supporto deve almeno prevedere le modalità di risposta ad un attacco di cyber, le iniziative da porre in essere a seguito di un attacco e come ripristinare i servizi dopo un attacco.
   Questa risorsa può essere interna alla *Company* o essere fornita da terzi. Nel fornire le risorse adeguate, è necessario considerare quanto segue:
   - il supporto tecnico della *Company* o di terze parti deve avere familiarità con l'infrastruttura ed i sistemi IT e OT integrati;
   - qualsiasi squadra di risposta interna o squadra esterna di risposta alle emergenze informatiche deve essere disponibile per fornire supporto qualificato e tempestivo alla DPA/CyCO;
   - deve essere previsto un mezzo di comunicazione alternativo tra la nave e la DPA/CyCO, che sia in grado di assicurare il collegamento indipendentemente da tutti gli altri sistemi di bordo;
   - gli audit interni devono confermare che sono disponibili risorse adeguate, comprese terze parti ove opportuno, per fornire supporto in modo qualificato e tempestivo a sostegno della DPA/CyCO.

[5] Disponibile nella sua ultima versione sul portale www.maritimeglobalsecurity.org
[6] Disponibile nella sua ultima versione sul portale https://www.cybersecurityframework.it/

Gli eventuali strumenti contrattuali di affidamento a terzi dei servizi ICT, inclusi quelli di cybersecurity, dovranno contenere anche gli elementi indicati nei punti precedenti. Le responsabilità resteranno comunque in capo al Comandante e al DPA.

8. FAMILIARIZZAZIONE e FORMAZIONE (Codice ISM punti 6.3, 6.5) - I membri dell'equipaggio ed il personale della Company devono ricevere adeguato indottrinamento sulle misure di sicurezza informatica come meglio illustrato al paragrafo 7 (Formazione) della presente Circolare.
   Il SMS deve pertanto contenere un piano di formazione e familiarizzazione e descrivere le procedure necessarie per determinare le esigenze in relazione alla organizzazione della Company e della posizione ricoperta dal singolo elemento.

9. EMERGENZA (Codice ISM punti 8.1, 8.2) - L'SMS deve contenere un "*cyber security contingency plan*" (vedasi sempre le Guidelines on Cyber Security Onboard Ships) che deve essere messo in pratica attraverso esercitazioni, simulazioni e training (punto 8 precedente e paragrafi 7 e 8 successivi). I piani devono almeno includere le misure per rispondere ad un attacco cyber, alle sue conseguenze e le necessarie misure di backup di ripristino e di attuazione di eventuali misure alternative. Il piano deve essere predisposto prevedendo casi di normale utilizzo e casi di compromissione dei sistemi OT.

10. RAPPORTI (Codice ISM punti 9.1, 9.2) - Gli incidenti, i mancati incidenti ed altri eventi rilevanti dovranno essere segnalati ai responsabili della *Company* di cui al punto 2 (Responsabilità) utilizzando le procedure previste dal manuale SMS che a loro volta procederanno ad effettuare le segnalazioni di cui al successivo paragrafo 10. Nella considerazione che un incidente informatico può fornire informazioni preziose sul modo in cui è stata sfruttata una vulnerabilità, la Company deve indagare sugli incidenti informatici che colpiscono IT e OT in conformità con le procedure aziendali, anche con il supporto di esperti esterni, se necessario.
    Inoltre, atteso che le informazioni provenienti da una indagine possono essere utilizzate per migliorare le misure di protezione tecniche e procedurali, le stesse dovranno essere comunicate agli Enti di cui al successivo paragrafo 10.
    Le procedure devono essere aggiornate con l'implementazione di azioni correttive per includere incidenti informatici e misure per prevenirne il ripetersi.

11. MANUTENZIONE DEI SISTEMI (Codice ISM punti 10.1, 10.2, 10.3, 10.4) - Le misure di sicurezza che sono state identificate dal RA come ricorrenti devono essere inserite nel sistema di manutenzione pianificato che monitora e documenta tali misure (es: aggiornamenti software). Inoltre, devono essere aggiornate le misure specifiche volte a promuovere l'affidabilità degli OT e deve essere inclusa la creazione ed il mantenimento di backup/ripristino nelle attività di ruotine relative alla manutenzione operativa dei sistemi di bordo.

12. DOCUMENTAZIONE (Codice ISM punto 11) - Se le misure individuate e i requisiti previsti rientrano nel campo dei dati sensibili, misure specifiche devono essere attuate al fine di renderle accessibili solo ad un gruppo limitato - realmente

coinvolto in campo cyber - di persone a bordo e a terra (Esempi: diritti di amministratore a bordo e gestione password, gestione backup e ripristino).

13. VERIFICHE (Codice ISM punto 12.1) - L'implementazione della gestione della sicurezza informatica nel sistema ISM aziendale e il continuo aggiornamento sono monitorati e verificati da audit (interni e statutari) e revisioni. Gli audit interni devono essere eseguiti a bordo e presso l'ufficio a intervalli non superiori a 12 mesi.

14. VALUTAZIONE (Codice ISM punti da 12.2 a 12.7) - La Società verifica e valuta regolarmente il sistema di gestione della sicurezza rispondendo almeno alle seguenti domande:
    - L'organizzazione (Bordo e terra) funziona secondo i requisiti SMS?
    - Le misure dell'SMS sono efficaci?
    - I revisori interni sono qualificati in sicurezza informatica?
    - I risultati degli audit sono portati all'attenzione del personale competente?
    - Le misure correttive e preventive necessarie sono avviate/implementate tempestivamente?
    - L'alta dirigenza ha valutato l'efficacia delle azioni correttive?

    Sono da includersi anche le domande di cui all'Annex A della MARSEC Doc. 9209, intitolata "Guidance on how to address cybersecurity onboard ships during audits, controls, verifications and inspections", pubblicata il 22 novembre 2023 dalla European Maritime Safety Agency (EMSA) e successive sue modifiche[7].

15. MIGLIORAMENTO CONTINUO - La Company deve tenere conto dei cambiamenti costanti e delle debolezze identificate nel proprio sistema e garantire l'aggiornamento del sistema di valutazione dei rischi e del SMS, avviando così il processo di miglioramento continuo (vedasi anche precedente punto 4 -rischio-).

### 5.2 Procedure del Sistema di gestione della sicurezza (SMS) e del Piano di sicurezza della nave (SSP)

Lo SSA e il SSP devono prevedere uno specifico riferimento alla gestione del rischio informatico[8] contenuto nel SMS.

Un esempio di come organizzare il Piano di sicurezza della nave (SSP) e le relative procedure, secondo gli indirizzi dell'IMO dovrà almeno considerare:

- le procedure relative all'accesso fisico alle aree dotate di sistemi IT e OT; ed
- un riferimento alle procedure di sicurezza informatica dell'SMS.

Utile, altresì, considerare la possibilità di formulare il riferimento all'ambiente ISM, in modo tale da non richiederne l'aggiornamento ogni volta che una procedura connessa alla sicurezza informatica contenuta nell'SMS viene modificata, aggiunta o rimossa.

[7] Disponibile sul portale www.emsa.europa.eu
[8] Codice ISPS B/8.3 reso obbligatorio dal Regolamento 725/2004 art. 3.5.

Di conseguenza, le restanti procedure sulla gestione del rischio informatico dovrebbero riflettersi nell'SMS, escludendo informazioni sensibili come la documentazione di cui al punto 5.1.5 del presente annesso che potrebbe essere sfruttata da attori malintenzionati esterni alla Company. Inoltre, sebbene non esista alcuna regolamentazione sull'archiviazione delle informazioni cyber, si ritiene che le stesse debbano essere trattate – nel processo di controllo ed archiviazione – in modo analogo alla valutazione di security (SSA) e al piano di sicurezza della nave (SSP).

Gli aggiornamenti al Sistema di gestione della sicurezza devono essere verificati ai sensi del punto 6 "*Manuale del safety management*" della Circolare Serie Generale 69/2007.

**5.3 MASS (Maritime Autonomous Surface Ship)**

Sulla base della recente regolamentazione sviluppata dall'IMO, è necessario considerare un paragrafo dedicato che affronti la tecnologia basata sulle MASS. Indipendentemente dai diversi livelli di automazione (MASS 1 - MASS 4), è chiaro che ci sono diverse questioni che devono essere considerate e affrontate per consentire una gestione corretta e sicura della nave, che consiste di diversi sistemi complessi.

Sebbene i principali vantaggi per la gestione delle navi e l'impatto ambientale derivanti da questa tecnologia siano evidenti, i rischi per la sicurezza informatica ad essa associati amplieranno ulteriormente la possibilità di attacchi informatici.

Per questo motivo, i *Remote Operations Center* (ROC) e le navi devono essere adeguatamente considerati durante le procedure di valutazione del rischio, identificando possibili e sfruttabili punti di ingresso per gli attacchi, poiché questi si baseranno su specifiche apparecchiature fisiche, infrastrutture e risorse basate su cloud. Pertanto, ipotizzando un maggiore utilizzo di questa tecnologia in futuro, il supporto alla sicurezza informatica e i controlli di sicurezza saranno più efficaci di quelli provenienti attraverso gli attacchi.

Sebbene i principali rischi associati al MASS siano simili ad altre minacce alla sicurezza informatica nel settore marittimo, si prevede che con l'adozione della tecnologia MASS aumenteranno i nuovi rischi correlati al controllo remoto e ai processi decisionali basati sui sensori.

Si rileva che la probabilità di occorrenza dei seguenti scenari di rischio informatico potrebbe aumentare, rendendo necessaria un'analisi approfondita e l'adozione di misure di mitigazione tecnicamente ed economicamente sostenibili. I rischi possono essere classificati come segue:

1. Rischi di accesso e autenticazione:
   - Accesso remoto non autorizzato ai sistemi;
   - Utilizzo di credenziali predefinite o non sicure;
   - Minacce derivanti da personale interno (*insider threats*);
   - Rischi generati da fornitori o soggetti terzi (*third-party risks*).
2. Rischi di configurazione e protezione dei sistemi:
   - Configurazioni inadeguate delle capacità e funzionalità di sicurezza;
   - Malfunzionamento o disattivazione dei sistemi anticollisione;
   - Manipolazione non autorizzata delle apparecchiature di plancia o della sala macchine.

3. Rischi di comunicazione e segnalazione:
   - Interferenze intenzionali o non intenzionali nelle comunicazioni (*jamming, spoofing*);
   - Intercettazione o disturbo delle comunicazioni;
   - Interferenze operative tra il Remote Operations Centre (ROC) e le unità navali.
4. Rischi operativi e di continuità:
   - Perdita di controllo dei sistemi di navigazione;
   - Riduzione o perdita della consapevolezza situazionale (*situational awareness*);
   - Altre forme di interferenza sui sistemi critici.

Pertanto, si raccomanda che le tecnologie MASS investano:

- sulla solidità della loro sicurezza tecnica e nelle risorse IT/OT prima di aumentare il livello di automazione;
- nello sviluppo delle capacità e delle competenze della forza lavoro degli operatori interessati;
- nella stretta collaborazione con i produttori di sistemi, per garantire che le navi automatizzate siano allineate alle migliori pratiche di sicurezza informatica.

Alcune delle funzionalità più importanti potrebbero includere (senza limitarsi a) blocchi degli account e autenticazione a più fattori (Multi-Factor Authentication - MFA), infrastruttura a chiave pubblica (Public Key Infrastructure - PKI), controllo degli accessi basato sui ruoli (Role-Based Access Control - RBAC), principio dei privilegi minimi, strumenti di monitoraggio e verifica delle attività degli utenti, configurazione e aggiornamenti appropriati degli strumenti di rete e di elaborazione.

Poiché l'automazione è un campo in continua evoluzione, questa sezione non fornisce e non può fornire un elenco esaustivo di possibili minacce, rischi esistenti e controlli necessari, ma intende essere una linea guida di alto livello che fornisca approfondimenti sulle nuove sfide per la tecnologia MASS. Una possibile soluzione per conformarsi alle disposizioni aggiornate è fare riferimento al framework NIST CSF 2.0 e s.m.i. basato sulle funzioni Identify, Protect, Detect, Respond, Recover e Govern adattate alle procedure di gestione del rischio.

### *5.4 Facility – Port facility*

Scopo

I rischi informatici rappresentano le minacce più significative per molti porti ed è pertanto fondamentale proteggere l'interfaccia tra navi, impianti portuali, porti e sistemi utilizzati dalla “comunità portuale”.

La sicurezza informatica non riguarda solo le misure messe in atto per mitigare le minacce causate da azioni malevole e/o distruzione intenzionale del sistema informatico. Riguarda anche la protezione dei sistemi informatici da minacce involontarie o dall'esposizione alla vulnerabilità causata da azioni benigne come scarsa manutenzione del software, progettazione del software, lacune nella disciplina informatica, accessibilità dell'utente o firewall inefficaci.

Pertanto, scopo del presente paragrafo è quello di identificare il processo legato alla cyber security e fornire una guida che possa supportare gi impianti portuali a cui si applica il Codice internazionale per la sicurezza delle navi e degli impianti portuali (ISPS) ed il "Programma Nazionale di Sicurezza Marittima (PNSM)" nella redazione del "*risk assessment*" ed al fine di proteggere i sistemi e le informazioni dalle minacce informatiche.

Quanto sopra con l'obiettivo di adottare tutte le misure per garantire, la gestione sicura dell'impianto, la tutela del personale coinvolto e la protezione dell'ambiente.

Processo Cyber Port Facility

Il codice ISPS (Parte B 15.3.5 - 15.16.5), il Regolamento 725/2004/CE ed il PNSM Rev.2 (PARTE IV - § 25), prevedono che l'impianto portuale adotti misure di valutazione di mitigazione del rischio relativo ad eventuali Cyberattacchi.

L'argomento ha trovato una sua ulteriore sensibilizzazione ed accelerazione dopo l'emanazione del Dlgs. n. 138/2024, relativo al recepimento della cosiddetta "Direttiva NIS2".

Il richiamo ai contenuti del nuovo Decreto legislativo n. 138/2024, che ha di fatto sostituito il Dlgs. n. 65/2018, è contenuto nel PNSM Rev. 2 - PARTE IV - § 25.4. Parimenti, il § 25.3 indica che «*I PFSP degli impianti portuali soggetti al Regolamento (CE) n. 725/2004 devono prevedere idonee misure di cyber security adottate per i propri sistemi nei confronti dei rischi di carattere informatico, a norma del Codice ISPS - paragrafo B/15.3.5: "radio and telecommunication systems, including computer systems and networks" (reso obbligatorio dal Regolamento 725/2004 art. 3.5) che stabilisce che i rischi informatici devono esser valutati nell'ambito del PFSA*».

Al fine di garantire una corretta conduzione della valutazione sotto il profilo della sicurezza cibernetica, tra i soggetti coinvolti nella predisposizione del PFSA deve essere incluso personale esperto ed adeguatamente formato in materia cyber; in mancanza di tali competenze, è necessario avvalersi del supporto di esperti qualificati, in conformità a quanto previsto dal Codice ISPS, paragrafo B/15.4.11, reso cogente dall'articolo 3, paragrafo 5, del Regolamento (CE) n. 725/2004.

Tali esperti devono essere in possesso di comprovate competenze specialistiche in materia di sicurezza cibernetica, applicate ai sistemi, alle reti e ai processi operativi del settore marittimo/portuale, nonché di adeguata formazione ed esperienza documentata nella valutazione dei rischi, nell'analisi delle vulnerabilità e nella definizione di misure di mitigazione coerenti con i requisiti normativi vigenti.

È proprio tale ultimo obbligo che indirizza - quale elemento centrale delle azioni di cyber security - alla "valutazione del rischio", prodromica al recepimento dei suoi risultati nell'ambito del PFSP dell'impianto portuale.

Alla luce di quanto sopra occorre distinguere tra impianti portuali soggetti alla normativa NIS2 ed impianti non inclusi nel perimetro NIS2.

- Per gli impianti portuali soggetti alla normativa NIS2, si ritiene che il corretto adempimento agli obblighi di valutazione e successiva gestione del rischio informatico di cui al Decreto legislativo n. 138/2024 sia idonea a garantire l'osservanza degli obblighi di cui al Regolamento (CE) n. 725/2004 e codice ISPS.

A tal fine le scadenze di adeguamento sono quelle previste dalla normativa NIS2.
Per tali impianti sarà sufficiente che, successivamente all'adeguamento alla NIS2, il PFSA - ed il successivo PFSP - facciano espresso rinvio, rispettivamente per la valutazione del rischio informatico e le conseguenti misure/procedure per la sua gestione, a quanto predisposto a norma del citato Decreto legislativo.
Resta inteso che si dovrà procedere alla nomina di un soggetto responsabile della Protezione Cyber Security come riportato alla prima alinea del successivo punto relativo agli impianti portuali non soggetti alla normativa NIS2. Il ruolo in questione può coincidere con una delle figure previste dalla Direttiva NIS2 e, più in generale, dalle determine dell'ACN. Tuttavia, sarà necessario che la persona designata completi il corso "Duties", relativo alle funzioni di competenza.

- Per gli impianti portuali non soggetti alla normativa NIS2, il Responsabile dell'impianto portuale (come definito dal PNSM Rev.2 - PARTE I - § 3.1.5), sentito il PFSO, dovrà procedere, inoltre, alle sottonotate attività:

  ✓ Nominare un soggetto responsabile della Protezione Cyber Security dei sistemi IT ed OT, operanti e al servizio dell'impianto portuale, ovvero delle attività ad esso collegate e necessarie per l'attuazione del vigente PFSP.
  Tale figura, per gli aspetti di competenza, si ritiene possa coincidere - salvo casistiche di impianti complessi - con il Cyber Port Facility Security Officer (CyPFSO), successivamente meglio identificato. Resta nelle prerogative ed obbligo del Responsabile dell'impianto portuale, sentito il PFSO, la verifica che il CyPFSO, se diverso dal PFSO, sia adeguatamente formato - come da successivo paragrafo 7 - e competente per il ruolo ricoperto. Il CyPFSO, se figura diversa, opera quale collaboratore del PFSO, non sostituendone le attribuzioni, responsabilità e compiti.

  ✓ Unitamente al PFSO e CyPFSO, se figura diversa, provvedere a fornire alle Autorità competenti alla redazione della valutazione di sicurezza - come da PNSM rev. 2, parte III § 4.1 - gli elementi necessari per l'elaborazione della valutazione del rischio informatico, al fine dell'approvazione del PFSA a cura dell'Autorità Designata (c.d. Cyber risk Assessment).
  A tal fine sarà tenuta in considerazione la Raccomandazione IACS Rec. 171 - *Recommendation on incorporating cyber risk management into Safety Management Systems*, contenente anche le discendenti attività di mitigazione del rischio da adottare;

  ✓ A valle dell'approvazione del PFSA e sulla base delle risultanze della valutazione, procedere, attraverso il suo PFSO, a predisporre/emendare il PFSP con le procedure previste per la gestione del rischio, eventualmente anche contenute in apposito annesso al Piano, per la prevista approvazione da parte dell'Autorità Designata.

Entro il 31.12.2026 dovranno essere predisposti ed approvati idonei "addendum" ai PFSA e PFSP vigenti contenenti la valutazione del rischio cibernetico (PFSA) e le relative procedure per la gestione del rischio (PFSP) secondo le indicazioni della presente Circolare.

Il contenuto di tali addendum dovrà esser consolidato all'interno dei PFSA e PFSP in occasione della prossima revisione quinquennale.

Banchine pubbliche

Nel caso di banchine pubbliche, gestite da un'Autorità di Sistema Portuale (AdSP), trovano piena applicazione i principi e le disposizioni già delineate nei paragrafi precedenti.

In particolare, l'AdSP, quale soggetto gestore della facility, deve:

- nominare un proprio CyPFSO/Responsabile Cyber o attribuire tali funzioni al PFSO già in carica;
- predisporre la valutazione del rischio cyber secondo quanto previsto dalla presente Circolare e secondo i riferimenti della Raccomandazione IACS Rec. 171, integrando le informazioni previste dal Programma Nazionale di Sicurezza Marittima (PNSM) e dal D.Lgs. 138/2024 (recepimento della Direttiva NIS2);
- procedere all'invio del PFSA, integrato con gli aspetti di valutazione del rischio Cyber, all'Autorità Designata per la relativa approvazione;
- aggiornare il PFSP, con riferimento alla valutazione del rischio, per la successiva approvazione della Autorità Designata.

Nel caso in cui l'AdSP sia già registrata sulla Piattaforma Logistica Nazionale (PLN), e utilizzi sistemi interconnessi con la stessa, si dovrà:

- tener conto, nella valutazione del rischio, anche delle possibili vulnerabilità derivanti dall'interconnessione con sistemi esterni, incluse le interfacce con PLN e altre piattaforme digitali utilizzate per la gestione logistica e portuale;
- coordinarsi con i referenti tecnici della PLN, ove necessario, per l'analisi delle interfacce e l'adozione di misure tecniche e organizzative congiunte.

Nel caso in cui la banchina pubblica insista in un porto non sede di AdSP, si applicano comunque i principi generali in materia di cybersicurezza previsti dalla presente Circolare. In particolare:

- ✓ In caso di impianto portuale senza abituali utilizzatori la Capitaneria di porto, in qualità di Autorità Designata ai sensi del Regolamento (CE) n. 725/2004, vigila sull'applicazione delle misure di cybersicurezza, con riferimento sia al PNSM, sia al Cyber Risk Assessment delle port facility presenti nel porto;

- ✓ In caso di impianto portuale con abituali utilizzatori, questi hanno l'obbligo di:
  - nominare un CyPFSO, secondo quanto previsto dal paragrafo 5.4;
  - provvedere a fornire all'Autorità Designata gli elementi necessari per l'elaborazione della valutazione del rischio informatico, al fine della predisposizione e approvazione del PFSA;

- assicurare l'integrazione delle misure di cybersicurezza nel piano di sicurezza dell'impianto, conformemente alle previsioni del Codice ISPS, del Regolamento 725/2004/CE e del PNSM.

La Capitaneria di porto, in assenza di un'AdSP, svolge, inoltre, funzioni di coordinamento e monitoraggio delle attività in materia di cybersicurezza, anche tramite l'attivazione di tavoli tecnici locali o interfaccia con ACN e altre autorità competenti.

### 5.5. Cyber risk Assessment dell'impianto portuale[9].

Il presente paragrafo fornisce gli elementi essenziali per la predisposizione del Cyber risk Assessment dell'impianto portuale la cui finalità è quella di identificare e descrivere le vulnerabilità della sicurezza informativa nel contesto di un impianto portuale.

L'annesso al PFSA relativo al cyber risk assessment deve, pertanto, ottemperare alle previsioni di cui al Codice ISPS A/15.5 e contenere almeno i seguenti passaggi:

1. Identificare una persona (Responsabile/CyPFSO): il Responsabile/CyPFSO può essere una sola persona (anche il PFSO) o un gruppo di persone (nel caso di impianti complessi) che - per la predisposizione di cyber risk assessment - abbia una conoscenza approfondita dei sistemi abilitati alla sicurezza informatica che hanno un effetto sulla sicurezza dell'impianto portuale, delle reti a cui sono collegati tali sistemi, delle minacce informatiche che interessano tali sistemi e reti e delle protezioni informatiche disponibili per l'impianto;
2. Identificare tutti i sistemi e le reti correlate alle vulnerabilità fisiche nel PFSA: i processi e le funzioni di sicurezza delle strutture dipendono sempre di più da computer o sistemi basati su computer, come monitor in rete e sistemi di badge elettronici. In genere, questi sistemi sono collegati a reti e se queste reti sono collegate a internet, anche in modo indiretto, è possibile che gli aggressori informatici penetrino nelle reti della facility e sovvertano i processi e le funzioni di sicurezza della facility disabilitando o alterando i sistemi.

   Quando una vulnerabilità fisica coinvolge uno o più sistemi abilitati alla sicurezza informatica, è difficile determinare l'ambito di qualsiasi piano di sicurezza informatica per proteggere tali sistemi specifici. La maggior parte degli attacchi informatici alle strutture comporta che un aggressore informatico effettui l'accesso iniziale alla rete di una struttura tramite un sistema che si connette a Internet e poi si sposti internamente da un sistema all'altro finché non è in grado di compromettere il sistema preso di mira. Pertanto, è palese che qualsiasi piano per proteggere un particolare sistema si basa sul piano di protezione per l'intera rete della struttura.

   Al fine di determinare l'ambito delle protezioni della sicurezza informatica è necessario:
   - identificare tutti i sistemi abilitati alla sicurezza informatica associati ai controlli di sicurezza/vulnerabilità fisica;
   - identificare le reti a cui questi sistemi si collegano;

[9] Vedasi anche linea guida MCAAG.

- quando si descrivono le protezioni di sicurezza informatica per rimediare alle vulnerabilità, descrivere il piano per proteggere la rete su cui operano i sistemi associati;
- fra i sistemi interconnessi vanno valutate anche le attività svolte in ambito di interfaccia utilizzando mezzi informatici di bordo connessi ed operanti con quelli dell'impianto portuale.

3. Stabilire una definizione di vulnerabilità cyber nel contesto del PFSA: la *Facility* deve disporre di un processo formale di gestione del rischio, mediante il quale vegano descritti i livelli di rischio accettabili e inaccettabili e attraverso il quale possa essere determinata la definizione delle vulnerabilità della sicurezza informatica correlate al PFSA.
4. Raccogliere le informazioni necessarie per identificare le vulnerabilità della sicurezza informatica e finalizzare l'elenco da trattare nell'allegato Cyber: dopo che il PFSO, eventualmente in collaborazione con il Responsabile della cyber (CyPFSO) se diverso dal PFSO, ha stabilito come definire le vulnerabilità della sicurezza informatica, è necessario procedere - attraverso tre passaggi - alla efficace identificazione delle vulnerabilità:
   - Costituire un team di esperti in materia con adeguata conoscenza della sicurezza fisica della struttura, delle operazioni IT, OT e di sicurezza informatica;
   - Raccogliere e fornire le informazioni organizzative sufficienti per garantire che il team di valutazione delle vulnerabilità della sicurezza informatica abbia consapevolezza adeguata;
   - Compilare un elenco delle vulnerabilità della sicurezza informatica e confrontarle con le vulnerabilità della sicurezza fisica del PFSA.
5. Determinare il piano di ripristino per ciascuna vulnerabilità espresso in termini di protezioni di sicurezza informatica adeguate alla facility: ogni vulnerabilità deve essere accompagnata da misure di mitigazione per porvi rimedio. Tutte le nuove protezioni per la sicurezza informatica proposte devono essere esaminate in base ai processi di approvazione e gestione del rischio stabiliti, concordati e documentati della facility. In caso di un attacco/incidente informatico, al fine di ripristinare tempestivamente - anche attraverso back-up di sistema - la funzionalità dei sistemi è necessario effettuare l'analisi profonda delle cause con l'obiettivo di prevenire il ripetersi di eventi simili.
6. Documentare le vulnerabilità relative alla sicurezza informatica ed eventuali relazioni con le vulnerabilità elencate nel PFSP e le protezioni all'interno del PFSP.
7. Miglioramento continuo: devono essere tenuti in debito conto i cambiamenti costanti e le debolezze identificate nel proprio sistema nonché garantire l'aggiornamento del cyber assessment, avviando così il processo di miglioramento continuo per determinare se le minacce, le vulnerabilità, le probabilità, gli impatti e i rischi siano cambiati e se le misure di controllo risultino ancora adeguate.

## 6. Porti

Allo stato attuale, la cybersicurezza dei porti, in quanto infrastrutture complesse e rilevanti per la continuità dei servizi essenziali, è espressamente disciplinata esclusivamente dalla Direttiva (UE) 2022/2555 (NIS2), recepita con D.Lgs. 138/2024.

La Direttiva 2005/65/CE del Parlamento europeo e del Consiglio sulla sicurezza dei porti, infatti, non contempla specificamente i rischi di natura cibernetica quale rischi da considerare obbligatoriamente nell'ambito della pertinente valutazione di sicurezza.

Pertanto, per i porti rientranti tra i soggetti essenziali e importanti di cui al D.Lgs. 138/2024 (Allegato I, punto 2 lettera c)), gli obblighi in materia di cybersicurezza sono quelli disciplinati dalla normativa NIS2 e dai relativi provvedimenti attuativi emessi dall'Agenzia per la Cybersicurezza Nazionale (ACN) relativamente ai soggetti individuati quali gestori dei porti definiti all'articolo 3, punto 1), della direttiva 2005/65/CE.

## 7. Responsabilità e Formazione

Mentre già da tempo vengono adottate misure tecniche contro le minacce informatiche, l'elemento umano rimane un aspetto cruciale che richiede un adeguato rafforzamento. Per combattere efficacemente le minacce e le vulnerabilità informatiche, è fondamentale quindi aumentare la consapevolezza degli individui attraverso una attenta, dedicata e puntuale formazione.

È necessario, quindi, garantire un livello adeguato di consapevolezza dei rischi informatici a tutti i livelli di un'organizzazione; consapevolezza e preparazione modulata ed adeguata ai ruoli ed alle responsabilità nella gestione del rischio informatico.

Le responsabilità in materia di sicurezza informatica restano in capo:

- al *Designated Person Ashore* (DPA) per la Company, ed al Comandante per quanto attiene alla nave per la parte ISM;
- al *Company Security Officer* (CSO), allo *Ship Security Officer* (SSO) ed al *Port Facility Security Officer* (PFSO) per la parte security.

Qualora tali soggetti rivestano anche i ruoli di Cyber Company Officer (CyCO), Cyber Security Officer (CySO) o Cyber Port Facility Security Officer (CyPFSO), essi dovranno frequentare esclusivamente i corsi sotto riportati ai punti 1., 2. e 3..

Diversamente, qualora le funzioni di CyCO, CySO e CyPFSO siano attribuite a soggetti diversi dal DPA, dal Comandante, dal CSO, dallo SSO o dal PFSO, i medesimi dovranno:

- completare i corsi previsti ai punti 1., 2. o 3. sotto riportati; e
- in aggiunta, chi ricopre il ruolo di CyCO dovrà conseguire un corso specifico in ambito ISM;
- chi assume il ruolo di CySO o CyPFSO dovrà completare il relativo corso "Duties", riferito alle funzioni di competenza[10].

[10] A norma del Decreto Direttoriale n. 1346 del 3.12.2013 per CySO e IMO Model Course 3.24 per CyPFSO (SECURITY DUTIES).

Inoltre, deve essere almeno prevista:

a) una formazione di base sulla sicurezza informatica per tutto il personale dipendente di terra[11] e di bordo direttamente coinvolto con l'utilizzo di mezzi informatici individuati come critici nell'ambito del Cyber Risk Assessment. La formazione deve essere comunque aggiornata ogni qualvolta il CyCO/CySO/CyPFSO lo riterrà opportuno alla luce di innovazioni o varianti ai sistemi informatici dell'impianto portuale o della nave e prima dell'uso del sistema da parte del personale;
b) una formazione specifica sulla sicurezza informatica per gli utenti OT, diretto a tutto il personale di terra coinvolto[12] e di bordo con aggiornamenti, per entrambi, quando ritenuto necessario dal CyCO/CySO/CyPFSO. La formazione deve essere comunque aggiornata ogni qualvolta il CyCO/CySO/CyPFSO lo riterrà opportuno alla luce di innovazioni o varianti ai sistemi informatici dell'impianto portuale o della nave e prima dell'uso del sistema da parte del personale;
c) una familiarizzazione sulla sicurezza informatica della specifica nave ed impianto per tutti i membri dell'equipaggio e personale della *facility* da ricevere al momento dell'imbarco o assunzione incarico e completare entro 7 (sette giorni).

La formazione viene erogata, come sopra delineato, dal:

1. CyCO, al personale di terra della Company;
2. CySO, al personale di bordo; e
3. CyPFSO, al personale dell'impianto portuale.

La formazione per tutti i dipendenti (lettera a)) e gli utenti OT (lettera b)) deve includere elementi sull'*igiene informatica*[13], il riconoscimento e il rilevamento di un incidente informatico in corso, nonché la risposta e il ripristino.

La familiarizzazione (lettera c)) deve, invece, indirizzare la consapevolezza del personale sui rischi legati alla sicurezza delle informazioni ed agli aggiornamenti sull'evoluzione delle diverse forme di attacco informatico.

La formazione di cui sopra deve essere completata prima dell'assunzione dell'incarico stesso ferme restando le disposizioni di cui al punto c) precedente.

In particolare, il:

1. **CyCO dovrà essere formato in alternativa tra:**
   - <u>CISM (Certified Information Security Manager)</u>
     Riconosciuta a livello globale, orientata alla gestione della sicurezza delle informazioni e ai rischi aziendali.
     Perfetta per chi deve coordinare, pianificare e monitorare programmi di sicurezza a livello organizzativo.

[11] Company ed impianti portuali
[12] Company ed impianti portuali
[13] L'insieme delle buone prassi da seguire per ridurre al minimo i rischi derivanti dall'utilizzo di sistemi informatici, preservando così l'integrità e la sicurezza dei dati personali.

- ISO/IEC 27001 Lead Implementer
  Per gestire l'implementazione di un Sistema di Gestione per la Sicurezza delle Informazioni (ISMS).
  Utile per garantire la compliance normativa e la gestione del rischio in contesti complessi come le infrastrutture portuali.
- CISSP (Certified Information Systems Security Professional)
  Più tecnica, ma adatta a una figura con visione strategica.
  Copre tutto il ciclo della cybersecurity: governance, asset security, engineering, incident response ecc.
- Certified Maritime Cyber Security Professional (CMCP)
  Alcune organizzazioni stanno introducendo corsi specifici per il contesto marittimo. Anche se meno noti, possono essere utili se riconosciuti a livello IMO o da enti portuali.

2. **CySO, dovrà essere formato in alternativa tra:**
   - formazione in Maritime Cyber Security Awareness / Management
     Alcuni corsi sono ora integrati nei moduli STCW, soprattutto dopo le linee guida IMO del 2021 sulla sicurezza informatica a bordo.
     Diverse accademie marittime offrono moduli riconosciuti a livello IMO.
   - IMO Model Course 6.10 – Cyber Security Awareness
     Si tratta di corsi allineati alle guidelines dell'IMO e BIMCO.
     Spesso sono brevi, ma specifici per il contesto della navigazione e della gestione nave-sistema IT/OT.
   - CompTIA Security+
     Certificazione entry-level ma solida per un ufficiale di bordo che deve avere una comprensione tecnica operativa della sicurezza (senza diventare un esperto full-time).
     Utile per comprendere minacce comuni, incident response e gestione base dei sistemi.
   - Maritime Cyber Security Officer Training
     Alcuni registri di classificazione e enti marittimi offrono corsi pratici dedicati a ufficiali di bordo con certificazione riconosciuta dal settore.

3. **CyPFSO, dovrà essere formato in alternativa tra:**
   - GIAC Global Industrial Cyber Security Professional (GICSP)
     Una delle migliori certificazioni al mondo per chi lavora su sistemi ICS/SCADA e OT.
     Perfetta per chi deve capire il legame tra impianti fisici, reti e sicurezza informatica.
     Include: analisi delle vulnerabilità, protezione degli asset OT, threat detection.
   - IEC 62443 Cybersecurity Certificate (Professional level)
     Certificazione specifica per la cybersecurity dei sistemi di controllo industriale (ICS) in ambito critico come porti, energia, trasporti.
     Adatta a chi si occupa di valutazioni del rischio e mitigazione.
   - Certified SCADA Security Architect (CSSA)
     Rilevante per chi lavora su reti SCADA in ambienti portuali complessi.
     Approfondisce sicurezza delle reti industriali, intrusion detection, incident response.

- ISO/IEC 27001 Lead Auditor o Lead Implementer
  Per chi deve aiutare l'impianto portuale a integrare la sicurezza informatica in un sistema di gestione certificato.
  Fondamentale per audit, valutazioni del rischio e gestione documentale.
- Certified Information Systems Auditor (CISA)
  Utile per chi deve supportare il PFSO nella valutazione e controllo dei sistemi IT/OT e delle procedure interne.
  Valido anche per la compliance.
- Maritime Cyber Security for Port Facilities
  Corso specifico per la sicurezza cyber delle infrastrutture portuali.
  Molti di questi corsi rilasciano certificati riconosciuti nel settore marittimo/IMO.

Qualsiasi proposta di formazione difforme rispetto a quanto previsto ai precedenti punti 1., 2. e 3. dovrà essere sottoposta al Comando Generale – VI Reparto e all'Autorità NIS – Settore Trasporti, affinché ne venga verificata la conformità ai requisiti minimi di sicurezza e alle disposizioni normative vigenti.

Il personale esperto dovrà quindi essere in possesso di comprovate competenze specialistiche in materia di sicurezza cibernetica applicata ai sistemi, alle reti e ai processi operativi del comparto marittimo-portuale, nonché di idonea formazione e di esperienza documentata nella valutazione dei rischi, nell'analisi delle vulnerabilità e nella definizione di misure di mitigazione coerenti con il quadro normativo vigente.

**8. Drill ed exercise**

La conoscenza sulla sicurezza informatica deve essere testata attraverso almeno una delle drill e/o exercise già schedulate, in coordinamento tra il SSO e CySO per il bordo, mentre tra PFSO e CyPFSO per l'impianto portuale - simulando scenari previsti nei relativi *assessment*. Tale attività deve essere registrata nei sistemi cartacei e/o informatici già utilizzati per le pari attività previste rispettivamente nel SMS e nel PFSP.
Le drill e/o exercise possono essere sia procedurali che tecniche.

**9. Audit interni**

Gli audit in materia di cyber sicurezza devono essere effettuati nell'ambito degli audit già previsti dal Codice ISM per le Company/navi, e dal Codice ISPS e dal relativo Regolamento (CE) n. 725/2004 per le port facilities. Tali verifiche devono essere condotte da personale qualificato - e secondo gli standard internazionali riconosciuti (es. IMO MSC-FAL.1/Circ.3Rev.3, MARSEC Doc.9209, ISO 27001, NIST) - indipendente rispetto a chi gestisce quotidianamente il sistema, al fine di garantire imparzialità, oggettività e coerenza nell'attuazione delle misure di sicurezza.
Quanto sopra salvo che non risulti impossibile per le:

- dimensioni e la natura della Company o della nave" (A/9.4.1) ovvero
- per le dimensioni o la natura dell'impianto portuale" (A/16.3.1).

## 10. Segnalazioni[14]

A decorrere dal 1° gennaio 2026 le segnalazioni di incidenti informatici sono effettuate in conformità a quanto previsto dal Decreto legislativo 4 settembre 2024, n. 138 (NIS 2) e dalle successive determinazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), tramite le figure e i canali ivi individuati, in particolare mediante la notifica di cui all'articolo 25 del citato decreto.

Fermo restando quanto sopra, ai fini del coordinamento in ambito marittimo e della sicurezza della navigazione, le segnalazioni di incidenti informatici con impatto su navi e impianti portuali devono essere integrate, secondo modalità coerenti con il processo NIS, come segue:

i. la Company, anche tramite le figure previste dalla normativa NIS e dalle determinazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), invii, senza ritardo, le segnalazioni di incidenti informatici a:
   a) l'Ufficio 3 – Maritime Security (maritimesecurity@mit.gov.it);
   b) l'IMRCC (sez4.uff3.rep3@mit.gov.it – itmrcc@mit.gov.it); e, per conoscenza,
   c) l'Organismo di sicurezza riconosciuto della nave.

ii. la Facility, anche tramite le figure previste dalla normativa NIS e dalle determinazioni dell'Agenzia per la Cybersicurezza Nazionale (ACN), invii, senza ritardo, le segnalazioni di incidenti informatici a:
   a) l'Ufficio 3 – Maritime Security (maritimesecurity@mit.gov.it);
   b) l'Autorità designata del porto in cui ricade l'impianto portuale.

## 11. Ispezioni di controllo dello Stato di approdo

Le istruzioni del MoU di Parigi forniscono, fra l'altro, linee guida per il personale Ispettore PSC in merito ai requisiti ISPS e sul Codice ISM.

In particolare, quella su ISM afferma che "*l'audit ISM è responsabilità dello Stato di bandiera e della Company e non rientra nell'ambito del controllo dello Stato di approdo*".

Pertanto, un Ispettore PSC, qualificato come DAO, che conduce un'ispezione PSC non può eseguire un audit del sistema di gestione della sicurezza ISM, in cui potrebbero essere incluse le procedure di sicurezza informatica a bordo della nave. Tuttavia, se, durante un'ispezione PSC, lo stesso ha fondati motivi per ritenere che la nave non sia conforme ai requisiti delle misure per migliorare la security marittima di cui alla Convenzione SOLAS e al Codice ISPS (ad esempio, password annotate su post-it, allegate agli schermi di automazione nell'ECR della nave), potrebbe valutare di effettuare un'ispezione DAO (o di riferire all'autorità competente MARSEC), ai sensi dell'art. 8 del Regolamento (CE) 725/2004. Per quanto riguarda la sicurezza informatica, ciò potrebbe accadere solo in un porto UE per navi battenti bandiera di uno Stato membro UE, considerando che il paragrafo B/8.3.5 dell'ISPS è obbligatorio solo ai sensi della legislazione UE.

È evidente, quindi, che le procedure di sicurezza informatica, indicate nel manuale SMS, potrebbero essere verificate durante un'ispezione dello Stato di bandiera, per la quale non valgono le limitazioni previste per l'ambito PSC.

[14] Per le segnalazioni afferenti gli incidenti informatici si applica esclusivamente la presente circolare e non anche la circolare security n. 45 var. 1, di MARICOGECAP – Reparto VI, e successive sue modifiche o integrazioni.

## 12. Norme di riferimento

L'elenco seguente rappresenta, non esaustivamente, riferimenti a standard internazionali o industriali che possono essere considerati come un background tecnico per questa circolare:

- IMO MSC-FAL.1/Circ.3, *"Guidelines on Maritime Cyber Risk Management"*, July 2017, Rev.2 June 2022, Rev.3 April 2025;
- NIST *"Framework for Improving Critical Infrastructure Cyber security"*, version 2.0 2024;
- *"The Guidelines on Cyber Security Onboard Ships"*, version 4, BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, OCIMF, WSC and IUMI, 2021;
- IACS UR E22, rev 3 *"On Board Use and Application of Computer Based Systems"*, June 2023;
- Raccomandazioni IACS (Rec. 166 e 171), UR E22, UR E26, UR E27 sulla resilienza cyber;
- Linee guida IAPH sulla sicurezza informatica per porti e strutture portuali;
- Maritime Cybersecurity Assessment and Annex Guide (MCAAG) – gennaio 2023;
- MARSEC Doc. 9209 della Commissione Europea sviluppato con il supporto di EMSA: "*Guidance on how to address cybersecurity onboard ships during audits, controls, verifications and inspections*";
- MARSEC Doc. 8910 della Commissione Europea - Guidance on how to treat cybersecurity at the port facility and port level;
- Decreto Legislativo n. 138 del 04/09/2024, pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana n. 230 del 01/10/2024 ed entrato in vigore il 16/10/2024, che ha recepito la direttiva NIS2 UE 2022/2555;
- ISPS Code e Guide to maritime security.

**Allegato A**

## Linee guida per la gestione efficace del rischio cibernetico

Queste linee guida presentano gli elementi funzionali che supportano una gestione efficace del rischio cibernetico. Gli elementi funzionali non sono sequenziali e devono essere attuati in modo simultaneo e continuo, ed integrati in un quadro di gestione del rischio. I controlli riportati nella tabella rappresentano esempi di misure e buone pratiche utili a supportare il cyber risk management, da applicare in modo proporzionato alla complessità della nave, della Company e dei sistemi IT/OT.
Essi non costituiscono requisiti minimi obbligatori, ma una guida metodologica basata sul NIST CSF 2.0 e sul MCAAG.

| Elemento Funzionale | Descrizione generale | Controlli |
|---|---|---|
| 1. GOVERN (Governare) | Stabilire e monitorare la strategia, le aspettative e le politiche di gestione del rischio. Definire ruoli e responsabilità del personale per la gestione del rischio cibernetico. Garantire la continuità operativa (gestione backup, disaster recovery, gestione crisi). | 1. Designare una persona o un'entità responsabile della pianificazione, delle risorse e dell'esecuzione delle attività di cybersicurezza.<br>2. Garantire che tale persona/entità disponga dell'autorità, del supporto e delle competenze necessarie in materia di gestione del rischio cibernetico. |
| 2. IDENTIFY (Identificare) | Determinare il rischio cibernetico attuale per le navi e le interfacce nave/porto. | 1. Identificare sistemi, asset, servizi, dati e capacità, nonché le interdipendenze tra i sistemi critici per la sicurezza, inclusi flussi informativi e catene di fornitura hardware/software.<br>2. Istituire e mantenere un inventario dei sistemi digitali a bordo.<br>3. Eseguire una valutazione del rischio sui sistemi e servizi critici, individuando minacce e vulnerabilità, e valutando probabilità e impatto di incidenti cyber su sicurezza, disponibilità, integrità e riservatezza. |
| 3. PROTECT (Proteggere) | Implementare processi e misure di controllo del rischio per proteggere i CBS (Cyber-Enabled Systems) e garantire la continuità operativa in caso di incidente cyber. | 1. Assegnare credenziali univoche, separare account utente e privilegiati, disattivare account di dipendenti/utenti cessati.<br>2. Cambiare tutte le password di default, imporre policy di password robuste, considerare autenticazione multifattore, comunicazioni sicure (voce, video, testo).<br>3. Limitare i servizi esposti a Internet, approvare hardware/software, archiviare log di sicurezza, segmentare reti OT da IT.<br>4. Implementare firewall, antivirus e politiche crittografiche.<br>5. Controllare l'uso di supporti rimovibili non autorizzati.<br>6. Obbligare formazione annuale di base in cybersicurezza per tutto il personale, formazione OT per gli utenti OT, e familiarizzazione per tutto l'equipaggio all'imbarco (inclusi elementi su igiene cibernetica, rilevamento e risposta).<br><br>7. Eseguire backup regolari, aggiornamenti software, e sviluppare/aggiornare piani di risposta agli incidenti.<br>8. Definire politiche di sicurezza per la supply chain hardware/software.<br>9. Stabilire procedure di audit e revisione periodica dell'efficacia delle misure di gestione del rischio cibernetico. |
| 4. DETECT (Rilevare) | Sviluppare, implementare e praticare attività necessarie per rilevare un incidente cyber tempestivamente. | 1. Mantenere un elenco aggiornato di minacce, tattiche, tecniche e procedure di attori malevoli, monitorando attivamente i sistemi.<br>2. Includere nella formazione annuale di base la capacità di riconoscere e rilevare incidenti cibernetici in corso. |
| 5. RESPOND (Rispondere) | Sviluppare, implementare e praticare attività e piani per garantire la resilienza e ripristinare i sistemi necessari alle operazioni di navigazione e alle interfacce nave/porto in caso di incidente cyber. | 1. Segnalare gli incidenti alle autorità competenti entro i tempi previsti dall'Amministrazione.<br>2. Mantenere registri degli incidenti cibernetici.<br>3. Includere nella formazione annuale la risposta a incidenti cyber. |
| 6. RECOVER (Ripristinare) | Identificare e implementare misure per ripristinare i CBS di bordo e le reti necessarie alle operazioni navali dopo un incidente cyber. | 1. Sviluppare, mantenere e attuare strategie di recupero e ripristino dei sistemi critici o essenziali.<br>2. Includere nella formazione annuale la capacità di recupero post-incidente.<br>3. Effettuare analisi delle cause (root cause analysis) per prevenire recidive. |