

**COMITATO INTERMINISTERIALE PER LA SICUREZZA DEI TRASPORTI  
MARITTIMI E DEI PORTI**

-----

**AUTORITA' COMPETENTE PER LA SICUREZZA MARITTIMA**

**ORGANIZZAZIONE DI SECURITY LEGGERA (SELE ) PER GLI IMPIANTI PORTUALI**  
Applicazione dell'articolo 3.3 del Regolamento (CE) n. 725/2004

**LINEE GUIDA**

## INTRODUZIONE

1. Scopo delle presenti linee guida è fornire un riferimento per l'elaborazione del piano di sicurezza nell'ambito dell'organizzazione di "security leggera" (SELE). Esse si riferiscono agli impianti che prestano servizio: alle navi HSC, DSC e aliscafi che effettuano navigazione nazionale oltre 20 miglia dalla costa, se abilitate al trasporto di  $\geq 450$  passeggeri ed alle navi assimilate come da punto 3 della scheda A Appendice I al presente documento; alle navi cisterna, petroliere, chimichiere e gasiere  $\geq 500$  GT che effettuano navigazione nazionale.
2. Gli impianti che prestano servizio alle navi di cui al precedente capoverso ed hanno già redatto un PFSP in attuazione dei commi 3.1 e 3.2 del Reg. 725/2004 non sono tenuti ad elaborare ed applicare il Piano di Security Leggera (SELE) se, anche nell'interfaccia con le navi cui si riferisce la SELE, adottano le misure previste nel pertinente PFSP redatto a mente dei predetti commi.
3. Le presenti linee guida mirano a rispondere al dettato dell'articolo 3.3 del Regolamento(CE) n.725/2004 del Parlamento europeo e del Consiglio in data 31 marzo 2004. Il presente documento tiene altresì conto delle indicazioni impartite dal Comitato interministeriale per la sicurezza dei trasporti marittimi e dei porti (CISM) che, nella riunione del 26 aprile 2007, ha approvato i quadri sinottici e le definizioni in essi contenute per l'applicazione di una organizzazione di security leggera a decorrere dal 24.03.2008 alle unità destinate al trasporto marittimo nazionale riportate in appendice I (schede A, B, C e D che sono parte integrante del presente documento).
4. Fatto salvo quanto detto al precedente punto 2., alla redazione del piano di sicurezza provvede l'impresa così definita al successivo par. 7, n° 14), che presta servizio alle predette navi. La redazione del Piano da parte delle imprese operanti nell'impianto che presta servizio alle navi in argomento è obbligatoria. I contenuti del piano, viceversa, si conformano e tengono conto, per quanto possibile e ragionevole, delle indicazioni delle presenti linee guida.
5. Entro il 30.10.08 le Autorità Designate provvederanno all'approvazione delle valutazioni di sicurezza. Entro 30 giorni dalla data di ricezione della valutazione di sicurezza, l'impresa di cui al punto 4 sopracitato dovrà presentare il piano di sicurezza che, approvato dal capo del Compartimento Marittimo entro i successivi 30 giorni, sarà sottoposto ad un periodo di sperimentazione obbligatoria che avrà termine il 30.09.2009.  
In tale periodo di sperimentazione, svolta sotto il monitoraggio dell'Autorità marittima, di intesa con l'A.P. per gli impianti esistenti in porti amministrati da A.P., verrà valutata, sempre d'intesa tra le predette Autorità, la coerenza delle misure di sicurezza contenute nel piano con gli obiettivi di security dell'impianto, riferendone gli esiti entro 31.10.2009 all'Autorità competente per la

sicurezza marittima. Tale Autorità effettuerà una valutazione generale dell'efficacia e della fattibilità delle forme di security applicate, riferendone successivamente gli esiti al CISM al fine di consentire allo stesso di valutare l'opportunità di apportare modifiche al presente documento e/o di passare da un sistema di raccomandazioni ad un regime dispositivo cogente in quei settori che sulla base dell'esperienza dovessero evidenziare fattori di criticità.

6. Le presenti istruzioni si rivolgono a realtà diverse tra loro. Nel rispetto delle specificità territoriali ed operative si presterà la massima attenzione nell'individuare per ciascun impianto una forma proporzionata ma coerente di security. Ogni sforzo deve, altresì, essere fatto dall'Autorità designata per supportare la precitata attività mettendo a disposizione il proprio "know-how" in materia di "security".

ell'attuazione delle presenti linee guida non ci si deve discostare dal principio generale di perseguire l'efficienza, l'economicità ed adeguatezza del trasporto marittimo e dell'operatività del porto.

7. Ai fini del presente documento si intende per:

- 1) **"misure speciali per migliorare la sicurezza marittima della Convenzione SOLAS"**, gli emendamenti, quali figurano all'allegato I del regolamento n. 725/CE del Parlamento Europeo e del Consiglio del 31 marzo 2004, che riportano il nuovo capitolo XI-2 dell'allegato alla Convenzione SOLAS nella sua versione aggiornata;
- 2) **"codice ISPS"**, il Codice internazionale per la sicurezza delle navi e degli impianti portuali nella sua versione aggiornata;
- 3) **"parte A del Codice ISPS"**, il preambolo e le prescrizioni obbligatorie, che costituiscono la parte A del Codice ISPS, quali figurano all'allegato II del regolamento n. 725/CE del Parlamento Europeo e del Consiglio del 31 marzo 2004, riguardanti le disposizioni del capitolo XI-2 dell'allegato alla Convenzione SOLAS, nella sua versione aggiornata;
- 4) **"parte B del Codice ISPS"**, gli orientamenti e le prescrizioni (art.3 comma 5 del Reg. 725/2004) costituenti la parte B del Codice ISPS che figurano nell'allegato III del regolamento n. 725/CE del Parlamento Europeo e del Consiglio del 31 marzo 2004, riguardanti le disposizioni del capitolo XI-2 dell'allegato alla Convenzione SOLAS, come modificata, e della parte A del Codice ISPS, nella sua versione aggiornata;
- 5) **"sicurezza marittima"**, la combinazione delle misure preventive e protettive dirette a tutelare il trasporto marittimo e gli impianti portuali contro le minacce di azioni illecite intenzionali;
- 6) **"Autorità competente per la sicurezza marittima"** il Comando generale del Corpo delle capitanerie di porto ;
- 7) **"punto di contatto per la sicurezza marittima"** Il Comando generale del Corpo delle capitanerie di porto che si avvale della centrale operativa IMRCC (Centro Nazionale di Coordinamento del Soccorso Marittimo);

- 8) **“Autorità designata”**, il Capo del Compartimento Marittimo (art. 16 Cod. Nav.). Nell’esercizio delle relative funzioni l’Autorità designata opera in accordo con l’Autorità Portuale, ove istituita;
- 9) **“Autorità portuale”**, è l’Ente di cui all’art.6 della Legge 28 gennaio 1994, n.84 e successive modificazioni;
- 10) **“traffico marittimo internazionale”**, qualunque collegamento marittimo via nave tra un impianto portuale nazionale e un impianto portuale di altro Stato o viceversa;
- 11) **“traffico marittimo nazionale”**, qualunque collegamento via nave effettuato nelle zone marittime da un impianto portuale di uno Stato e lo stesso impianto portuale o un altro impianto portuale nazionale;
- 12) **“servizio di linea”**, una serie di traversate organizzate in modo da assicurare un servizio di collegamento tra due o più impianti portuali:
  - a) secondo un orario pubblicato; oppure
  - b) con una regolarità o una frequenza tali da costituire un servizio sistematico riconoscibile;
- 13) **“impianto portuale”**, quella porzione di area portuale direttamente ed immediatamente connessa con le attività di imbarco oggetto di tutela, di seguito definita “impianto”;
- 14) **“impresa”**, il soggetto autorizzato, secondo le norme di legge, ad effettuare – per conto proprio o di terzi (ovvero in regime di autoproduzione a mente dell’art. 8 del D.M. 31.3.1995, n. 585) – le operazioni portuali di cui all’art. 16, c. 1 della L. 28.1.1994, n. 84 e s. m. e i., ovvero il soggetto concessionario di cui all’art. 18, L. 28.1.1994, n. 84 e s. m. e i.
- 15) **“interfaccia nave/porto”**, le interazioni che hanno luogo quando una nave è direttamente ed immediatamente interessata da attività che comportano il movimento di persone, o di merci o la fornitura di servizi portuali verso la nave o dalla nave;
- 16) **“azione illecita intenzionale”**, atto intenzionale, che, per la sua natura o per il suo contesto, potrebbe danneggiare le navi utilizzate nel traffico marittimo tanto internazionale quanto nazionale, i loro passeggeri o il loro carico o i relativi impianti portuali;
- 17) **“Nave passeggeri”** significa una nave che trasporta più di dodici passeggeri;
- 18) **“HSC”** significa una nave come definita dalla SOLAS Reg. X/1.3.;
- 19) **“DSC”** significa una nave come definita dal DSC code Res A.373(X) cap. 1.4.1.;
- 20) **“Aliscafo”** significa una nave come definita dal D.P.R. 8 novembre 1991, n.435 Art.1.2.;
- 21) **“Nave da carico”** significa qualsiasi nave che non sia una nave da passeggeri;
- 22) **“Nave cisterna”** significa una nave da carico costruita o adattata per il trasporto alla rinfusa di carichi liquidi di natura infiammabile;
- 23) **“Nave chimichiera”** significa una nave chimichiera come definita alla Regola VII/8.2;
- 24) **“Nave gasiera”** significa una nave gasiera come definita alla Regola VII/11.2;
- 25) **“Nave petroliera”** significa una nave petroliera come definita alla Regola II-1/2.12;

- 26) **“Società”** significa una società come definita alla Regola IX/1;
- 27) **“Attività da nave a nave”** significa ogni attività non connessa ad un impianto portuale che implichi il trasferimento di merci o persone da una nave all'altra;
- 28) **“Incidente di sicurezza”** significa qualsiasi atto o circostanza sospetti che minaccino la sicurezza di una nave, ivi comprese le unità mobili di perforazione offshore e le unità ad alta velocità, ovvero la sicurezza di un porto, impianto portuale o di un'interfaccia nave/porto o di un'attività da nave a nave;
- 29) **“Livello di sicurezza”** significa la qualificazione del grado di rischio che un incidente di sicurezza possa essere tentato o possa verificarsi;
- 30) **“Livello di sicurezza 1”** è il livello per cui vanno costantemente mantenute misure di sicurezza minime adeguate;
- 31) **“Livello di sicurezza 2”** è il livello per cui vanno mantenute adeguate misure di sicurezza supplementari per un determinato periodo, in conseguenza di un incremento del rischio che si verifichi un problema di sicurezza;
- 32) **“Livello di sicurezza 3”** è il livello per cui vanno mantenute adeguate misure di sicurezza specifiche, per il periodo limitato in cui un problema di sicurezza è probabile ed imminente, anche quando non sia possibile individuare l'obiettivo specifico;

Le presenti linee guida sono state approvate dal CISM nella riunione in data

\_\_\_\_\_.

## **CAPITOLO I**

### **GENERALITA'**

1. Le politiche di security leggera poste in essere per rispondere al dettato dell'art. 3.3. del Reg. (CE) n. 725/2004 del 31.3.2004, tendono all'ottimale contemperamento (nella fase di interfaccia) delle esigenze di security dell'impianto portuale, della nave che utilizza l'impianto, delle persone presenti nell'impianto e di quelle a bordo con le esigenze di operatività ed economicità delle attività marittimo-portuali.

Le imprese sono responsabili dell'attuazione delle misure di Security leggere individuate nel piano. A tal fine devono dotarsi delle risorse, attrezzature e materiali eventualmente necessari, tenendo ovviamente in considerazione le contestuali misure, risorse, attrezzature e materiali impegnati a fini di security dalla nave che si interfaccia con l'impianto.

2. E' cura dell'impresa individuare un Responsabile della sicurezza dell'impianto, ed eventualmente i relativi sostituti, che avrà piena conoscenza del piano, delle norme, regole, direttive e prassi richiamate nel piano stesso, nella misura necessaria per una sua buona gestione.

Il Responsabile della security dell'impianto fornisce al personale dell'impianto ed agli eventuali addetti alla sicurezza del medesimo (qualora dal Piano emerga la necessità di tali figure) informazioni necessarie per l'attuazione delle misure previste dal Piano e le necessarie direttive.

3. Il Responsabile della security dell'impianto si raccorda con il Responsabile di security di bordo delle navi che attraccano all'impianto per lo svolgimento di attività di interfaccia, al fine di porre in essere in modo sinergico e coordinato i rispettivi compiti di security.

## CAPITOLO II

### VALUTAZIONE DI SECURITY DELL'IMPIANTO

#### A. GENERALITA'

1. Un più elevato grado di sicurezza (security) dell'interfaccia nave-impianto non è realizzabile mediante la semplice somma di singole misure che, pur se astrattamente idonee, non hanno identica valenza a seconda della realtà territoriale, infrastrutturale ed operativa in cui si applicano. Più probabilmente un complessivo incremento del grado di sicurezza dell'impianto e dell'interfaccia sarà funzione di un "giusto mix" di più misure/attività. Per individuare questo giusto mix si dovranno considerare:
  - le caratteristiche tecniche dell'impianto – infrastruttura e relativo lay out;
  - i punti di accesso;
  - le sovrastrutture ed attrezzature presenti. In tale ambito si dovrà considerare attentamente, tenendo conto della loro localizzazione se ricomprendere nell'ambito dell'impianto (anche ai fini delle attività di controllo che si prevederanno nel Piano), le pensiline o le altre zone, con strutture di riparo e non, utilizzate dai passeggeri e dai visitatori in attesa di salire a bordo. Non costituiscono invece area dell'impianto, ai fini del presente documento e dello svolgimento delle attività di controllo, le zone per l'incolonnamento e la sosta degli automezzi;;
  - le attività che si svolgono nell'impianto nella fase di interfaccia, anche in relazione alla tipologia di nave che vi opera;
  - le caratteristiche qualitative e quantitative del personale che opera nella fase di interfaccia (personale specificamente addetto alla security e altro personale che esplica attività per l'interfaccia);
  - le apparecchiature ed i sistemi di safety, security, di allerta e collegamento esistenti nell'interfaccia e le relative procedure di gestione ed organizzazione;
  - le vulnerabilità, sia strutturali che di organizzazione, rispetto ad incidenti di security rilevanti;
  - altro elemento da considerare con attenzione è quello della pianificazione ed organizzazione di security delle navi che si interfacciano con l'impianto, con particolare riguardo al segmento dell'organizzazione e gestione di security da parte della nave durante le attività di carico, al fine di evitare dispendiose duplicazioni di attività o inutili ridondanze. (Ad esempio, se una nave avente due punti di possibile accesso a bordo nella fase di interfaccia prevede, in base alla propria pianificazione di security, l'utilizzazione di un solo punto di accesso, non sembrerebbe logico prevedere una qualsiasi forma di controllo da parte dell'impianto anche per il secondo accesso). Parimenti importante, ai fini di una ragionevole valutazione di security, è la considerazione dei sistemi e delle procedure di security poste in essere a monte dell'interfaccia (es. eventuali procedure di verifica, controlli, ispezioni poste in essere all'ingresso del porto e/o del terminal);
  - le possibili misure che concorrono a mitigare i fattori di rischio, da assumere singolarmente nonché in eventuali combinazioni alternative tra loro. Va rammentato peraltro che è

opportuno (talora addirittura potrebbe essere preferibile) prendere in attenta considerazione non solo misure “fisiche” (attrezzature, impianti, ecc.) ma anche quelle procedurali ed organizzative.

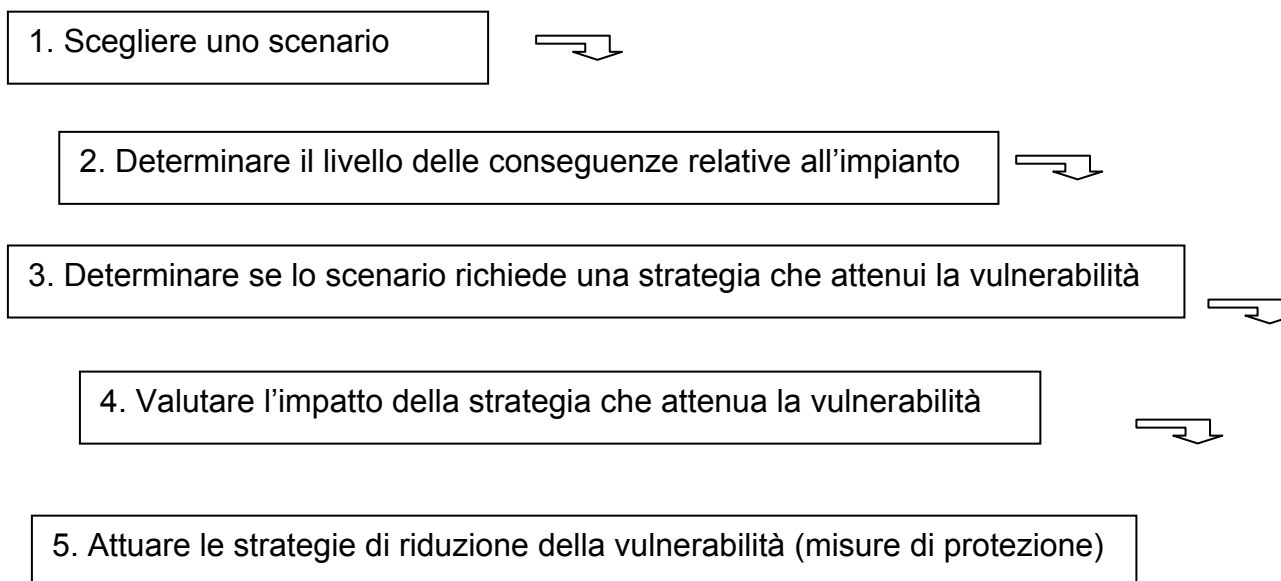
A tal riguardo appare opportuno valorizzare nella massima misura possibile, ai fini della valutazione, le misure di sicurezza predisposte autonomamente da parte di uffici e presidi di polizia operanti in porto, particolarmente per le tipologie di traffico tra quelle cui si applica la SELE (navi HSC, DSC ed aliscafi) aventi caratteristiche (schedulazione degli orari) che prefigurano una programmabilità dell'intervento dei predetti uffici e presidi. Le possibili misure/strategie alternative vanno anche considerate in relazione ai vari livelli di minaccia alla security stabiliti. Quindi alcune misure/strategie potrebbero non essere necessarie/opportune al “livello di security 1”, ma potrebbero invece esserlo al “livello 2”. Così come andrebbero valutate attentamente (ma con massima ponderazione) le ipotesi di temporanee sospensioni dell'operatività al massimo “livello di security” (level 3) qualora per garantire l'operatività dello specifico interfaccia considerato emergesse la necessità di misure/strategie eccessivamente onerose rispetto alla probabilità di verificarsi dell'evento stesso.

2. Circa il processo logico sistematico da impiegare nella valutazione di sicurezza dell'impianto, si ripropone sostanzialmente quello contenuto nelle “linee guida per la redazione della documentazione di valutazione dei rischi (Port facility)” già approvato dal CISM il 6 aprile 2004, allegato alla circolare “Port Security” N. 01 in data 7.4.2004 dell'allora Ministero Infrastrutture e Trasporti - Dipartimento per la Navigazione ed il Trasporto Marittimo ed Aereo – Comando Generale del Corpo delle Capitanerie di Porto – ovviamente adattato per tenere conto della specificità dei traffici serviti dagli impianti cui si applica la SELE.

## **B. VALUTAZIONE DI SECURITY**

### **1. Possibile processo logico-sistematico per la valutazione di sicurezza dell'impianto.**

Quella che segue è una valutazione della sicurezza basata sull'analisi del rischio semplificata, tracciata nel seguente diagramma di flusso. Quando si effettua la valutazione, i procedimento ed i risultati dovrebbero essere documentati (viene fornito un esempio nella tavola 5).



Nota: ripetere questo procedimento finchè non siano stati valutati tutti i diversi scenari.

### **Fase 1 - Potenziali minacce**

Per iniziare una valutazione, chi effettua la valutazione deve considerare i possibili scenari nei quali può presentarsi, in determinate circostanze, una potenziale minaccia. È importante che lo scenario o gli scenari siano inseriti in contesti reali e coerenti con quanto emerso dalla valutazione della minaccia.

I possibili scenari da considerare, salvo specificità locali, devono comprendere:

- l'ingresso di persone non autorizzate;
- l'introduzione di armi, esplosivi ed altre sostanze pericolose non autorizzate.

### **Fase 2 - Valutazione delle conseguenze**

Ciascuno scenario dovrebbe essere valutato in termini di conseguenze potenziali dell'attacco. Sono inclusi tre elementi nella valutazione delle conseguenze: danni alle persone (morti e feriti), impatto economico e impatto ambientale. Riguardo a quest'ultimo impatto va tenuto conto dell'ambito territoriale impattabile (i porti sono bacini chiusi ed eventuali dispersioni di prodotti inquinanti difficilmente potrebbero interessare aree vaste) e delle misure / attrezzature di contenimento degli impatti ambientali di cui dispongono la quasi totalità dei porti. Segue una descrizione dei componenti delle conseguenze:

Tab.1 Elementi di valutazione

<b>Danni alle persone</b>	Il numero ipotizzabile (valutazione oggettiva) di vite che si potrebbero perdere e dei feriti che potrebbero registrarsi in conseguenza di uno scenario d'attacco
<b>Impatto economico</b>	Il potenziale impatto (valutazione oggettiva) economico di uno scenario di attacco.
<b>Impatto ambientale</b>	Il potenziale impatto ambientale (valutazione oggettiva) di uno scenario di attacco.

Le conseguenze per ogni scenario devono essere valutate con un punteggio appropriato. Nella tabella seguente sono forniti i punteggi e i parametri di valutazione delle conseguenze. Tali risultati devono essere intesi come stime approssimative. Il punteggio specifico è determinato utilizzando la valutazione della conseguenza che risulta più elevata. Ad esempio se le componenti morti, feriti e impatto economico hanno un valore "Moderato" o "1" ma l'impatto ambientale ha valore "Significativo" o "2", il punteggio totale della conseguenza è da considerarsi "2".

Tab. 2 Gradazione delle conseguenze

Assegnare una valutazione pari a:	Se l'impatto è
<b>3</b>	<b>CATASTROFICO</b> = numerose perdite di vite o feriti; importante impatto su scala nazionale o impatto economico a lungo termine; distruzione completa di aspetti multipli dello ecosistema in una grande area
<b>2</b>	<b>SIGNIFICATIVO</b> = significativa presenza di morti o feriti; importante impatto economico regionale; danno a lungo termine ad una parte dell'ecosistema
<b>1</b>	<b>MODERATO</b> = nessuna o bassa presenza di morti o feriti; impatto economico basso; lieve danno ambientale

### Fase 3 - Valutazione della vulnerabilità

Ciascuno scenario va valutato in termini di vulnerabilità dell'impianto ad uno specifico attacco. Gli elementi del grado di vulnerabilità sono accessibilità e organizzazione della security. Assumendo che il Responsabile per la security ha il controllo sui fattori inerenti l'accessibilità e la organizzazione della security, questi elementi devono essere calibrati per ogni scenario. Questi due elementi di vulnerabilità possono essere definiti come segue:

Tab. 3 Elementi di valutazione

<b>Accessibilità</b>	Accessibilità all'impianto nello scenario di attacco. Essa riguarda le barriere fisiche e geografiche che possano scoraggiare la minaccia senza considerare l'organizzazione della security.
<b>Organizzazione della security</b>	Capacità del personale dell'impianto di scoraggiare l'attacco. Essa include piani di security, capacità di effettuare comunicazioni, personale di sorveglianza/supervisione, sistemi di rilevazione delle intrusioni e la tempestività di tutte e forze di polizia esterne di prevenire l'attacco

La valutazione iniziale della vulnerabilità si effettua considerando solo le strategie e le misure protettive già esistenti ed in atto.

Nella seguente tabella sono riportati criteri e punteggi di vulnerabilità con esempi di riferimento. Occorre valutare ogni scenario per ottenere il punteggio individuale di ogni elemento, poi sommare tutti gli elementi e calcolare il punteggio totale (fase 3).

Tab. 4 Gradazione della vulnerabilità

<b>Accessibilità</b>	<b>Organizzazione della security</b>	<b>Valutazione</b>
Nessuna deterrenza (es. accesso all'impianto nave e movimento interno senza restrizioni)	Nessuna capacità di deterrenza (es. assenza di un piano, assenza di sorveglianza/supervisione, indisponibilità di mezzi di comunicazioni d'emergenza, le forze dell'ordine esterne non sono disponibili per una prevenzione tempestiva)	<b>3</b>
Buona deterrenza (es. vi è una sola barriera; accesso limitato)	Buona capacità di deterrenza (es. istruzioni/procedure basiche di security, qualche mezzo di comunicazione, presenza – seppure limitata di personale di sorveglianza e/o con capacità di supervisione, disponibilità limitata di forze dell'ordine esterne, limitati sistemi di rilevamento)	<b>2</b>
Eccellente deterrenza (es. accesso limitato con barriere fisiche multiple, restrizioni di accesso)	Perfetta capacità di scoraggiare gli attacchi (per es. un piano di sicurezza dettagliato, comunicazioni efficaci in caso di emergenza, personale con compiti di sicurezza ben addestrato ed adeguatamente equipaggiato; sistemi di rilevamento, tempestività delle forze dell'ordine nell'intervenire per la prevenzione)	<b>1</b>

#### **Fase 4 - Mitigazione**

Chi effettua la valutazione individuerà quali scenari possano richiedere l'applicazione di strategie di mitigazione della vulnerabilità (misure protettive).

Qui di seguito sono descritti i termini utilizzati per le categorie di mitigazione in Tabella 5:

“**Mitigare**” indica che vanno sviluppate strategie di mitigazione, quali misure e/o procedure, per ridurre i rischi in un determinato scenario. Chi effettua la valutazione deve essere in grado di documentare (in appendice al Piano) gli scenari valutati, i risultati delle valutazioni, la descrizione delle misure di mitigazione valutate e le motivazioni che hanno portato a porre in essere o meno dette misure;

“**Considerare**” indica che dovrebbero essere considerati lo scenario e le strategie di mitigazione da sviluppare caso per caso. Chi effettua la valutazione deve essere in grado di documentare (in appendice al Piano) gli scenari valutati, i risultati delle valutazioni, la descrizione delle misure di mitigazione valutate e le motivazioni che hanno portato a porre in essere o meno dette misure;

“**Documentare**” indica che lo scenario può non richiedere una misura di mitigazione ma che esso deve solo essere documentato.

La Tabella 5 è uno strumento, di larga massima, d’assistenza per l’individuazione degli aspetti che necessitano di interventi per mitigare il rischio. I “risultati numerici” non devono essere considerati come unica base per decidere di applicare o meno le misure specifiche, infatti sono uno strumento per l’identificazione delle potenziali vulnerabilità e dei metodi di valutazione delle stesse.

Tab. 5: Matrice della vulnerabilità e delle conseguenze

		Grado di vulnerabilità (Tab. 4)		
		2	3 - 4	5 - 6
Grado delle conseguenze (Tab. 2)	3	Considerare	Mitigare	Mitigare
	2	Documentare	Considerare	Mitigare
	1	Documentare	Documentare	Considerare

È quindi possibile registrare gli scenari considerati, il grado delle conseguenze (Tabella 2) e della vulnerabilità (Tabella 4), il punteggio totale di vulnerabilità e la categoria di mitigazione (Tabella 5).

Nel determinare quali scenari possano richiedere l’applicazione di metodi di mitigazione, chi effettua la valutazione può trovare utile l’utilizzo della Tabella 6 riportata qui di seguito.

Tab. 6 Quadro sinottico per la strategia di mitigazione

Fase 1	Fase 2	Fase 3			Fase 4
Scenario	Grado delle conseguenze (Tabella 2)	Grado di vulnerabilità (Tabella 4)			Risultati per la mitigazione (Tabella 5)
		accessibilità +	Organizzazione della security =	Risultato totale	

### FASE 5 - Metodi di applicazione

L'obiettivo di queste valutazioni si raggiunge quando, dopo aver determinato quali scenari necessitano di mitigazione, sono individuate le opportune strategie (misure protettive) per ridurre la vulnerabilità. L'aspirazione è ridurre i rischi associati allo scenario identificato. Quando si considerano le strategie di mitigazione è generalmente più semplice ridurre le vulnerabilità anziché le conseguenze o le minacce.

Nella valutazione dell'efficacia delle strategie specifiche di mitigazione (misure di protezione), chi effettua la valutazione può trovare utile l'impiego della Tabella 7 qui di seguito riportata.

Tab. 7 Interazione dell'attività di mitigazione

Fase 1	Fase 2	Fase 3	Fase 4			Fase 5
Strategia di mitigazione (Misura protettiva)	Scenario(i) influenzato(i) dalla Strategia di mitigazione (dalla fase 1 nella Tabella 6)	Grado delle conseguenze	Nuovo grado di vulnerabilità (Tabella 3)			Nuovi risultati di mitigazione (Tabella 5)
			Accessibilità +	Organizzazione della security =	Risultato totale	
1.	1.					
	2.					
	...					
2.	...					

A ciascuna colonna della Tabella 7 corrispondono i seguenti punti:

- vanno elaborate le strategie di mitigazione (misure protettive) e registrarle nella prima colonna della Tabella 7;
- usando lo scenario della Tabella 6, elencare tutti gli scenari che potrebbero essere influenzati dalla strategia di mitigazione scelta;

3. il grado delle conseguenze rimane lo stesso come riportato nella Tabella 6 per ciascuno scenario;
4. rivalutare il grado di vulnerabilità (Tabella 4) di ciascun elemento, tenendo in considerazione la strategia di mitigazione, per ciascuno scenario;
5. con il punteggio delle conseguenze e il nuovo punteggio totale delle vulnerabilità, utilizzare la Tabella 5 per determinare i nuovi risultati di mitigazione.

Due fattori devono essere considerati nello stabilire se attuare una strategia di mitigazione: l'efficacia e la fattibilità. Una strategia può essere ritenuta altamente efficace se la sua attuazione abbassa la categoria di mitigazione (es. da "Mitigare" a "Considerare" in Tabella 5). Una strategia è da considerarsi parzialmente efficace se, applicata singolarmente o insieme ad una o più altre strategie, abbassa il solo grado complessivo di vulnerabilità (ad esempio: quando una strategia di mitigazione che, pur riducendo il punteggio della vulnerabilità da "5-6" a "3-4", se il grado delle conseguenze rimane a "3", non riduce la categoria di mitigazione che resta al livello "Mitigare").

## **2. Elaborazione ed approvazione della valutazione di sicurezza.**

L'Autorità Portuale, in collaborazione con l'Autorità Marittima, per i porti ricompresi nella circoscrizione dell'A.P., o l'Ufficio del Compartimento marittimo competente per gli altri porti, elabora la valutazione di sicurezza, sentita e in costante raccordo con, l'impresa operante nell'impianto, ovvero con l'impresa concessionaria dell'impianto. Può essere elaborata un'unica valutazione per impianti aventi comuni caratteristiche ed utilizzazione.

Per l'elaborazione le Autorità competenti potranno avvalersi, se necessario, del supporto di professionalità esterne.

Ultimata l'elaborazione della valutazione di sicurezza, la stessa viene sottoposta all'approvazione del Capo del Compartimento Marittimo, il quale provvederà ad inviarla d'intesa con l'Autorità portuale per i porti ricompresi nella circoscrizione della stessa, alle imprese interessate al fine di procedere alla redazione del piano di sicurezza.

### **INDICAZIONI FORMALI**

Il documento di valutazione di sicurezza redatto tenendo conto delle Linee Guida sopra riportate sarà trasmesso alle imprese ai fini della successiva redazione del Piano di Sicurezza ed avrà il frontespizio di cui all'allegato 1 e una pagina "REGISTRAZIONE VARIANTI" come da fac-simile (allegato 2).

**COMITATO INTERMINISTERIALE PER LA SICUREZZA DEI TRASPORTI  
MARITTIMI E DEI PORTI**

-----

**AUTORITA' COMPETENTE PER LA SICUREZZA MARITTIMA**

**ORGANIZZAZIONE DI SECURITY LEGGERA (SELE ) PER GLI IMPIANTI PORTUALI  
VALUTAZIONE DI SICUREZZA**

Applicazione dell'articolo 3.3 del Regolamento (CE) n. 725/2004

**Porto di.....**

Impianto cui si riferisce la valutazione di security (denominazione) : .....

.....

Elaborato da : .....

Data preparazione : .....

Copia controllata n° ..... di ..... copie

**ESTREMI DI APPROVAZIONE**

Data di approvazione.....



## CAPITOLO III

### PIANO DI SECURITY LEGGERA (SELE)

#### 1. Generalità

Questo documento è finalizzato a fornire una guida per l'individuazione, sulla base delle risultanze della valutazione di sicurezza di cui al precedente capitolo, delle misure fisiche e/o organizzativo-procedimentali, da porre in essere nella fase di interfaccia impianto-nave.

Al fine di ottimizzare le condizioni di security, di contemperarle con la necessaria fluidità dei traffici marittimi e dell'operatività portuale, nonché di evitare duplicazioni di attività che appaiano ingiustificate, le misure di sicurezza (security) previste ed adottate dall'impianto si devono integrare con quelle della nave.

A tal fine il responsabile di sicurezza dell'impianto e quello della nave concorderanno i singoli adempimenti da porre in essere prima dell'attivazione dell'interfaccia.

Laddove, in considerazione delle peculiari caratteristiche infrastrutturali, strutturali, organizzative ed operative, emerga l'impossibilità di predisporre ed organizzare nell'impianto le attività di controllo che ordinariamente devono essere svolte nell'impianto stesso, la nave predisporrà ed adotterà opportune misure alternative sulla scorta delle presenti linee guida in accordo con l'autorità designata.

#### 1.1 **Redazione ed approvazione piano**

Il piano di sicurezza deve essere redatto da parte dell'impresa e presentato al Capo del Compartimento Marittimo, in 3 copie in formato cartaceo ed 1 copia in formato elettronico. Un'ulteriore copia è contestualmente presentata all'Ufficio di Polizia di Frontiera, se presente in loco, che ha facoltà, entro 15 giorni calendariali dalla data di presentazione, di far pervenire alla Capitaneria di Porto (ed all'A.P. per i porti di competenza) proprie osservazioni. La Capitaneria di Porto provvederà ad approvare il Piano, di intesa con l'A.P., per i porti di competenza, entro 30 giorni calendariali dalla data di presentazione.

#### 2. Individuazione dell'impianto

Ai fini dell'attività e delle misure di controllo da porre in essere le aree dell'impianto direttamente funzionali all'interfaccia con la nave sono individuate nel Piano tenendo in considerazione:

- tipologia e dimensioni delle navi che vi faranno scalo;
- operazioni che vi dovranno effettuare le navi utilizzatrici (imbarco solo carico ovvero solo passeggeri ovvero passeggeri ed automezzi);
- l'ubicazione dell'impianto e l'estensione dell'area portuale all'interno della quale l'impianto si colloca.

#### 3. Conterminazione dell'impianto

Per il solo periodo di tempo funzionale all'espletamento delle attività preordinate/connesse con l'interfaccia con una nave operativa, la zona dell'impianto portuale direttamente interessata dall'imbarco e dalla movimentazione di cose e persone è conterminata anche mediante

strutture non fisse (es. transenne stradali o simili) tali da offrire resistenza all'illecito scavalco o passaggio.

Si dovrà verificare la possibilità di ancorare al terreno le strutture di delimitazione, al fine di rendere più difficile un loro illecito spostamento/rimozione.

A cura dell'Autorità marittima, ovvero dell'A.P. dove istituita, sarà disciplinata la circolazione nell'area dell'impianto anche relativamente ai periodi in cui non è attiva l'interfaccia, con previsione nel medesimo periodo, del divieto di sosta (se possibile) nonché eventualmente di fermata.

Nel Piano sarà opportunamente richiamata la predetta regolamentazione.

#### **4. Organizzazione di security**

Il piano deve:

a) specificare l'organizzazione di security dell'impresa, inclusi i compiti del personale che ha responsabilità al riguardo;

b) fornire le generalità complete (nome e cognome) e l'indirizzo del titolare dell'impresa e del/dei responsabile/i della sicurezza nonché i loro recapiti.

Il responsabile della sicurezza e l'eventuale personale impiegato con compiti di security deve avere piena conoscenza dei compiti ad esso attribuiti e deve essere dotato dei mezzi necessari per un efficace espletamento di detti compiti.

Nella misura necessaria ai compiti assegnati (in base alle previsioni del Piano) sarà fornita al personale stesso un'adeguata formazione. L'indicazione delle modalità di formazione del personale sarà contenuta nel Piano.

Il Piano è protetto dall'accesso o divulgazione non autorizzata.

Nel Piano, se redatto in forma elettronica, sono indicate le procedure per prevenire la cancellazione, la distruzione o modifiche non autorizzate.

#### **5. Comunicazioni**

Il piano dovrebbe descrivere i sistemi di comunicazione utilizzati per le comunicazioni tra il personale addetto alla sicurezza dell'impianto e l'ulteriore personale che opera nell'impianto, il responsabile di sicurezza della nave, l'Autorità Marittima e la Polizia di Stato. Le comunicazioni possono essere effettuate con modalità diverse (radio portatile, telefoni cellulari, telefoni, sistemi di allarme / interfono, sistema a voce).

Per la scelta del sistema di comunicazione si avrà riguardo alle caratteristiche infrastrutturali, strutturali ed operative di ciascun impianto.

#### **6. Sistemi di sicurezza – equipaggiamenti**

Il piano dovrebbe accennare brevemente una descrizione sui sistemi di sicurezza e sugli equipaggiamenti utilizzati all'interno dell'impianto portuale. Per esempio:

illuminazione, allarmi o sirene, equipaggiamento di sorveglianza, come monitor video e telecamere, sistemi elettronici per l'identificazione degli accessi, combinazione di più elementi tra quelli sopra elencati.

Nel piano si indicheranno le verifiche, i test e i controlli sui sistemi ed equipaggiamenti utilizzati, da effettuarsi secondo quanto stabilito dalle specifiche del fornitore e la relativa frequenza.

## **CAPITOLO IV**

### **MISURE DI SICUREZZA: CONTROLLO ACCESSI, AREE AD ACCESSO LIMITATO, MOVIMENTAZIONE DEL CARICO, MOVIMENTAZIONE DELLE FORNITURE DI BORDO**

#### **1. Controllo accessi**

Il piano deve indicare le misure finalizzate ad assicurare, per quanto ragionevolmente possibile, che nell'impianto non vengono introdotte, se non autorizzate, armi, sostanze pericolose e comunque congegni diretti a determinare danni o distruggere, navi, e impianti portuali o provocare la morte di persone nonché deve indicare le modalità per controllare gli accessi all'impianto portuale.

##### **1.1 Identificazione delle aree d'accesso**

Il piano deve indicare:

- i punti di accesso all'impianto e le modalità per prevenire gli accessi non autorizzati per ogni livello di sicurezza;
- le modalità per l'accesso all'impianto, nonché per permanere all'interno (persone e veicoli);
- i luoghi dove effettuare i controlli del personale, i suoi effetti personali e veicoli.

##### **1.2 Frequenza del controllo di accesso**

Il piano deve stabilire la frequenza dei controlli da determinarsi tenendo a riferimento le percentuali indicate nel Programma Nazionale di Sicurezza Marittima.

##### **1.3 Requisiti per il controllo d'accesso**

Il piano deve descrivere le modalità per il controllo degli accessi in funzione del livello di security adottato. Tali misure comprendono:

- assegnare personale di guardia;
- accertare l'identità di ogni persona che desidera entrare nell'impianto portuale e che ha un legame con la nave, in particolare passeggeri, equipaggio e ospiti, controllando le relative motivazioni, verificando ad esempio istruzioni di imbarco, biglietti di viaggio, carte di imbarco, ordini di lavoro, ecc.;
- ispezionare i veicoli utilizzati dalle persone che desiderano entrare nell'impianto portuale e che hanno un legame con la nave;
- istituire eventualmente un sistema di registrazione di pass da utilizzare in base al livello di sicurezza adottato;
- vietare l'accesso alle persone che non fanno parte del personale dell'impianto portuale o non sono impiegate al suo interno, se non sono in grado di dimostrare la propria identità;
- stabilire eventuali ronde per il controllo degli accessi non utilizzati, i quali dovranno essere adeguatamente chiusi in modo da impedire il libero accesso;
- attivare eventuale illuminazione prevista per la security.

In linea di principio, l'accesso all'impianto nella fase di interfaccia con la nave è consentito solo:

- per i passeggeri, ai fini dell'imbarco, previo controllo del possesso di idoneo titolo di viaggio ed identità;

- per quanti diretti a bordo in veste di visitatori ovvero per prestare servizi alla nave che si interfaccia con l'impianto, nonché per l'equipaggio, previo controllo dell'identità e verifica della rispondenza con la nave;
- per le autorità (e rispettivo personale), previa verifica dell'identità e garantendo – in ogni caso – l'accesso rapido alle autorità che devono rispondere ad eventuali incidenti di security verificatisi nell'impianto (ovvero a bordo della nave che si interfaccia con l'impianto) nonché al personale dei servizi di pronto intervento sanitario o di safety;
- per il personale addetto alle operazioni portuali e per quello addetto a servizi che si espletano nella fase di interfaccia (es. ormeggiatori, guardie fuochi, ecc.) previa identificazione.

## **1.4 Controlli sull'accertamento dell'identità delle persone ed ispezione bagagli e veicoli**

### **1.4.1 Passeggeri e relativi bagagli**

- controllo biglietto d'imbarco e possesso documento identità dei passeggeri imbarcanti per eventuale riscontro;
- utilizzo di eventuale Metal Detector fisso o portatile;
- controllo, possibilmente mediante X-Ray scanner, dei bagagli ed identificazione degli stessi;

### **1.4.2 Visitatori**

- controllo identità e rispondenza con elenco persone di previsto arrivo;
- utilizzo di eventuale Metal Detector fisso o portatile;
- controllo del bagaglio personale, possibilmente mediante X-Ray scanner;
- registrazione degli ingressi/uscite nonché impiego di "pass" a livelli di sicurezza SL2 e SL3;
- fornire informazioni sulla security (es.: identificazione e relativo divieto per aree ad accesso limitato)
- limitazione o sospensione dell'ingresso ai livelli di sicurezza SL2 e SL3 ed eventualmente accompagnamento dei visitatori.

### **1.4.3 Autorità**

- verificare identità;
- fornire informazioni sulla security (es.: identificazione delle aree ad accesso limitato);
- accompagnamento se necessario e richiesto;
- garantire l'accesso rapido alle autorità che devono rispondere all'incidente di security ovvero ai servizi di pronto intervento sanitario o di safety.

### **1.4.4 Veicoli**

Provvedere al controllo dei veicoli da caricare a bordo.

I controlli consisteranno nella verifica, al momento dell'accesso degli stessi all'impianto, a cura degli addetti alle operazioni di controllo, della concordanza tra il titolo autorizzativo (permesso d'accesso, titolo di imbarco) e gli estremi del veicolo stesso quale la targa ed eventualmente la marca e il tipo.

#### **1.4.5 Bagagli non accompagnati**

- controllo, possibilmente mediante X-Ray scanner, e relativa identificazione (connessione con il proprietario) degli stessi;
- limitazione o sospensione della movimentazione ai livelli di security SL2 e SL3.

## **2. Aree ad accesso limitato**

Il piano individua le aree ad accesso limitato al fine della loro tutela e di:

- Prevenire o dissuadere accessi non autorizzati;
- Tutelare le persone autorizzate ad accedervi.

### **2.1 Individuazione di aree ad accesso limitato**

Le aree ad accesso limitato sono quelle più sensibili ai fini della security quali quelle di seguito esemplificamente elencate:

- cabine di trasformazione e di distribuzione elettrica;
- locali dove sono presenti gruppi di continuità;
- locali dove è presente l'Hardware di sistemi CCTV (se esistenti);
- depositi di stoccaggio di merci pericolose;
- i luoghi in cui sono conservate le informazioni sensibili sotto il profilo della sicurezza;
- le zone in cui sono conservate le apparecchiature di sorveglianza e di sicurezza;
- gli impianti di radio e telecomunicazioni, di alimentazione elettrica ed idrica.

Nell'eventualità di localizzazione nell'impianto di aree quali quelle sopra indicate, le stesse sono identificate opportunamente, a cura del responsabile di sicurezza dell'impianto o a cura dei gestori delle predette aree, con idoneo cartello riportante dizione quale quella che esemplificativamente si riporta:

“Area ad accesso limitato –  
Ingresso consentito al solo personale  
in possesso di specifica autorizzazione”

### **2.2 Misure di sicurezza per le aree ad accesso limitato**

Il piano deve descrivere le procedure che stabiliscono le misure di sicurezza per le aree ad accesso limitato.

Le procedure devono tenere conto del livello di security in atto e, di massima prevedere:

- modalità per Identificare il personale autorizzato ad accedervi;
- condizioni di accesso;
- controlli durante le fasi di carico e scarico di veicoli; movimento dei carichi, ecc.

In linea di massima Il controllo delle aree ad accesso limitato sarà pianificato in funzione del livello di security in atto e si estrinsecherà secondo diverse possibili modalità alternative (es. ronde, impianti CCTV – se disponibili, ecc.) scelte tenendo conto della realizzabilità economica nonché dell'attività di monitoraggio e pattugliamento di per sé garantite dalle forze di polizia presenti in porto.

### **3. Movimentazione del carico (se applicabile)**

Le misure e le procedure di controllo sui carichi che entrano nell'impianto ai fini dell'imbarco sono finalizzate a mitigare il rischio di security tenendo comunque presente le esigenze commerciali dell'impianto e della nave che si interfaccia.

Tali misure sono differenziate in relazione alla tipologia di carico e di nave.

Il piano deve descrivere le procedure e le misure di sicurezza relative alla movimentazione del carico, alcune delle quali possono essere applicate in collegamento con le navi, al fine di:

- Prevenire le manomissioni dolose del carico;
- Prevenire l'imbarco di carichi non previsti;
- Identificare i carichi;
- Identificare i carichi accettati per il deposito temporaneo in aree ad accesso limitato;
- Restringere, se necessario, l'ingresso di carichi la cui data di imbarco non è stata confermata;
- In caso di frequenti operazioni di carico con la stessa nave, coordinare le misure di sicurezza in conformità a procedure prestabilite.

#### **3.1 Misure di sicurezza per la movimentazione del carico**

Le misure di sicurezza applicabili in particolare comprendono:

- controlli documentali all'ingresso;
- controlli sulla rispondenza del carico con la polizza del carico fornita;
- verifiche visive sull'integrità dei sistemi di chiusura delle diverse unità di carico.

##### **3.1.1 Requisiti supplementari per imbarco/sbarco merci pericolose**

Il Piano deve descrivere le procedure per implementare le misure di sicurezza per la movimentazione di merci pericolose, ai vari livelli di security, al fine di assicurare un adeguato livello di sicurezza a persone e cose presenti nell'impianto nella fase di movimentazione delle merci pericolose.

#### **3.2 Misure di sicurezza per la movimentazione delle forniture di bordo**

Il piano deve descrivere le procedure per implementare le misure di sicurezza per la consegna delle forniture di bordo ai differenti livelli di sicurezza adottati.

Le misure di sicurezza applicabili per controllare la consegna delle provviste di bordo in particolare comprendono:

- verifica di massima della rispondenza delle forniture di bordo con le richieste della nave;
- identificazione del conducente dell'eventuale veicolo;
- ispezione delle forniture di bordo, al fine di verificare l'integrità delle stesse mediante:
  - ispezione visiva;
  - esame fisico;
  - altre modalità.

## CAPITOLO V

### PROCEDURE PER I PRINCIPALI INCIDENTI DI SECURITY

#### 1. GENERALITA'

Scopo di questo capitolo è quello di dettare linee guida che possano essere utilizzate nella gestione di incidenti di security rilevanti. Per incidente di security rilevante si intende un particolare evento derivante da atto illecito doloso o una serie di circostanze sospette ad esso collegabili che minaccino la sicurezza (security) di un impianto e delle persone comunque in esso presenti.

Il responsabile dell'impianto nel redigere procedure e nell'impartire istruzioni, dovrebbe considerare la possibilità di dover dirimere, in base al professionale giudizio, eventuali contingenti e non preventivabili conflitti tra le esigenze di safety e di security.

Resta salva la potestà decisionale del responsabile, nell'ambito delle proprie competenze e responsabilità, in assenza di disposizioni da parte delle competenti autorità, di adottare misure o intraprendere attività non individuate nelle presenti linee guida qualora, a seguito di valutazione dell'evento, si ritenga ciò ragionevole ed opportuno per ridurre l'entità del rischio. Sono da annoverare tra gli incidenti di security rilevanti (ISR) :

- allarme bomba/rinvenimento oggetti sospetti (IED = Improvised explosive devices);
- rinvenimento armi e munizioni;
- impossessamento e sequestro.

In ogni caso lo sforzo organizzativo dovrebbe essere commisurato a realistici scenari tenendo altresì in considerazione:

- la tipologia ed entità dei traffici;
- la presenza di forze dell'ordine.

#### 2. PIANIFICAZIONE DI CONTINGENZA

##### 2.1 Scenari

Ferme restando le pianificazioni di emergenza del Ministero dell'Interno sarebbe buona pratica che da parte del responsabile dell'impianto venga sviluppata una semplice ma concreta "pianificazione di contingenza" per i sotto riportati scenari:

- minaccia bomba;
- ricerca di bomba/oggetti sospetti (IED);

- sgombero di sezioni/aree dell'impianto;
- evacuazione dell'impianto.

La pianificazione di contingenza dovrebbe includere l'elencazione delle attività essenziali da svolgere e delle persone da impiegare in tali attività, nonché gli enti/persone da contattare incluso il personale della Polizia di Stato o delle altre Forze di Polizia aventi competenza territoriale sullo scalo in questione nelle more del loro intervento .

Sarebbe opportuno ottimizzare tale pianificazione di contingenza di security con quella eventualmente già esistente di safety. Ciò per evitare duplicazioni e/o discrasie tra le stesse.

## **2.2 Evacuazione**

Le procedure per l'evacuazione sono una parte essenziale del piano di contingenza. Queste procedure risulterebbero di grande utilità in eventi d'emergenza sia di security che di safety. Di seguito si riporta una lista di alcuni aspetti che dovrebbero essere considerati nell'individuare le procedure d'evacuazione più rispondenti alle esigenze di ciascun impianto:

- conformazione delle eventuali strutture;
- numero totale delle persone che potrebbero essere presenti nell'impianto;
- presenza di persone per le quali potrebbero esservi specifiche necessità (es. età, stato fisico ecc.);
- nel caso di strutture ove normalmente possano esservi numerose persone, si dovrebbe prestare attenzione ad individuare una via alternativa di fuga, in direzione diversa da quella principale, nel caso la stessa risultasse bloccata.

## **2.3 Consapevolezza**

Il responsabile dell'impianto dovrebbe incentivare la consapevolezza del personale sull'importanza di un'attenta vigilanza e di un professionale approccio all'esigenza di incrementare il livello di sicurezza (security) nel settore del trasporto marittimo nazionale. In tale ottica la politica aziendale dovrebbe contemplare l'aspetto dell'indottrinamento e della famigliarizzazione dei propri dipendenti ricorrendo anche a periodiche, semplici ma efficaci attività di addestramento/esercitazione. A richiesta, l'Autorità designata e la Polizia di Stato potrebbero intervenire a supporto di tali attività.

# **3. RAPPORTAZIONE DEGLI INCIDENTI DI SECURITY RILEVANTI**

## **3.1 Procedure**

L'impianto dovrebbe avere procedure interne per la segnalazione/rapportazione degli incidenti di security rilevanti (ISR) che soddisfino le seguenti esigenze:

- consentire al personale di segnalare gli ISR al responsabile dell'impianto;
- consentire al responsabile dell'impianto, previa una valutazione dei fatti, di riportare le rilevanti situazioni alle Autorità di Polizia competenti.

### **3.2 Segnalazione interna**

Il personale dovrebbe essere consapevole della procedura di segnalazione. Tale procedura dovrebbe essere semplice da seguire e tale da incoraggiare l'attività di segnalazione.

Il responsabile dell'impianto dovrebbe procedere ad una verifica-accertamento, per ogni segnalazione di ISR, nella misura considerata necessaria in base al suo professionale giudizio.

### **3.3 Rapportazione esterna**

Per la rapportazione degli ISR il responsabile dell'impianto dovrebbe poter contare su aggiornate schede contenenti i numeri utili per contattare le rilevanti autorità. Tali schede dovrebbero contenere le indicazioni dei punti di contatto, preferibilmente relative a più di un sistema di comunicazione.

All'uopo presso le Autorità designate potrebbero essere tenuti appositi elenchi dai quali gli impianti possano eventualmente attingere informazioni utili per la compilazione/aggiornamento delle proprie schede.

## **4 ALLARME BOMBA, RINVENIMENTO OGGETTI SOSPETTI**

### **4.1 Premessa**

Lo scopo del presente documento è quello di fornire alcune nozioni e principi utili per ridurre la possibilità di introduzione di ordigni esplosivi e di dare istruzioni sulle modalità di azione in caso di allarme. Tali indicazioni hanno carattere generale e forniscono elementi guida da ottimizzarsi attraverso l'applicazione di misure organizzative che meglio rispondano alle peculiarità dello specifico impianto e della contingente situazione.

Occorre tener sempre presente che la visibilità (percezione che dall'esterno si ha dell'attività) di misure di prevenzione, anche parziali, può risultare determinante in quanto scoraggia i male intenzionati, generalmente più propensi a prediligere obiettivi facili e senza rischio o più vulnerabili.

Gli ordigni esplosivi improvvisati sono composti da cariche, sistemi di innesco estremamente vari e diversi sia nel design che nella tecnica e nelle potenzialità distruttive. Di seguito si riportano le attività ritenute essenziali in caso di rinvenimento di un possibile IED:

- **NON TOCCARE L'OGGETTO, NON TENTARE DI RIMUOVERLO;**
- **NON PROVOCARE VIBRAZIONI;**
- **NON VARIARE LO STATO DI ILLUMINAZIONE SULL' IED;**

- **NON VARIARE IL CAMPO MAGNETICO (NON UTILIZZARE RADIO O CELLULARI ecc.) NEI PRESSI DELL'IED;**
- **FAR ALLONTANARE LE PERSONE DAL LOCALE INTERESSATO E DA QUELLI IMMEDIATAMENTE ADIACENTI (ORIZZONTALI/ VERTICALI);**
- **AVVISARE IL RESPONSABILE DELL'IMPIANTO.**

## 4.2 Eventi IED

Un evento IED può avere origine da:

- segnalazione, anche anonima, o notizia di intelligence;
- scoperta di un oggetto sospetto nell'impianto o in prossimità della nave.

### a) segnalazione telefonica o radio

Chi risponde dovrebbe cercare di ottenere la maggiore quantità di informazioni possibili quali:

- elementi riconoscitivi, provenienza della persona che chiama (accento, rumori di fondo, ecc. );
- tipo di ordigno e sua localizzazione;
- ora prevista di esplosione.

Sarebbe opportuno che, ove possibile, la telefonata/conversazione venga trattata da un responsabile.

Al fine di favorire la raccolta di informazioni nella maniera più completa potrà essere compilato il form in **allegato 3**, che dovrebbe essere sempre disponibile presso gli eventuali apparati radio e centralino telefonico.

### b) segnalazione scritta

In caso di segnalazione scritta è importante, al fine di favorire le indagini da parte delle autorità competenti, che oltre al contenuto venga conservata anche la busta o l'involucro prestando la massima attenzione a non modificare o compromettere la possibilità di rilevare eventuali impronte digitali.

Nel caso di impiego della posta elettronica comando di bordo si dovrebbe curare il "salvataggio" dell'e-mail ed avvisare i competenti organi della Polizia di Stato.

### c) scoperta di un oggetto sospetto

La scoperta di un oggetto sospetto può essere il risultato di una scoperta casuale o di un'attenta ricerca.

**N.B.** Fino a quando non si sia dimostrato che l'eventuale oggetto rinvenuto sia innocuo, lo stesso dovrebbe essere considerato come un ordigno IED e pertanto si dovrebbe:

- evitarne la rimozione;
- evitare di coprirlo o racchiuderlo in un contenitore;

- evitare di variare l'assetto delle luci e non apportare sensibili variazioni nel campo magnetico derivanti dall'impiego di apparecchiature radio o di telefonia mobile;
- aprire le aperture (porte, finestre ecc) delle aree limitrofe per favorire lo sfogo dell'eventuale esplosione.

### 4.3 Precauzioni anti IED

Sarebbe opportuno, previo un appropriato indottrinamento del personale, prestare sempre attenzione ad eventuali oggetti (per es. bagagli) ed alle auto lasciate incustodite (all'imbarco o allo sbarco) per le quali non venga prontamente individuato il proprietario.

### 4.4 Modalità di reazione in caso di allarme IED

#### 4.4.1 Reazione

Le presenti linee guida sono da considerarsi indicazioni di carattere generale la cui applicabilità dipende dalle singole realtà.

Il responsabile dell'impianto dovrebbe considerare che una tempestiva e corretta informazione alla Polizia di Stato consentirebbe a quest'ultima di intervenire e di dare le istruzioni ritenute più opportune per il singolo caso. Per tanto le sottoriportate indicazioni potrebbero essere d'ausilio al responsabile dell'impianto nelle circostanze in cui non si sia potuto ancora stabilire il contatto con il precitato organo di Polizia.

Il personale dovrebbe essere addestrato sulle procedure ed attività da porre in essere in relazione alla specifica situazione.

A seguito di una segnalazione o del ritrovamento di un ordigno, si dovrebbe disporre per l'effettuazione di chiamate con semplici parole in codice, da stabilirsi a cura di ciascun impianto, che dovranno significare: EMERGENZA - ALLARME IED - TUTTO IL PERSONALE VERIFICHI L'EVENTUALE PRESENZA DI OGGETTI SOSPETTI NEL PROPRIO POSTO DI LAVORO ovvero altro similare ordine previsto dalle pertinenti procedure.

Qualora le dimensioni e la strutturazione dell'impianto rendano ciò possibile e ragionevole, un punto di coordinamento delle attività connesse alla segnalazione IED dovrebbe essere stabilito in un luogo ritenuto sicuro. Esso dovrebbe essere preposto allo svolgimento delle seguenti attività:

- raccolta, valutazione e valorizzazione delle informazioni;
- direzione dell'attività del personale fino all'arrivo della competente Autorità di Polizia;
- coordinamento delle azioni con le autorità competenti.

Nel punto di coordinamento sarebbe opportuno che siano resi disponibili i materiali necessari al personale incaricato di eseguire la ricerca sistematica dell'eventuale ordigno (se possibile: elmetti, dotazioni a sicurezza intrinseca, maschere per fumi intensi, eventuali luci schermate rosse, elenco del personale impiegato nei vari team di ricerca, rotoli di nastro bicolore per la segnalazione delle zone interdette, cartellini colorati ecc...).

Sarebbe altresì opportuno che siano assicurate le comunicazioni tra il personale del punto di coordinamento, quello delle squadre di ricerca (radio portatili, cellulari ecc...) da poter attivare alla bisogna ed in luoghi ritenuti sicuri.

Nel punto di coordinamento dovrebbero essere altresì disponibili: i piani/le planimetrie dell'impianto e delle strutture, l'eventuale piano di contingenza nonché l'elenco del personale presente.

Il responsabile dell'impianto ovvero chi ha assunto la direzione delle operazioni dovrebbe prevedere:

- la sospensione delle attività non ritenute essenziali all'interno dell'impianto e, per quanto possibile, nelle sue vicinanze;
- l'approntamento degli eventuali sistemi antincendio;
- l'informazione alle navi presenti della corrente situazione, richiedendo, se del caso:
  - la sospensione delle attività non essenziali;
  - che le persone presenti a bordo non scendano nell'impianto;
  - che le navi interfacciate con l'impianto apprestino quanto necessario per lasciare gli ormeggi.

#### **4.4.2 Sgombero dell'area ed evacuazione dell' impianto**

Lo sgombero delle persone dall'area interessata dall'eventuale rinvenimento dell'oggetto IED dovrebbe essere disposto dal personale che effettua la ricerca. L'evacuazione delle persone presenti nell'impianto dovrebbe avvenire all'ordine del responsabile dell'Autorità di Polizia che ha assunto la direzione delle operazioni, ovvero del responsabile dell'impianto che provvederà, comunque a darne immediata informazione alla citata autorità.

Sarebbe opportuno che il personale evacuato rimanga a disposizione nei pressi dell'impianto fino all'arrivo delle forze dell'ordine per la realizzazione di un eventuale cordone di sicurezza.

Il responsabile dell'impianto ovvero chi ha assunto la direzione delle operazioni dovrebbe inoltre:

- richiedere alla competente Autorità marittima l'allontanamento delle navi nelle immediate vicinanze;
- far ricorso ai più opportuni sistemi di informazione (impianto di informazione pubblica) per la diramazione delle istruzioni alle persone presenti;
- procedere ad una spunta delle persone evacuate.

#### **4.4.3 Rapportazione dell'allarme**

Il responsabile dell'impianto dovrà prontamente riportare l'evento alla Polizia di Stato.

Nel caso la situazione lo consenta, sarebbe opportuno estendere l'informazione alle altre Forze di Polizia che possano utilmente intervenire, all'Autorità marittima ed ai Vigili del Fuoco.

Per la registrazione delle più salenti attività, il responsabile dell'impianto valuterà l'opportunità di impiegare la allegata check list in **allegato 4)** che potrà essere integrata in base alle singole esigenze.

## 4.5 Ricerca di IED

Le presenti indicazioni dovrebbero essere considerate quando, in assenza di specifiche disposizioni da parte della competente Polizia di Stato ovvero di istruzioni da parte di altre Forze di Polizia, il responsabile dell'impianto ritenga ciò necessario.

### 4.5.1 Prima ricerca

Il personale da impiegare nell'esecuzione della ricerca IED e le modalità di ricerca dipendono dalla tipologia dell'impianto e dalla composizione quantitativa e qualitativa del personale.

La ricerca dovrebbe essere eseguita lungo percorsi preventivamente definiti in modo da comprendere locali tra loro omogenei per ubicazione.

Si dovrebbe inoltre prevedere la possibilità di parzializzare i percorsi (es. zona A, percorsi: A1, A2, A3,...) in modo da privilegiare la rapidità della ricerca. La parzializzazione consentirebbe inoltre di indirizzare la ricerca in specifiche aree.

Sarebbe opportuno che all'esecuzione della ricerca vengano destinati team composti da due persone ciascuno, di cui uno scelto tra coloro che normalmente operano nelle zone interessate, in quanto più idonei alla rilevazione di eventuali oggetti estranei. Nell'esecuzione della ricerca il personale dovrebbe essere dotato delle dotazioni di protezione individuali di cui al precedente punto 4.4.1, di adesivi (anche di tipo post-it) di diverso colore, utili per la segnalazione di stato dei diversi locali (prima e seconda ricerca) e di questionario per il rilievo delle caratteristiche dell'ordigno eventualmente rinvenuto (**Allegato 5**).

La ricerca dovrebbe essere eseguita:

- evitando movimenti bruschi e verificando l'eventuale presenza di ostacoli lungo il proprio percorso prima di spostarsi da un punto di osservazione ad un altro. In particolare, nell'affrontare passaggi raramente frequentati, sarebbe opportuno accertare l'assenza di fili tesi a varie altezze in corrispondenza di potenziali punti di transito;
- evitando di variare l'assetto delle luci e di apportare sensibili variazioni nel campo magnetico derivanti dall'impiego di apparecchiature radio o di telefonia mobile;
- ponendo la massima attenzione alla presenza di rumori insoliti/meccanici (es. ticchettio);
- effettuando una ricerca sistematica, attraverso la separazione dello spazio in tre differenti strati, a partire dal basso verso l'alto, da verificare in successione.

Qualora in un locale, a seguito di una prima ricerca, non sia stata rilevata la presenza di oggetti sospetti, l'esecutore della ronda dovrebbe procedere a:

- chiudere la porta di accesso al locale curando che non sbatta;
- apporre l'apposito segnale previsto (adesivo di colore giallo);
- riferire l'esito al punto di coordinamento IED

Se è stato annunciato un orario di esplosione, la ricerca dovrebbe essere interrotta anticipatamente (15 minuti prima dell'ora comunicata) per permettere l'eventuale evacuazione delle persone ed il completamento delle eventuali possibili misure di difesa passiva tendenti alla riduzione dei danni, lasciando proseguire la ricerca al personale artificiere eventualmente intervenuto.

#### **4.5.2 Scoperta**

Qualora in un locale sia stata rilevata la presenza di un oggetto sospetto, l'esecutore della ricerca dovrebbe procedere come segue:

- non toccare l'oggetto, non tentare di rimuoverlo, non immergerlo nell'acqua o racchiuderlo in un contenitore;
- evitare di variare l'assetto delle luci e non apportare sensibili variazioni nel campo magnetico derivanti dall'impiego di apparecchiature radio o di telefonia mobile;
- mantenersi a distanza dall'oggetto cercando di rilevarne il maggior numero di caratteristiche in base al questionario in dotazione;
- abbandonare il locale con cautela evitando di urtare o far cadere oggetti lungo il percorso;
- contraddistinguere il locale con il segnale di pericolo (adesivo di colore rosso), provvedendo a segnalare l'interdizione all'accesso mediante nastro bicolore;
- lasciare aperte tutte le porte lungo il percorso di uscita;
- far allontanare tutte le persone che si trovino nelle aree immediatamente adiacenti e lungo il percorso di ritorno al punto di coordinamento IED;
- avvisare il punto di coordinamento IED

Il responsabile dell'impianto dovrebbe tempestivamente riportare il fatto all'autorità competente di cui al precedente punto 4.4.3 ed attenersi alle eventuali disposizioni impartite.

A seguito della localizzazione dell'eventuale ordigno, la portelleria dei locali adiacenti dovrebbe essere lasciata aperta in modo da permettere lo sfogo dell'eventuale esplosione verso l'esterno.

L'isolamento elettrico totale del locale dove è stato individuato l'ordigno andrebbe evitato, al fine di non apportare sensibili variazioni nel campo magnetico e non

variare l'assetto delle luci, fatto che potrebbe attivare eventuali inneschi fotosensibili. Occorrerebbe però predisporre per assicurare l'immediata disalimentazione del locale o dell'area a seguito di esplosione o di specifica richiesta del personale artificiere eventualmente intervenuto.

#### **4.5.3 Ripetizione della ricerca**

In caso di esito negativo della prima ricerca, sarebbe opportuno ripetere la ricerca sostituendo, se possibile, il personale incaricato. In questo caso l'avvenuta ispezione di un locale ed il nuovo esito negativo potrebbero essere segnalati con l'apposizione dell'apposito segnale (adesivo di colore verde).

In caso di esito positivo della prima ricerca potrebbe comunque essere opportuno ripetere il controllo nelle altre zone dell'impianto per verificare l'eventuale presenza di ulteriori IED.

#### **4.5.4 Intervento di artificieri**

Il personale artificiere, una volta intervenuto, assumerà il controllo operativo per la gestione dell'intervento e la neutralizzazione e/o rimozione dell'ordigno.

## **5. ARMI, MUNIZIONI ED ESPLOSIVI**

### **5.1 Generalità**

Ferme restando le disposizioni del Codice penale, del T.U.L.P.S. e delle altre leggi speciali, nonché degli articoli 193 e 1199 del Codice della navigazione e dell'articolo 384 del relativo regolamento (Navigazione marittima), per gli scopi del presente documento:

- è arma da fuoco/sparo ogni oggetto da cui un dardo, un proiettile o un missile possa essere eiettato usando un propellente;
- è altresì arma propria quella da getto (lancia, arco, balestra, fucile subacqueo, ecc...), quella da taglio o punta (spada, pugnale, ecc...) e quella dirompente (bomba a mano ecc...).

Le precedenti definizioni includono ogni arma disattivata o riproduzione di arma. Sono esclusi quegli oggetti che sono evidenti giocattoli per bambini.

### **5.2 Trasporto armi e munizioni**

Il porto ed il trasporto delle armi in genere è compiutamente disciplinato dalla vigente normativa. Per l'imbarco a bordo delle navi italiane, la richiamata normativa speciale del Codice della navigazione e del relativo regolamento d'esecuzione prescrive specifiche disposizioni. Con le "Istruzioni pesanti di security per le navi" sono state divulgate migliori pratiche per la gestione di questo particolare problema.

Per quanto sopra, il responsabile dell'impianto dovrebbe prevedere procedure che consentano di segnalare le situazioni dalle quali possano scaturire incidenti di security

rilevanti ( es.: introduzione abusiva di armi) i sia alla competente Autorità di polizia sia alla nave affinché la stessa possa applicare quanto previsto. Onde consentire un'opportuna informazione dell'utenza, il responsabile dell'impianto dovrebbe individuare un'idonea forma di avviso (es.: cartellonistica ecc.) da esporre presso i punti individuati per la vigilanza e, per quanto possibile, presso le eventuali biglietterie.

### **5.3 Rinvenimento armi e munizioni**

Il responsabile dell'impianto dovrebbe assicurare che il personale dello stesso sia consapevole della pericolosità connessa con la presenza di armi e munizioni e della necessità di assicurare una discreta ma continua vigilanza.

Per il caso di rinvenimento di armi o munizioni dovrebbero essere individuate specifiche procedure per consentire:

- la rilevazione sommaria dei dati salienti (tipologia, ubicazione, memorizzazione delle persone presenti nelle immediate vicinanze ecc...);
- la rapida segnalazione dell'evento al responsabile dell'impianto;
- l'allontanamento dall'area interessata delle persone non appartenenti al personale dell'impianto;
- il piantonamento dell'area per assicurare che le armi e le munizioni non vengano toccate o rimosse se non a seguito di disposizioni delle competenti autorità;
- la tempestiva rapportazione alla Polizia di Stato.

## **6. IMPOSSESSAMENTO E SEQUESTRO**

Anche le presenti migliori pratiche sono da considerarsi indicazioni di carattere generale la cui applicabilità dipende dalle singole realtà.

Il responsabile dell'impianto dovrebbe considerare che una tempestiva e corretta informazione alla Polizia di Stato consentirebbe a quest'ultima di intervenire e di dare le istruzioni ritenute più opportune per il singolo caso. Per tanto, le sottoriportate indicazioni potrebbero essere d'ausilio al responsabile dell'impianto nelle circostanze in cui non si sia potuto ancora stabilire il contatto con il precitato organo di Polizia. Per quanto possibile, ogni sforzo dovrebbe essere fatto per trasmettere alle autorità competenti ogni utile informazione (Natura dell'attacco, numero degli attaccanti, armi impiegate o ostentate, presenza ostaggi, danni alle persone, ecc..).

Nell'applicare gli indirizzi di seguito riportati, il personale dell'impianto dovrebbe essere consapevole che i vari incidenti di security rilevanti sono caratterizzati da elementi soggettivi quali, per esempio, lo scopo dell'atto (simbolico, dimostrativo ecc...) e la personalità degli attaccanti (motivazione, esperienza ecc...).

Vi deve, quindi, essere la consapevolezza che la valutazione dei singoli eventi non possa prescindere da un professionale apprezzamento delle contingenti situazioni. Fatto che potrebbe suggerire l'opportunità di uno scostamento dalle prassi raccomandate.

Le opzioni disponibili al personale dell'impianto dipenderanno dalle finalità e metodiche dell'attacco (terrorismo o azioni criminali d'altra natura) e dagli strumenti di pressione (Ostaggi) impiegati dagli attaccanti. In generale non dovrebbe essere presa in considerazione l'ipotesi di effettuare sortite ovvero di tentare la cattura di uno o più degli attaccanti. Potrebbe invece risultare d'ausilio per le Forze dell'ordine, specie nel caso di punto di sorveglianza remoto, attivare, ove disponibili, tutti i sistemi di registrazione (CCTV ecc..) cercando di rendere il meno evidente possibile tale funzionamento.

Qualora gli attaccanti abbiano guadagnato il controllo dei punti nevralgici dell'impianto e/o abbiano catturato ostaggi, il responsabile dell'impianto ed il personale dovrebbero cercare di mantenere la calma anche per rassicurare gli eventuali passeggeri/visitatori.

Ove venga deciso o venga imposto di radunare le persone presenti in punti di raccolta, si dovrebbe cercare di far confluire la scelta verso quei punti che rispondano al requisito della presenza di una via di sfuggita alternativa alla principale.

Il responsabile dell'impianto dovrebbe essere consapevole che vi possono essere molteplici circostanze nelle quali l'assecondare le richieste degli attaccanti potrebbe essere la sola ragionevole alternativa e che ogni resistenza o ostruzionismo potrebbero essere inutili e pericolosi. Ciò risulta particolarmente rilevante nel caso di presa di ostaggi da parte degli attaccanti. In tale circostanza, in assenza di specifiche istruzioni da parte delle autorità competenti, il personale dell'impianto dovrebbe dimostrare un atteggiamento fermo ma collaborativo prestando attenzione a particolari quali:

- la rapidità, ma non la foga, nel dimostrare di tentare di soddisfare le richieste fatte dagli attaccanti;
- l'impostazione del timbro di voce calmo ma sonoro;
- l'evitare che un insistente sguardo diretto possa essere interpretato quale segnale di sfida;
- l'evitare di avvicinarsi troppo agli attaccanti, se del caso arretrando lentamente o cedendo il passo;
- il porre particolare attenzione al linguaggio utilizzato o a pratiche (es. : uso di alcolici) che possano essere considerate offensive.

**INFORMAZIONI DA RACCOGLIERE IN CASO DI COMUNICAZIONE  
DI BOMBA ALL' INTERNO DELL' IMPIANTO**

RUMORI DI FONDO (motori, musica, traffico, lavori, ecc.) ?
UOMO \ DONNA \ RAGAZZO \ RAGAZZA ? FASCIA D'ETA' APPROSSIMATIVA
LINGUA \ DIALETTO ?
ACCENTO PARTICOLARE ?
TONO DI VOCE (ALTO, NORMALE, ECCITATO, CALMO) ?
E' UNA VOCE FAMILIARE ?
E' UNA VOCE DISTORTA (FAZZOLETTO) ?

<b>NOTIZIA (se possibile dare l'impressione di cattiva comprensibilità, cercare di far ripetere la notizia e sillabare mentre si scrive)</b>

<b>PROVA AD OTTENERE LE SEGUENTI INFORMAZIONI (poni le domande nel seguente ordine):</b>
PERCHE' E' STATA MESSA LA BOMBA?
QUANDO ESPLODERA' LA BOMBA?
CHE FORMA HA LA BOMBA?
DOVE E' STATA MESSA LA BOMBA?
CHI SEI?
DA DOVE STAI CHIAMANDO?

<b>COMPLETA CON:</b>
MEZZO DI RICEZIONE
ORARIO DI RICEZIONE DELLA CHIAMATA
NOME \ COGNOME OPERATORE

DA CONSEGNARE IMMEDIATAMENTE AL RESPONSABILE DELL' IMPIANTO

**C H E C K L I S T**  
**M I N A C C I A B O M B A**

<b>MISURA DI SECURITY</b>	<b>NOTE</b>
Alertare il personale usando il Public Address System o altro mezzo ritenuto idoneo.	
Rapportare alla Polizia di Stato o, in assenza, alle altre forze di polizia.	
Informare le altre Autorità: CC, GdF, CP, AP, Vigili del Fuoco.	
Sospendere le operazioni non essenziali.	
Approntamento degli impianti antincendio.	
Approntamento disalimentazione elettrica a zone.	
Richiesta alle navi di approntamento manovra per lasciare l'ormeggio.	
Stabilire team e zone ricerca IED. Distribuire dotazioni.	
Inizio prima ricerca.	
In caso di rinvenimento IED, sgombero e segnalazione dell'area interessata.	
Ripetizione ricerca.	
Evacuazione passeggeri e visitatori.	
Evacuazione personale non essenziale.	
Evacuazione generale.	
Altro.	

**QUESTIONARIO RILIEVO CARATTERISTICHE  
DEL POSSIBILE IED**

<b>LOCALE RITROVAMENTO</b>			
<b>POSIZIONE NEL LOCALE</b>			
<b>FORMA DELL'OGGETTO</b>			
<b>DIMENSIONI APPROSSIMATE</b>			
<b>EVENTUALI APPENDICI</b>	<b>SI</b>	<b>NO</b>	
<b>CAVI VISIBILI</b>	<b>SI</b>	<b>NO</b>	
<b>EVENTUALI RUMORI</b>	<b>SI</b>	<b>NO</b>	
<b>EVENTUALI ODORI</b>	<b>SI</b>	<b>NO</b>	
<b>EVENTUALI SISTEMI DI RIZZAGGIO</b>	<b>SI</b>	<b>NO</b>	

ORA RILIEVO .....

NOME / COGNOME OPERATORE .....

DA CONSEGNARE IMMEDIATAMENTE AL RESPONSABILE DELL' IMPIANTO

## CAPITOLO VI

### NUMERI UTILI PER LA RICHIESTA DI INFORMAZIONI E LA RAPPORTAZIONE DI INCIDENTI DI SECURITY PER GLI IMPIANTI PORTUALI OPERATIVI

#### 1. GENERALITA'

Scopo di questo capitolo è quello di individuare alcune delle caratteristiche delle comunicazioni che possono essere utilizzate nella reportazione di incidenti di security rilevanti.

Si ritiene comunque che la disponibilità di aggiornati elenchi dei vari punti di contatto sia l'indispensabile premessa per un efficiente interscambio anche delle altre informazioni attinenti la maritime security più in generale.

Il responsabile dell'impianto nel redigere procedure e nell'impartire istruzioni, dovrebbe considerare la necessità di dirimere, in base al professionale giudizio, eventuali contingenti e non preventivabili conflitti tra le esigenze di safety e quelle di security.

#### 2. LISTE PUNTI DI CONTATTO

L'impianto dovrebbe poter contare su dati aggiornati dei vari punti di contatto delle autorità, degli enti e degli altri soggetti rilevanti, in materia di security.

Il responsabile dell'impianto dovrebbe procedere alla redazione di schede riportanti i più salienti dati dei vari punti di contatto. Tali schede potrebbero essere:

- redatte sulla falsa riga del fac-simile riportato in **Allegato 6**;
- integrate con altri dati ritenuti eventualmente necessari/opportuni;

Le schede dei punti di contatto dovrebbero essere tenute costantemente aggiornate nella consapevolezza che la pronta e corretta individuazione del soggetto a cui fornire o richiedere l'informazione normalmente consente di ridurre:

- il tempo necessario per la gestione della comunicazione;
- il margine d'errore nella valutazione dei contenuti della comunicazione, venendo evitate attività di "rilancio/ponte" da parte dei soggetti non direttamente competenti.

#### 3. MEZZO DI COMUNICAZIONE

Nell'individuazione del mezzo di comunicazione da impiegare per lo scambio di informazioni di security, il responsabile dell'impianto dovrebbe considerare fattori quali:

- la disponibilità di sistemi che offrano un'adeguata copertura (es.: geografica) tra il trasmittente ed il ricevente;

- l' idoneità del sistema a far transitare l'informazione qualora la stessa rivesta carattere di riservatezza;
- l' idoneità del sistema a far transitare l'informazione "da punto a punto" qualora sia ritenuto opportuno che la sua conoscenza non debba essere aperta a molti in maniera indiscriminata (es.: Broadcasting).

Nella scelta del "media" da utilizzare resta ovviamente salva la professionale valutazione di fattori quali la necessità e l'urgenza che potrebbero giustificare l'impiego di qualsivoglia mezzo/sistema di comunicazione.

#### **4. TIPOLOGIA DELLA COMUNICAZIONE**

Anche a seguito delle valutazioni accennate nel precedente paragrafo 3, il responsabile dell'impianto dovrebbe individuare se lo scambio possa/debba avvenire:

- verbalmente o in forma scritta;
- direttamente in maniera interpersonale ovvero in forma telematica.

Qualunque sia la forma ed il sistema individuato per l'interscambio, le parti dovrebbero essere consapevoli del fatto che la "qualità" dell'informazione è funzione dei seguenti parametri: rilevanza, accuratezza, tempestività, comprensibilità ed utilizzabilità.

**PIANO DI SECURITY LEGGERA  
IMPIANTI PORTUALI**

numeri utili per richiesta informazioni e reportazione situazioni per  
*l'Impianto portuale di .....*

<b>Organizzazione</b>	<b>Nome</b>	<b>Telefono Ufficio</b>	<b>Cellulare</b>	<b>Altri tipi di contatto</b>
<i>Responsabili per la security delle varie società, se esistenti, delle navi scalanti l'impianto portuale o incaricati a terra delle società:</i> a) <input type="checkbox"/> ..... b) <input type="checkbox"/> ..... ecc.				
<i>Numeri telefonici delle navi che scalano abitualmente l'impianto portuale:</i> a) <input type="checkbox"/> ..... b) <input type="checkbox"/> ..... ecc.		N.A.		
<i>Punto di contatto per il personale di vigilanza dell'impianto portuale, se esistente.</i>				
<b>I.M.R.C.C.</b> Roma	Centrale Operativa			
<b>Capitaneria di Porto:</b> a) <input type="checkbox"/> Autorità designata b) <input type="checkbox"/> Autorità marittima	Sala Operativa			
<b>Autorità Portuale:</b>	Referente Security			
<b>Polizia di Stato:</b> a) <input type="checkbox"/> Uff. Polizia Front. b) <input type="checkbox"/> Commissariato c) <input type="checkbox"/> Questura	Centralino			
<b>Guardia di Finanza</b>	Centralino			
<b>Vigili del Fuoco</b>	Personale di guardia			
<b>Dogana</b>	Centralino			
<b>Servizi Tecnico Nautici:</b> a) <input type="checkbox"/> Piloti b) <input type="checkbox"/> Ormeggiatori c) <input type="checkbox"/> Rimorchiatori d) <input type="checkbox"/> Barcaioi				

**CAPITOLO VII****PROTEZIONE DEL PIANO DI SICUREZZA/ AUDIT INTERNI/RIESAME/ EMENDAMENTI AL PIANO DI SICUREZZA****1 . PROTEZIONE DEL PIANO DI SICUREZZA**

Il piano di sicurezza incluse le relative revisioni, una volta approvato dal Capo del Compartimento Marittimo competente, è restituito in due esemplari all'impresa che provvede a consegnarli, rispettivamente, al Responsabile ed all'eventuale sostituto Responsabile di security dell'impianto.

Il Piano è protetto da parte degli interessati e reso non accessibile alle persone non coinvolte nelle attività indicate nel piano stesso. E' esplicitamente vietato fare qualunque fotocopia del piano completo e dei relativi allegati senza il preventivo consenso dell'Autorità marittima che ha proceduto all'approvazione.

**2. AUDIT INTERNI**

Il responsabile dell'impianto dovrebbe essere consapevole dell'importanza di effettuare periodici controlli sull'efficacia delle procedure di security individuate.

Questa consapevolezza dovrebbe essere incentivata anche dalla legittima aspettativa che gli sforzi organizzativi si traducano in un valore aggiunto per l'industria marittima nazionale.

In tale ottica dovrebbero essere sviluppate politiche aziendali che motivino ed incentivino:

- Il personale ad applicare le pratiche individuate ed a interagire in modo propositivo per segnalare le difficoltà incontrate per ottimizzare le trasformazioni organizzative;
- gli organi societari a procedere alla redazione di adeguate procedure e di un programma di autovalutazioni interne.

Al fine di procedere all'individuazione di un sistema di autovalutazione coerente con gli obiettivi di questo documento, le autovalutazioni interne dovrebbero:

- essere opportunamente tarate tenendo conto della specifiche attività svolte dall'impianto;
- avere riguardo del proprio assetto organizzativo, valutandone i punti di forza e di debolezza nell'interazione con il bordo;
- essere condotti, per quanto possibile, da personale diverso da quello normalmente impiegato nel settore visitato;
- essere programmati in maniera tale da consentire anche un "controllo sul campo" dell'efficacia delle attività condotte;
- essere effettuati ad intervalli non superiori a 12 mesi. Sarebbe opportuno procedere ad audit interni addizionali qualora insorgessero evidenti fattori di criticità.

Gli esiti degli audit interni sulla rispondenza delle procedure sviluppate e sull'efficacia delle attività svolte, dovrebbero essere attentamente valutati al fine di:

- rilevare se il sistema di gestione per la security previsto dal piano è efficacemente messo in atto e mantenuto;
- riportare al Capo del Compartimento marittimo competente le eventuali anomalie riscontrate individuando le eventuali misure correttive e proporre le eventuali modifiche.

Le evidenze dei processi di audit interni in quanto informazioni sensibili dovranno essere protette da accessi non autorizzati e resi disponibili durante le eventuali verifiche effettuate da parte dell'Autorità marittima.

### **3. RIESAME**

Il piano deve indicare che si procederà ad un riesame dello stesso se ci sono state modifiche nell'impianto (esempio di tipo strutturali, infrastrutturali, operative, procedurali, ecc).

Tale riesame può essere limitato a quelle sezioni influenzate dalle modifiche allo stesso. Al termine del riesame si procederà a proporre al Capo del Compartimento Marittimo le eventuali modifiche al piano di sicurezza vigente.

## **INDICAZIONI FORMALI**

Il Piano di Security leggera (SELE) redatto tenendo conto delle Linee Guida sopra riportate sarà contenuto in un documento anche in forma cartacea ed avrà il frontespizio di cui all'allegato 7 e una pagina "REGISTRAZIONE VARIANTI" come da fac-simile allegato 8.

**COMITATO INTERMINISTERIALE PER LA SICUREZZA DEI TRASPORTI  
MARITTIMI E DEI PORTI**

- - - - -

**AUTORITA' COMPETENTE PER LA SICUREZZA MARITTIMA**

**ORGANIZZAZIONE DI SECURITY LEGGERA (SELE ) PER GLI IMPIANTI PORTUALI  
PIANO DI SICUREZZA  
DELL' IMPRESA .....**

Applicazione dell'articolo 3.3 del Regolamento (CE) n. 725/2004

**Porto di.....**

Impianto / impianti cui si riferisce la valutazione di security (denominazione)

.....

Data preparazione : .....

Copia controllata n° . . . . . di . . . . . copie

**ESTREMI DI APPROVAZIONE**

Data di approvazione: .....

