

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

AUTORITA' COMPETENTE PER LA SICUREZZA MARITTIMA

**ORGANIZZAZIONE DI SECURITY LEGGERA (SELE) PER LE NAVI
PIANO DI SICUREZZA**

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

Tipo e nome :

Matricola e compartimento :

Nominativo internazionale :

Stazza :

Società (Company) :

Preparato da : (Responsabile per la security della Società)

Data preparazione:

Copia controllata n° di copie

ESTREMI APPROVAZIONE

..... (Compartimento marittimo)

..... (Capo Compartimento)

Data approvazione:

INDICE

Registrazione varianti		pag. 3
Introduzione		Pag. 4
Capitolo I	Politica ed organizzazione della Società per la security	pag. 8
Capitolo II	Dati rilevanti per la security	pag. 14
Capitolo III	Valutazione di security della nave	pag. 16
Capitolo IV	Controllo accessi nave, aree ad accesso limitato, identità passeggeri e visitatori Imbarco del carico e delle provviste	pag. 24
Capitolo V	Audit interni e revisione del piano di security nave	pag. 32
Capitolo VI	Procedure per i principali incidenti di security	pag. 35
Capitolo VII	Richiesta informazioni e rapportazione di situazioni	pag. 50
Allegato 1	Informazioni da raccogliere in caso di comunicazione di bomba a bordo	pag. 52
Allegato 2	Check list – Minaccia bomba con nave in porto	pag. 53
Allegato 3	Check-list – Minaccia bomba con nave in navigazione o alla fonda	pag. 54
Allegato 4	Questionario rilievo caratteristiche del possibile IED	pag. 55
Allegato 5	Numeri utili per richiesta informazioni e rapportazione situazioni per la nave durante la navigazione o l'interfaccia con l'impianto portuale	pag. 56
Appendice I	Quadri sinottici dell'applicazione dell'art. 3.3 del Reg. (CE) 725/2004	pag. 57-61

INTRODUZIONE

Scopo delle presenti linee guida è quello di fornire uno strumento per l'elaborazione del piano di sicurezza nave nell'ambito dell'organizzazione di "security leggera" (SELE). Quanto sopra per 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).

La redazione del piano è obbligatoria per le pertinenti navi così come individuate nelle precitate schede. I contenuti del piano dovranno, per quanto possibile e ragionevole, conformarsi alle indicazioni delle presenti linee guida che non si riferiscono alle navi ed alle Società (company) già oggetto di specifica disciplina in base ai comma 1 e 2 dell'articolo 3 del precitato Regolamento (CE) n.725/2004.

Entro il 01.12.2008, le società dovranno presentare i piani di sicurezza delle navi gestite che, approvati dall'Amministrazione entro i successivi 30 giorni, saranno sottoposti ad un periodo di sperimentazione obbligatoria che avrà termine il 30.09.2009.

In tale periodo di sperimentazione, svolto sotto il monitoraggio dell'Autorità marittima, verrà valutata la coerenza delle misure di sicurezza contenute nel piano con gli obiettivi perseguiti in relazione alla specifica nave, riferendone gli esiti entro il 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 dovessero evidenziare fattori di criticità.

La Società, nell'impartire istruzioni e nel redigere procedure, deve considerare la potestà del comando di bordo di dirimere, in base al professionale giudizio, eventuali contingenti e non preventivabili conflitti tra le esigenze di safety e di security.

Le presenti istruzioni si rivolgono ad un'ampia gamma di realtà. Ciò premesso, nell'applicare quanto riportato nel presente documento, la Società ed il comando di bordo dovrebbero prestare la massima attenzione nell'individuare per la propria nave una forma proporzionata ma coerente di security. Ogni sforzo deve, altresì, essere fatto dall'Autorità designata per supportare la precitata attività mettendo a disposizione dell'utenza il proprio "know-how" in materia di "maritime security".

Nell'attuazione delle presenti linee guida non ci si dovrebbe discostare dal principio generale di perseguire l'efficienza, l'economicità ed adeguatezza del trasporto marittimo.

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**», un luogo in cui avviene l'interfaccia nave/porto;
- 14) «**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;
- 15) «**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;
- 16) «**Nave passeggeri**» significa una nave che trasporta più di dodici passeggeri.
- 17) «**HSC**» significa una nave come definita dalla SOLAS Reg. X/1.3.
- 18) «**DSC**» significa una nave come definita dal DSC code Res A.373(X) cap. 1.4.1.
- 19) «**Aliscafo**» significa una nave come definita dal D.P.R. 8 novembre 1991, n.435 Art.1.2.
- 20) «**Nave da carico**» significa qualsiasi nave che non sia una nave da passeggeri.
- 21) «**Nave cisterna**» significa una nave da carico costruita o adattata per il trasporto alla rinfusa di carichi liquidi di natura infiammabile.
- 22) «**Nave chimichiera**» significa una nave chimichiera come definita alla Regola VII/8.2.
- 23) «**Nave gasiera**» significa una nave gasiera come definita alla Regola VII/11.2.
- 24) «**Nave petroliera**» significa una nave petroliera come definita alla Regola II-1/2.12.
- 25) «**Società**» significa una società come definita alla Regola IX/1.

- 26) “**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.
- 27) “**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.
- 28) “**Livello di sicurezza**” significa la qualificazione del grado di rischio che un incidente di sicurezza possa essere tentato o possa verificarsi.
- 29) “**Livello di sicurezza 1**” è il livello per cui vanno costantemente mantenute misure di sicurezza minime adeguate.
- 30) “**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.
- 31) “**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

POLITICA ED ORGANIZZAZIONE DELLA SOCIETA' PER LA SECURITY

1.1 Politica

La presente politica si riferisce alle navi gestite dalla
..... da qui in avanti denominata "Società".

La Società, ben consapevole delle proprie responsabilità in questo campo, pone il massimo impegno verso la sicurezza (safety), la protezione dell'ambiente e la security delle navi gestite. Coerentemente, si impegna a:

- mettere in risalto il ruolo del Comandante della nave che è investito della massima autorità e responsabilità di decidere per quanto riguarda la sicurezza a bordo e di richiedere l'assistenza della Società e delle Autorità competenti nazionali nella misura del necessario;
- riconoscere che, in caso di conflitto tra ragioni economiche o commerciali e gli aspetti di cui sopra, il Comandante decida dando la priorità a quest'ultimi;
- fornire al Responsabile per la security della Società, al Comandante della nave ed al Responsabile per la security della nave il sostegno necessario per perseguire gli obiettivi e far fronte alle responsabilità derivanti dalla normativa nazionale;
- dare riscontro alle segnalazioni di eventi che possano compromettere la sicurezza delle persone, della nave o che possano determinare un inquinamento marino ed, a tale scopo, a provvedere con adeguate risorse umane e mezzi materiali;
- esaminare periodicamente l'applicazione della politica societaria in modo da assicurare che gli obiettivi prefissati siano raggiunti e che le procedure e le istruzioni siano adeguate ed efficaci.

La Società, con la presente dichiarazione, stabilisce che il proprio personale, sia a terra sia a bordo le navi, deve mettere il dovuto impegno affinché siano raggiunti gli obiettivi in materia di Security elencati di seguito:

- proteggere le navi, gli eventuali passeggeri, gli equipaggi e, comunque, le altre persone presenti a bordo, nonché l'eventuale carico dalle minacce di azioni illecite intenzionali;
- operare le navi e trattare il carico e le provviste in maniera sicura;
- promuovere la conoscenza della Security tra tutto il proprio personale;
- mantenere al massimo livello l'efficienza tecnica ed operativa delle navi.

Per raggiungere i sopra menzionati obiettivi, la Società si impegna a fornire le necessarie risorse materiali nonché personale qualificato, definendo la propria organizzazione, identificando

specifici compiti e responsabilità, stabilendo requisiti di addestramento e coordinando tutte le attività in modo da:

- garantire la sicura operatività delle navi in conformità alle norme ed ai regolamenti di legge nazionali ed internazionali applicabili;
- stabilire misure contro tutti i rischi identificati, provvedendo a mitigare quelli con livelli troppo alti;
- migliorare continuamente la preparazione tecnica e l'efficienza operativa del personale di bordo e di terra.

1.2 Organizzazione

La Società provvede a designare uno o più Responsabile/i per la security della Società ed eventualmente i relativi sostituti. Tale individuazione dovrà essere riportata nel successivo Capitolo II . L'individuazione del Responsabile della security di bordo e dell'eventuale sostituto avverrà mediante atto sottoscritto dal legale rappresentante della Società. Tale atto è custodito in annesso al presente documento.

1.2.1 Lingua di lavoro

La lingua di lavoro negli uffici della Società è l'italiano ma il Responsabile per la security della Società deve avere una buona conoscenza della lingua inglese. Nel caso la lingua di lavoro nella Società sia diversa dall'italiano, il responsabile per la security della società deve avere una buona conoscenza della lingua italiana.

La documentazione relativa al presente Piano (registrazioni, procedure, lettere circolari, rapporti, comunicazioni ecc.) per gli uffici sarà in italiano ed eventualmente in.....(specificare lingua/e).

A bordo della nave la lingua comune di lavoro è quella eventualmente registrata dal Comandante nel Giornale Nautico parte II. In assenza di tale determinazione la lingua di lavoro è l'italiano. Nel caso la lingua di lavoro di bordo sia diversa dall'italiano, il piano di sicurezza della nave deve avere una traduzione in tale lingua. La Società cura che i Responsabili della security di bordo delle proprie navi abbiano una sufficiente conoscenza della lingua italiana ed inglese.

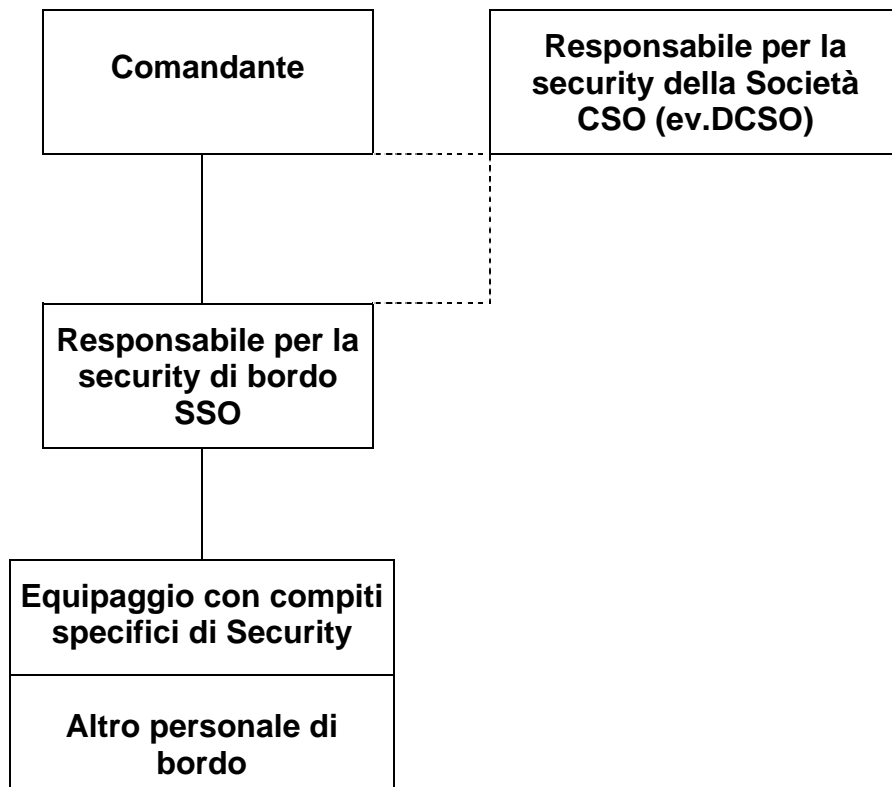
1.2.2 Struttura organizzativa per la Security

L'organizzazione per la security a bordo della nave è quella indicata nell'organigramma di cui al sotto riportato schema (A).

Il legale rappresentante della Società designa il/i Responsabile/i per la security della Società ed eventualmente i rispettivi sostituti per mezzo di una comunicazione scritta e provvede a far fronte alle risorse ed al supporto necessari per mettere il Responsabile per la security della Società in grado di espletare le proprie funzioni.

Schema A

(NOME NAVE)..... STRUTTURA ORGANIZZATIVA PER LA SECURITY



Approvato

.....

(Il legale rappresentante della Società)

1.2.3 Responsabile per la security della Società

I principali doveri e compiti del Responsabile per la security della Società , d'ora innanzi indicato anche con l'acronimo CSO, e, ricorrendone le circostanze, del suo eventuale sostituto sono:

- acquisire informazioni sul livello delle probabili minacce per la nave, sulle base delle valutazioni di security ed altre informazioni pertinenti;
- provvedere affinché sia effettuata la valutazione di security della nave;
- occuparsi dell'elaborazione, della presentazione per l'approvazione ed in seguito dell'attuazione e rispetto del piano di security della nave;
- provvedere affinché il piano di security della nave venga costantemente aggiornato nella misura necessaria per assicurarne l'efficacia;
- organizzare audit interni e riesami delle attività di security;
- provvedere affinché le anomalie e le non conformità individuate durante gli audit interni, i riesami periodici, le ispezioni di security e le verifiche della conformità siano tempestivamente corrette;
- assicurare un addestramento adeguato per il personale della nave con specifici compiti di security;
- potenziare la sensibilizzazione del personale in materia di security;
- assicurare comunicazioni e cooperazione efficaci tra il Responsabile per la security di bordo ed i competenti Port Facility Security Officers / responsabili per la security degli impianti portuali;
- provvedere affinché, se si ricorre a piani di security per tipo di nave o per la flotta, il piano per ciascuna nave rifletta accuratamente le informazioni specifiche per ciascuna nave;
- assicurare l'effettivo coordinamento ed attuazione del piano di security partecipando alle esercitazioni previste.

1.2.4 Comandante

L' autorità e le connesse responsabilità di security del Comandante sono quelle indicate nella SOLAS capitolo XI-2 Regola 8 e, più nel dettaglio:

- il Comandante non deve essere obbligato dalla società, dal noleggiatore o da terzi, ad astenersi dal prendere od eseguire decisioni che, secondo il suo giudizio professionale, siano necessarie per salvaguardare l'efficiente funzionamento della nave o la sua sicurezza. Rientrano tra tali decisioni il rifiuto di accesso a persone (ad eccezione di quelle identificate come debitamente autorizzate da un Governo Contraente) o dei loro effetti e il rifiuto di caricare a bordo merci, ivi compresi container ed altre unità di trasporto chiuse;

- se, a giudizio del Comandante, durante le operazioni della nave si verifica un conflitto grave ed insanabile tra prescrizioni relative alla sicurezza (safety) e prescrizioni relative alla sua protezione (security), egli privilegia le prime. In tali casi, il Comandante può dar corso a misure temporanee di protezione e ne informa immediatamente l'Autorità designata del porto in cui la nave sta effettuando le proprie operazioni o intende entrare. Tutte le misure temporanee di protezione adottate devono, per quanto possibile, essere commisurate al livello di security in atto.

1.2.5 Responsabile per la security di bordo

I principali doveri e compiti del Responsabile per la security di bordo, d'ora innanzi indicato anche con l'acronimo SSO, sono:

- svolgere regolari ispezioni di security della nave per verificare l'osservanza costante delle misure di security necessarie;
- garantire l'osservanza e la supervisione dell'attuazione del piano di security della nave, comprese eventuali modifiche dello stesso;
- coordinare gli aspetti di security della movimentazione dei passeggeri, del carico e delle provviste di bordo con il restante personale della nave e con i Responsabili per la security degli impianti portuali;
- proporre le modifiche al piano di security della nave;
- comunicare al CSO le eventuali anomalie e non conformità individuate durante gli audit interni, i riesami periodici, le ispezioni di security e le verifiche della conformità ed attuare eventuali azioni correttive;
- curare la sensibilizzazione del personale di bordo in materia di security;
- accertarsi che il personale di bordo con specifici compiti di security abbia ricevuto un adeguato addestramento in materia di security;
- comunicare gli incidenti di security;
- coordinare l'attuazione del piano di security della nave con il CSO e con il responsabile per la security dell'impianto portuale;
- assicurare il corretto impiego, prova, calibratura e manutenzione delle attrezzature di security eventualmente presenti.

1.2.6 Compiti del personale di bordo

I compiti e le responsabilità di Security del personale di bordo possono essere diversificati a seconda del livello di security applicabile. Per il personale di bordo con specifici compiti di

security si dovrà riportare il relativo mansionario mediante una sintetica lista. Di seguito, a titolo d'esempio, se ne riporta uno stralcio:

Lista del personale con compiti specifici di security

Ruolo	Livello 1	Livello 2	Livello 3
1° Ufficiale	Nessuno	A disposizione a bordo	Gestisce comunicazioni d'emergenza in plancia. A comando aziona SSAS
Nostromo	Nessuno	A disposizione a bordo	Dirige team di guardia e di ricerca IED
Marinaio A	Nessuno	Nessuno	Capo team sorveglianza degli accessi nave dal lato mare

(Quanto sopra è solo a titolo di esempio come metodo da applicare)

CAPITOLO II

DATI RILEVANTI PER LA SECURITY

2.1 Dati della nave

Tipo di nave:

Matricola e porto d'iscrizione:

Nominativo internazionale:

Numero IMO:

Numero MMSI:

Numero equipaggio (Min. e Max.):

Velocità di crociera:

Autonomia alla VdC:

Velocità alla massima potenza continuativa e a pieno carico:

Autonomia alla VMPC:

Lunghezza ft:

Larghezza fo:

Stazza lorda:

Eventuale numero passeggeri (Max.):

Eventuale tipologia carico:

Eventuali apparati (SSAS, AIS e LRIT):

(altro)

2.2 Dati della Società

Nome della Società:

Indirizzo:

Telefono fisso:

Fax:

Email:

2.3 Dati dell'Armatore (se diverso dalla Società):

2.4 Responsabile per la security della Società

Nome:

Telefono fisso:

Cellulare:

Fax:

Email:

2.5 Sostituto del Responsabile per la security della società (eventuale):

Nome:

Telefono fisso:

Cellulare:

Fax:

Email:

2.6 Piani nave

Al piano di security deve essere annesso, come minimo, un piano generale della nave ove siano chiaramente indicati:

- l'identificazione degli accessi (es.: portelloni, rampe, scalandroni, portelli di murata ecc.);
- le aree ad accesso limitato (es.: plancia, locale macchina, locali organi di governo e altri locali considerati vitali).

Qualora per dimensioni e tipologia costruttiva un singolo piano risulti scarsamente intelligibile si dovrà far ricorso a piani diversificati.

2.7 Servizi

La nave adibita al trasporto di....., effettua viaggi (regolari/spot etc.) nelle aree geografiche di..... e viene utilizzata dai noleggiatori:

Il Responsabile per la security della Società ed il Responsabile per la security di bordo provvedono a mantenere aggiornati i dettagli di quanto sopra indicato.

CAPITOLO III

VALUTAZIONE DI SECURITY DELLA NAVE

3.1 Generalità

Scopo di questo capitolo è quello di delineare una serie di attività di carattere generale che, in concorso tra di loro, possano incrementare il livello complessivo di sicurezza (security) della nave.

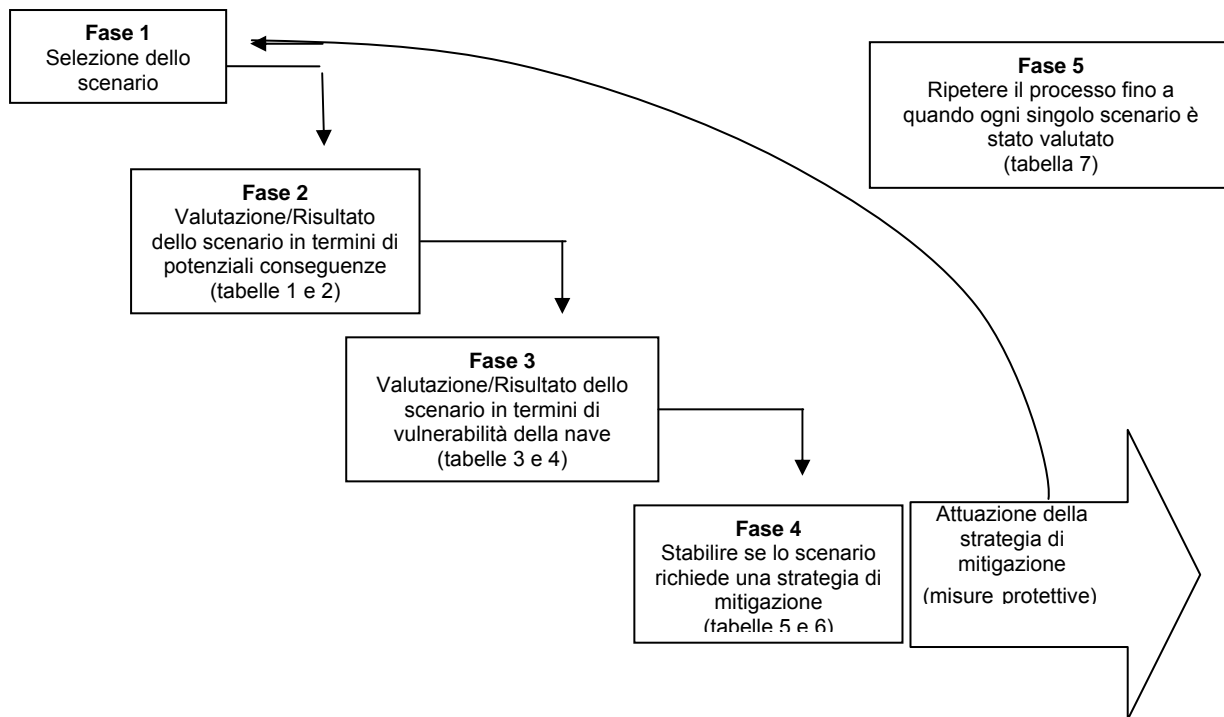
La Società ed il comando di bordo dovrebbero considerare che l'esecuzione di una singola misura di security, per quanto condotta con incisività, normalmente non garantisce un adeguato e complessivo livello di sicurezza. Più probabilmente, un complessivo incremento del grado di sicurezza della nave sarà funzione dell'attuazione del "giusto mix" di più misure/attività. E', pertanto, da attuare una politica tesa ad un omogeneo innalzamento del livello di protezione, evitando sacche di vulnerabilità.

Nell'individuare l'assetto organizzativo più confacente alle esigenze di security, il responsabile per la security della nave deve considerare:

- la tipologia del servizio svolto, dei viaggi effettuati e delle infrastrutture portuali toccate;
- le vulnerabilità, sia strutturali che di organizzazione, rispetto agli incidenti di security rilevanti, così come individuati nel capitolo VI;
- le necessarie strategie di mitigazione del rischio.

La valutazione della security è un processo che identifica le criticità nell'infrastruttura (physical security), nell'adeguatezza, quantitativa e qualitativa del personale (organic security), nei processi o in altre aree che possano condurre ad una carenza di sicurezza. Da dette valutazioni possono altresì scaturire le indicazioni per eliminare o mitigare tali criticità. Ad esempio, una valutazione della security potrebbe rivelare criticità nei sistemi di sicurezza di un'organizzazione, quali il sistematico mancato sollevamento della scala pilota o la mancata chiusura di sicurezza o il controllo dei portelloni laterali dopo il carico. Per diminuire tale rischio, la nave dovrebbe applicare delle procedure per garantire che tali punti di accesso siano bloccati e controllati attraverso vari mezzi. Un ulteriore miglioramento della security potrebbe essere quella di usare meccanismi di chiusura e/o reti di metallo a porte e finestre che immettono ad aree ad accesso limitato per prevenire l'ingresso di personale non autorizzato. Un esempio di procedura di valutazione dei rischi è descritto nella Tabella 6 che costituisce anche un sistema per documentare i processi ed i relativi risultati. Il processo logico-sistematico da impiegare nella

valutazione di sicurezza della nave deve essere coerente con quello individuato nel seguente schema:



3.2 Fase 1 - Potenziali minacce

Per iniziare una valutazione, la Società 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 che le risorse a disposizione (capacità ed intenti) siano indirizzate coerentemente con quanto emerso dalla valutazione della minaccia.

I possibili scenari da considerare devono almeno comprendere:

- l'ingresso di persone non autorizzate;
- l'introduzione di armi, esplosivi ed altre sostanze pericolose non autorizzate;
- l'impossessamento e dirottamento della nave;
- la presa di ostaggi.

3.3 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. Segue una descrizione dei componenti delle conseguenze:

Tab.1 Elementi di valutazione

Danni alle persone	Il numero ipotizzabile (valutazione oggettiva) di vite che si potrebbero perdere e dei feriti che potrebbero registrarsi in conseguenza di uno scenario d'attacco
Impatto economico	Il potenziale impatto (valutazione oggettiva) economico di uno scenario di attacco.
Impatto ambientale	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
3	CATASTROFICO = numerose perdite di vite o feriti; importante impatto su scala nazionale o impatto economico a lungo termine; distruzione completa di aspetti multipli dell'ecosistema in una grande area
2	SIGNIFICATIVO = significativa presenza di morti o feriti; importante impatto economico regionale; danno a lungo termine ad una parte dell'ecosistema
1	MODERATO = nessuna o bassa presenza di morti o feriti; impatto economico basso; lieve danno ambientale

3.4 Fase 3 - Valutazione della vulnerabilità

Ciascuno scenario deve essere valutato in termini di vulnerabilità della nave ad uno specifico attacco. Gli elementi del grado di vulnerabilità sono quattro: disponibilità, accessibilità,

organizzazione della security e robustezza della nave. Assumendo che il Responsabile per la security della Società 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

<p>Accessibilità</p>	<p>Accessibilità della nave nello scenario di attacco. Essa riguarda le barriere fisiche e geografiche che possano scoraggiare la minaccia senza considerare l'organizzazione della security.</p>
<p>Organizzazione della security</p>	<p>L'abilità del personale di bordo di scoraggiare l'attacco. Essa include piani di security, capacità di effettuare comunicazioni, personale di guardia, sistemi di rilevazione delle intrusioni e la tempestività del rafforzamento delle regole esterne per prevenire l'attacco</p>

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 della Tabella 6).

Tab. 4 Gradazione della vulnerabilità

Accessibilità	Organizzazione della security	Valutazione
Nessuna deterrenza (es. accesso alla nave e movimento interno senza restrizioni, basso bordo libero)	Nessuna capacità di deterrenza (es. assenza di un piano, assenza di posti di guardia, indisponibilità di mezzi di comunicazioni d'emergenza, modesta organizzazione interna della Società)	3
Buona deterrenza (es. efficaci sistemi di barriere; accesso limitato da circa 50 m dalla nave, assenza di settori ciechi)	Buona capacità di deterrenza (es. istruzioni/procedure basiche di security, qualche mezzo di comunicazione, corpo di guardie di ridotta composizione in relazione alla nave)	2
Eccellente deterrenza (es. accesso limitato da circa 100m dalla nave; barriere fisiche multiple, alto bordo libero)	Perfetta capacità di scoraggiare gli attacchi, elementi di security nascosti ed occultati , che rappresentano elementi addizionali non visibili o evidenti.	1

3.5 Fase 4 - Mitigazione

Il Responsabile per la security della Società, ovvero colui il quale procede alla valutazione, deve stabilire quali scenari possano richiedere l'applicazione di strategie di mitigazione (misure protettive).

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

“**Mitigare**” indica che devono essere sviluppate strategie di mitigazione, quali misure di sicurezza e/o procedure, per ridurre i rischi in un determinato scenario. La Società deve essere in grado di documentare, a chi di competenza, 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. La Società deve essere in grado di documentare, a chi di competenza, 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, il Responsabile per la security della Società 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	

3.6 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), il Responsabile per la security della Società 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 (rimane lo stesso)	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:

1. si devono elaborare le strategie di mitigazione (misure protettive) e registrarle nella prima colonna della Tabella 7;
2. 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”).

Il Responsabile per la security della Società deve considerare che alcune strategie potrebbero rivelarsi proporzionate ai vari “livelli di minaccia alla security” stabiliti. La fattibilità di una strategia di mitigazione può variare in base al *“livello di Security”*, quindi alcune strategie potrebbero non essere garantite al *“livello di Security 1”* ma potrebbero esserlo invece ai *“livelli 2 o 3”*. Ad esempio, al *“livello di Security 1”*, potrebbe non essere necessario l’impiego di sommozzatori per ispezionare la parte immersa della struttura della banchina o della nave. Cosa che potrebbe invece essere prevista in caso di minacce specifiche e/o di aumento del *“livello di Security”*. Le strategie di mitigazione dovrebbero infine garantire il mantenimento di un livello di security per raggiungere gli obiettivi prefissati.

Il Responsabile per la security della Società deve realizzare un processo attraverso il quale si valuti continuamente la sicurezza totale, considerando le conseguenze, le vulnerabilità e le loro variazioni nel tempo il tempo e quali altre strategie di mitigazione possano essere applicate.

CAPITOLO IV

CONTROLLO ACCESSI NAVE, AREE AD ACCESSO LIMITATO, IDENTITA' PASSEGGERI E VISITATORI. IMBARCO DEL CARICO E DELLE PROVVISI

4.1 Generalità

Tutti gli accessi alla nave devono essere protetti e controllati al fine di garantire la security.

Di seguito vengono elencati tutti i punti di accesso (indicati nei piani di cui al Capitolo I) e relativi controlli da effettuare. Con livelli di security superiori al SL1 i punti di accesso dovranno essere ridotti al minimo indispensabile; tali punti di accesso, quando non utilizzati su decisione del Comandante e dello SSO, devono essere chiusi e non più utilizzati se non previa formale autorizzazione.

4.2 Punti di accesso - Individuazione

I punti di accesso alla nave sono i seguenti: (Se ne riportano alcuni a titolo esemplificativo)

- Scalandroni
- Passerelle (sono da considerarsi anche quelle per operazioni nave/nave)
- Biscagline
- Portelloni laterali per imbarco provviste e bunkeraggio nr..
- Rampe
- Altri (eventuale).....

Per tutti i punti di cui sopra dovranno essere indicate le procedure per il controllo, la limitazione dell'accesso ed i divieti di accesso per ognuno dei livelli di sicurezza previsti.

4.3 Controllo accessi

L'estensione dei controlli ed azioni da effettuarsi sono in funzione del Livello di Security da adottare e comprendono le seguenti attività:

- stabilire i punti di accesso, da utilizzare durante l'interfaccia con l'impianto portuale o altra nave, tra quelli descritti nel presente piano;
- assegnare personale di guardia dotandolo di apposito apparecchio di radio comunicazione con l'altro personale di guardia;
- assicurare che i punti di accesso alla nave, diversi da quelli stabiliti per l'utilizzo, siano correttamente chiusi ;

- controllare l'identità di qualsiasi persona prima di permettergli l'accesso a bordo;
- verificare che persone estranee non possano accedere previa effettuazione di quanto previsto per l'ingresso a bordo in relazione al livello di security applicabile;
- individuare con l'impianto portuale le aree stabilite per il controllo del carico e delle provviste prima dell'ingresso alla nave;
- controllare il carico e le provviste di bordo prima del loro imbarco;
- istituire un sistema di registrazione e di "pass" da utilizzare in base ai livelli di security applicabili;
- stabilire ronde per il controllo degli accessi non utilizzati e per le aree ad accesso limitato;
- assicurare che le biscagline non siano disponibili all'utilizzo quando non in uso;
- attivare eventuale illuminazione prevista per la Security;
- vigilare su tutte le dotazioni, pertinenze e strutture che possono agevolare l'ingresso non autorizzato a bordo (es.: cavi d'ormeggio e catene ancore, gru e picchi, oblò/finestroni, nastri trasportatori e/o manichette del carico).

4.4 Controllo persone all'imbarco incluso bagagli e bagaglio non accompagnato

Nel caso di rifiuto di sottoporsi ai controlli previsti dal presente piano di sicurezza non si dovrà permetterne l'entrata di persone o cose e si dovrà informare prontamente lo SSO.

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare e comprendono:

4.4.1 Passeggeri e relativi bagagli

- controllo biglietto d'imbarco e relativo documento identità dei passeggeri imbarcanti;
- utilizzo di Metal Detector fisso o portatile;
- controllo, possibilmente mediante X-Ray scanner, dei bagagli ed identificazione degli stessi;
- eventuale distribuzione di brochure sulla Politica di Security della nave;
- registrazione ed impiego "pass" a livelli di sicurezza SL2 e SL3.

4.4.2 Bagagli non accompagnati

- accertamenti sulla presenza a bordo del proprietario;
- controllo, possibilmente mediante X-Ray scanner, dei bagagli e relativa identificazione (connessione con il proprietario) degli stessi;
- limitazione o sospensione della movimentazione dei bagagli non accompagnati ai livelli di security SL2 e SL3.

4.4.3 Veicoli

- controllo dei veicoli da caricare a bordo.
- I controlli consisteranno nella verifica, al momento dell'accesso degli stessi alla nave, 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.

4.4.4 Visitatori

- controllo identità e rispondenza con elenco persone di previsto arrivo;
- utilizzo di 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 di bordo (es.: identificazione e relativo divieto per aree ad accesso limitato)
- limitazione o sospensione dell'ingresso ai livelli di sicurezza SL2 e SL3 ed accompagnamento dei visitatori.

4.4.5 Autorità

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

4.4.6 Personale addetto al carico

- chiarire con l'impianto portuale il sistema di identificazione del personale (il riconoscimento potrà essere fatto a cura dell'impianto portuale);
- informare il personale di bordo addetto ai controlli di security sul sistema di individuazione;
- informare il personale di terra sulle limitazioni previste per le Aree ad Accesso Limitato.

4.5 Aree ad accesso limitato - generalità

Le Aree ad Accesso Limitato, come definite nei seguenti paragrafi, sono stabilite per controllare le zone ritenute “chiave” per le operazioni, controllo e sicurezza della nave. Dette aree devono essere accessibili solo al personale di bordo o alle persone debitamente autorizzate.

I punti di ingresso alle aree ad accesso limitato devono essere chiusi e serrati a meno che il Comandante decida che, per contingenti ragioni operative, questi non possano essere chiusi.

Le aree ad accesso limitato vengono controllate durante le ronde eventualmente istituite in relazione ai Livelli di Security.

Le aree ad accesso limitato sono tutte identificate opportunamente con il seguente cartello:

AREA AD ACCESSO LIMITATO – VIETATO L’INGRESSO

CONSENTITO L’INGRESSO AL SOLO PERSONALE AUTORIZZATO

4.5.1 Aree ad Accesso Limitato - individuazione

Le aree ad accesso limitato in linea teorica sono quelle definite dall’ISPS Code Parte A Sez. 9.4.2 tenendo conto della guida fornita nella Parte B para. 9.18-9.21. Alcune di queste potrebbero essere classificate tali solo a livelli di security elevato (SL2 o SL3).

In base alle risultanze della valutazione di sicurezza per la nave sono individuate le aree ad accesso limitato: (si riporta una lista a titolo esemplificativo)

- ponte di comando;
- stazione radio (se non nel Ponte di comando);
- sala macchine;
- sala controllo macchine (se non inclusa nel locale macchine)
- vie di sfuggita dalla Sala macchine
- locale timoneria
- locali elica prodiera
- locale impianti antincendio e VVF
- locale diesel emergenza
- locali garage (quando in navigazione)
- pick-up area per operazioni con elicottero (per come tecnicamente fattibile)
- locali controllo carico
- locali pompe del carico
- locali per l’imbarco ed accesso ai serbatoi acqua potabile, fuel, olio, pompe e collettori

- locali equipaggio

Altre aree ad accesso limitato possono essere definite con l'autorità designata nel caso di un aumento del livello di security. In tal caso dette aree devono essere gestite dallo SSO in accordo alle decisioni concordate ed informando opportunamente il personale di bordo addetto ai compiti di security. Il CSO deve essere debitamente informato al fine della valutazione della necessità di eventuali risorse aggiuntive.

4.5.2 Aree ad Accesso Limitato - Sistemi di chiusura accessi

In base al livello di Security in atto, per la chiusura degli accessi possono essere utilizzati sistemi di chiusura quali key-cards, piombatura o speciali nastri adesivi dal cui esame visivo si può dedurre facilmente che gli stessi sono stati aperti da personale non autorizzato. Questo ultimo sistema può essere utilizzato anche per le vie di sfuggita **non** dal lato di fuga. In tutti i casi si dovranno prevedere istruzioni di comportamento da parte del personale di bordo. Per le vie di sfuggita deve essere assicurato che queste possano essere aperte dal lato della fuga.

L'utilizzo delle chiavi e dei lucchetti viene gestito dal Comandante e dallo SSO che provvede a fornirle al personale di bordo in accordo ai relativi compiti come applicabile e mantiene un elenco di distribuzione. Nel caso di perdita o di sottrazione delle chiavi di cui sopra, lo SSO ne deve essere informato subito.

4.5.3 Aree ad Accesso Limitato - Monitoraggio

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security in atto e comprendono:

- stabilire personale di guardia o ronda definendo numero persone, turni e frequenza ronde e modalità;
- attivare illuminazione prevista per la security ed eventuale illuminazione di terra;
- prevedere continua sorveglianza e/o attivazione di impianti fissi di rilevazione;
- assicurare che l'accesso alle aree sia consentito solo al personale autorizzato;
- verificare l'autorizzazione delle persone presenti nelle aree.

4.6 Carico (se applicabile) – generalità

Scopo di questo paragrafo è quello di individuare una serie di attività la cui concorsuale applicazione possa incrementare il livello di sicurezza (security) durante le operazioni di imbarco del carico. La Società deve sviluppare politiche aziendali atte a contemperare le esigenze

commerciali con quella di innalzare il livello di sicurezza della nave. Il comando di bordo e l'equipaggio devono essere consapevoli di tali politiche e devono essere altresì messi in grado di poterle efficacemente applicare.

In tale ottica la Società e il comando di bordo devono sviluppare procedure, calzanti con la tipologia dell'unità e del servizio svolto, che rispondano a requisiti di efficienza ed efficacia.

Il controllo delle operazioni di caricazione della nave deve permettere di evitare manomissioni dolose del carico nonché l'imbarco di carico non previsto. Le misure di security per il carico devono essere definite nello spirito di quanto indicato dall'ISPS Code parte A sez. 7 tenendo conto della guida fornita nella parte B para. 9.25 e 9.26.

4.6.1 Carico – controlli

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security in atto e comprendono:

- fornire polizze del carico, piano caricazione ed informazioni come appropriato al personale addetto al controllo;
- stabilire con l'impianto portuale come effettuare l'identificazione del carico (es.: marcatura con adesivi dedicati o altro);
- stabilire con l'impianto portuale le aree da utilizzare per il controllo prima dell'imbarco di auto, autoarticolati, moto, contenitori ed altri carichi;
- informarsi circa eventuali sistemi di controllo per la security da parte del porto/impianto portuale con i quali prevedere di coordinarsi;
- fornire istruzioni specifiche concordate al personale di controllo nel caso di operazioni nave/nave;
- controllare gli spazi carico prima e dopo la caricazione;
- controllare la rispondenza del carico con la polizza di carico fornita;
- controllare l'integrità del carico da imbarcare a mezzo esame visivo o mediante impiego di eventuali sistemi di controllo.

4.7 Provviste - generalità

Scopo di questo paragrafo è quello di individuare una serie di attività la cui concorsuale applicazione possa incrementare il livello di sicurezza (security) durante le operazioni di imbarco delle provviste. La Società deve sviluppare politiche aziendali atte a contemperare le esigenze commerciali con quella di innalzare il livello di sicurezza della nave. Il comando di bordo e

l'equipaggio devono essere consapevoli di tali politiche e devono essere altresì messi in grado di poterle efficacemente applicare.

In tale ottica la Società e il comando di bordo devono sviluppare procedure, calzanti con la tipologia dell'unità e del servizio svolto, che rispondano a requisiti di efficienza ed efficacia.

La Società deve individuare procedure che possano consentire un'adeguata forma di controllo sull'imbarco di provviste a bordo delle navi. Tale aspetto, di rilevante entità per alcuni tipi di navi, deve essere gestito con semplici ma efficaci procedure tali da consentire di ridurre il rischio che:

- a bordo possano essere introdotte cose non richieste e/o attese;
- le forniture, ancorché apparentemente conformi alle richieste, possano invece essere state manomesse.

Per far fronte a tali esigenze è opportuno che la Società, l'armatore ed il comando di bordo intrattengano relazioni con soggetti le cui organizzazioni aziendali possano offrire una "filiera" tale da garantire che:

- i beni richiesti siano forniti, per quanto opportuno, contenuti in idonei contenitori controllati e sigillati all'origine;
- i conducenti degli automezzi impiegati nel trasporto siano persone conosciute ed aventi un recapito certo;
- gli automezzi impiegati nei trasporti, dopo il preliminare controllo che dovrebbe precedere il carico delle provviste, non rimangano incustoditi.

Qualora per oggettive difficoltà l'approvvigionamento non possa avvenire tramite fornitori del tipo sopraccitato, il comando di bordo deve assicurare che vengano svolte le seguenti attività:

- controllo della regolarità della richiesta se l'ordine non è stato originato dalla nave;
- identificazione del conducente;
- controllo della rispondenza tra la richiesta e la fornitura;
- controllo a campione dell'integrità dei contenitori.

Le precitate attività devono essere, per quanto possibile, effettuate prima di procedere all'imbarco. Dopo il controllo è necessario procedere allo stivaggio delle provviste negli spazi ad esse destinati.

4.7.1 Forniture di bordo - controlli

L'estensione dei controlli ed azioni da effettuare sono in funzione del Livello di Security da adottare e comprendono:

4.7.1.1 Bunkeraggi

- fornire al personale di controllo durante l'imbarco i dati sul fornitore, sulle modalità di conferimento e sui quantitativi da imbarcare;
- informarsi circa eventuali sistemi di controllo per la security da parte del porto/impianto portuale con i quali provvedere a coordinarsi;
- attivare impianti CCTV se presenti;
- illuminare la zona imbarco;
- identificare il personale addetto all'imbarco;
- nel caso di imbarco da bettolina informarsi su quali controlli di security applica il Comandante della stessa;
- stabilire tipo di comunicazione con il personale di terra/bettolina;
- permettere l'ingresso alla nave da parte del personale di terra/bettolina per il solo tempo necessario alle operazioni;
- verificare le quantità imbarcate.

4.7.1.2 Provviste di bordo

- fornire al personale di controllo durante l'imbarco i dati sul fornitore, sulle modalità di conferimento e sui quantitativi da imbarcare;
- informarsi circa eventuali sistemi di controllo per la security da parte del porto/impianto portuale con i quali provvedere a coordinarsi;
- nel caso di operazioni nave/nave fornire istruzioni specifiche concordate al personale di controllo;
- mantenere aggiornati gli inventari nave (per le merci e le sostanze pericolose anche la relativa ubicazione a bordo);
- controllare gli spazi dedicati alle provviste prima/dopo caricazione;
- attivare impianti CCTV se presenti;
- verificare la rispondenza delle provviste con le richieste di bordo previste;
- verificare l'integrità degli imballaggi delle forniture a mezzo esame visivo o altro idoneo sistema (es.: controllo con Metal detector, utilizzo di cani ecc.).

CAPITOLO V

AUDIT INTERNI E REVISIONE DEL PIANO DI SECURITY NAVE

5.1 Generalità

Il Piano della Security deve essere coerente con quanto indicato nell'ISPS Code Parte A Sez. 9.4, tenendo conto della guida fornita nella Parte B e deve perseguire gli scopi sotto elencati:

- contribuire alla prevenzione di atti illegali contro la nave, il suo equipaggio, i passeggeri ed il carico;
- chiarire la politica della Società per una sicura ed efficiente condotta delle navi gestite;
- chiarire come la nave e la Società rispondono ad eventi pianificati e non pianificati relativi alla security che possono accadere;
- costituire il necessario riferimento per tutte le attività relative alla security a bordo della nave;
- descrivere come venga applicata la politica della Società e rappresentare una guida di riferimento per tutto il personale coinvolto nelle attività sulla nave ed in Società. Le procedure individuate in questo piano richiedono pertanto un positivo approccio da parte di tutto il personale sia di bordo che di terra.

Il piano di sicurezza è di proprietà della nave ed il suo uso è ristretto alla Società ed alla nave stessa nelle persone del Comandante e del Responsabile per la security di bordo e non può essere reso disponibile senza l'autorizzazione del Responsabile per la security della Società.

Il Piano, incluse le relative revisioni, è approvato dal Capo del Compartimento marittimo con le stesse modalità di cui alla circolare titolo "Security" n° 01 in data 02.12.2003 e successive integrazioni. Gli unici piani approvati sono quelli con evidenza in originale dell'approvazione come sopra indicato.

Lista di distribuzione controllata

Il Piano deve essere protetto da parte degli interessati e non deve essere reso accessibile alle persone non coinvolte nelle attività indicate nel piano stesso. Il piano è approvato in n.5 originali. Sulla copertina del Piano viene indicato il nr. della copia. 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. Di seguito si riporta la lista di distribuzione controllata standard. Eventuali variazioni nella distribuzione delle copie del piano all'interno del complesso Società/nave dovranno essere preventivamente richieste dal

Responsabile per la security della Società alla competente Autorità marittima. La lista di distribuzione deve essere aggiornata di conseguenza.

Società	Nave	Amministrazione
1 Responsabile per la security della Società	3 Responsabile per la security di bordo	4 Autorità che procede all'approvazione del piano
2 Sostituto responsabile per la security della Società (eventuale)		5 Centrale operativa di COGECAP alla quale dovrà essere fornita anche una copia su supporto informatico.

Generalmente il piano e la nave non sono soggetti a controlli da parte dell'Autorità competente per la sicurezza marittima a meno che un ufficiale debitamente autorizzato non abbia fondati motivi per ritenere che la nave non sia conforme ai requisiti di security richiesti. In tal caso gli ufficiali debitamente autorizzati possono accedere al piano per individuare le eventuali appropriate azioni correttive.

5.3 Riesame

Annualmente il piano di security nave viene assoggettato a riesame interno sulla base delle valutazioni effettuate dal CSO e dallo SSO al fine di garantirne la dovuta efficacia. Durante tale revisione si dovranno tener in debito conto le risultanze di:

- verifiche effettuate dall'Amministrazione;
- audit interni;
- esperienze a seguito di esercitazioni o addestramenti svolti a bordo sulla security ed eventuali problematiche emerse;
- incidenti relativi alla security occorsi alla nave o rapporti di incidenti avvenuti su altre navi
- esperienze acquisite nel tempo in materia di security o in risposta a nuovi requisiti.

Le modifiche del Piano devono essere validate dal CSO ed approvate dall'Amministrazione. Quando le parti revisionate vengono inviate alle persone indicate nella lista di distribuzione, queste devono provvedere a:

- accertarsi che il plico contenente la documentazione non sia stato manomesso (nel caso deve essere avvisato subito il CSO);

- aggiornare il piano con le parti revisionate registrando quanto effettuato nel foglio Revisioni contenuto nel piano;
- distruggere le parti sostituite.

E' responsabilità del CSO provvedere, a seguito delle modifiche apportate al piano, l'invio dei relativi aggiornamenti alla nave.

5.4 Audit Interni

Gli audits interni hanno lo scopo di determinare se:

- il sistema di gestione per la security della nave è conforme alle disposizioni stabilite;
- il sistema di gestione per la security è efficacemente messo in atto e mantenuto;
- le attività sono svolte in conformità ai requisiti di base dell'ISPS Code ad eventuali ulteriori requisiti imposti dall'Amministrazione di bandiera.

La periodicità degli audits interni è almeno annuale e al CSO spetta la responsabilità della loro pianificazione. Tali controlli interni dovranno soddisfare quantomeno i seguenti requisiti:

- sono svolti da auditors qualificati che siano preferibilmente indipendenti rispetto alle attività auditate;
- vengono eseguiti utilizzando la modulistica.....;
- prevedono la verifica delle azioni messe in atto per correggere eventuali rilievi da audits precedenti o da verifiche effettuate dall'Amministrazione;
- i risultati degli audits sono registrati nel modulo....., che contiene eventuali rilievi, documentazione di supporto e le conclusioni dell'auditor.

I documenti relativi agli audits interni sono conservati, per un periodo di due anni' dallo SSO a bordo e dal CSO in Società e devono essere resi disponibili durante le eventuali verifiche esterne da parte di funzionari debitamente autorizzati.

5.5 Gestione rilievi

Nel caso di rilievi relativi ad anomalia nel funzionamento delle apparecchiature o dei sistemi di sicurezza o di sospensione di una misura di sicurezza per qualsivoglia motivo, devono essere individuate ed attuate temporanee misure di sicurezza equivalenti. Tali misure sono notificate dal CSO all'Autorità che ha approvato il piano ed alle Autorità designate interessate .

CAPITOLO VI

PROCEDURE PER I PRINCIPALI INCIDENTI DI SECURITY

6.1 Generalità

Scopo di questo capitolo è quello di individuare “migliori pratiche” (best practices) che possano essere utilizzate dai CSO nella redazione dei piani relativamente alla 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 una nave, dell’equipaggio, dei passeggeri o delle persone comunque presenti a bordo.

Deve essere fatta salva la potestà decisionale del comando di bordo, in assenza di ordini da parte delle competenti autorità, di adottare misure o intraprendere attività non individuate nelle presenti “migliori pratiche” 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/sequestro.

Ferme restando le pianificazioni di emergenza del Ministero dell’Interno – Autorità Nazionale di Pubblica Sicurezza, è necessario che da parte della Società, dell’armatore, del comando di bordo venga sviluppata per la nave una semplice ma concreta “pianificazione di contingenza” per i sotto riportati scenari:

- minaccia di bomba a bordo;
- ricerca di bomba/oggetti sospetti (IED) a bordo;
- rinvenimento di armi, munizioni ed esplosivi;
- sgombero di sezioni/aree della nave;
- evacuazione della nave.

La pianificazione di contingenza deve includere l’elencazione delle attività essenziali da svolgere e delle persone da impiegare in tali attività, nonché gli enti/persona da contattare.

Le procedure per l’evacuazione sono una parte essenziale del piano. Queste procedure potrebbero risultare 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 ciascuna nave:

- presenza di adeguati e prontamente disponibili mezzi di sfuggita;
- numero totale delle persone che potrebbero essere presenti a bordo;
- presenza di persone per le quali potrebbero esservi specifiche necessità (es. età, stato fisico ecc.);
- presenza di una via alternativa di fuga, in direzione diversa da quella principale, tale da consentire alle persone di trovare scampo nel caso quella principale risultasse bloccata.

6.1.1 Consapevolezza

La Società ed il comando di bordo devono incentivare la consapevolezza dell'equipaggio sull'importanza di un'attenta vigilanza e di un professionale approccio all'esigenza di incrementare la sicurezza (security) nel settore del trasporto marittimo nazionale.

In tale ottica la politica aziendale deve contemplare l'aspetto dell'indottrinamento e della familiarizzazione dei propri dipendenti, sia a bordo che a terra, 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.

6.2 Rapportazione degli incidenti di security rilevanti

6.2.1 Procedure

Il piano di security della nave deve individuare le 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 comando di bordo;
- consentire al comando di bordo, previa una valutazione dei fatti, di riportare le rilevanti situazioni agli organi competenti.

6.2.2 Segnalazione interna

Il personale di bordo deve essere consapevole della procedura di segnalazione. Tale procedura deve essere semplice da seguire e tale da incoraggiare l'attività di segnalazione. Il comando di bordo deve procedere ad una investigazione, per ogni segnalazione di ISR, nella misura considerata necessaria in base al suo professionale giudizio.

6.2.3 Rapportazione esterna

Per la rapportazione degli ISR il comando di bordo deve poter contare su aggiornate schede contenenti i numeri utili per contattare le rilevanti autorità. Tali schede devono contenere le indicazioni dei punti di contatto, preferibilmente relative a più di un sistema di comunicazione.

6.2.4 Falsi allarmi

Quando le segnalazioni di ISR non sono considerate credibili, da parte del comando di bordo non è richiesta una rapportazione. Il comando di bordo dovrebbe però considerare di mantenere una registrazione degli elementi salienti di quanto avvenuto al fine di renderli disponibili in caso di eventuale richiesta da parte degli organi inquirenti.

6.3 Allarme bomba, rinvenimento oggetti sospetti

6.3.1 Premessa

Lo scopo del presente paragrafo è quello di fornire alcune nozioni e principi utili per ridurre la possibilità di introduzione a bordo 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 della specifica nave e della contingente situazione e che dovranno essere inserite nel presente piano.

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 COMANDO DI BORDO.

6.3.2 Eventi IED

Un evento IED può avere origine da:

- segnalazione, anche anonima, o notizia di intelligence;
- scoperta di un oggetto sospetto a bordo o in prossimità della nave.

a) segnalazione telefonica o radio

Chi risponde deve 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.

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

Al fine di favorire la raccolta di informazioni nella maniera più completa dovrà essere compilato il form in allegato 1, che deve essere sempre disponibile presso gli apparati radio e presso l'eventuale 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 la Società e il comando di bordo devono 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 a bordo 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 deve essere considerato come un ordigno IED e pertanto si deve:

- 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 boccaporti e portelli delle aree limitrofe per favorire lo sfogo dell'eventuale esplosione.

6.3.3 Precauzioni anti IED

6.3.3.1 Visite a bordo

Le visite di persone non facenti parte dell'equipaggio (per le navi passeggeri limitatamente alle aree/locali agli stessi non destinati) devono essere fatte preferibilmente in gruppi di persone, ove possibile sotto il controllo di un responsabile.

L'itinerario dovrebbe, di norma, escludere i locali sensibili della nave (plancia, stazione radio, sala macchine, ecc.) ed al termine della visita si deve prevedere una ronda di controllo lungo l'itinerario seguito.

6.3.3.2 Intervento a bordo di personale tecnico/operai

Nel caso di accesso a bordo di tecnici/operai per l'effettuazione di lavori, tale personale deve essere identificato, registrato e, ove possibile, monitorato da un membro dell'equipaggio allo scopo designato.

Al termine della giornata lavorativa e prima dell'uscita dei tecnici/operai, il personale designato deve accertare l'avvenuta rimozione di tutto il materiale utilizzato per i lavori, salvo che la permanenza a bordo non sia stata autorizzata.

Allo scopo sarebbe utile prendere nota dei materiali introdotti, in modo da poter procedere al controllo dell'avvenuta rimozione.

6.3.3.3 Altre precauzioni

E' opportuno, previo un appropriato indottrinamento dell'equipaggio, prestare sempre attenzione ad eventuali oggetti (per es. bagagli) eventualmente lasciati incustoditi a bordo o in prossimità della nave ed alle auto lasciate incustodite (all'imbarco o allo sbarco) per le quali non venga prontamente individuato il proprietario.

6.3.4 Modalità di reazione in caso di allarme IED

6.3.4.1 Reazione

L'equipaggio deve 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 a bordo, si dovrebbe disporre per l'effettuazione di chiamate con semplici parole in codice, da stabilirsi nave per nave, che dovranno significare: EMERGENZA – ALLARME IED – TUTTO L'EQUIPAGGIO VERIFICHI L'EVENTUALE PRESENZA DI OGGETTI SOSPETTI NEL PROPRIO POSTO DI LAVORO ovvero altro similare ordine previsto dalle pertinenti procedure.

Deve essere stabilito un punto di coordinamento delle attività connesse alla segnalazione IED in un luogo ritenuto sicuro dell'unità. Esso deve essere preposto allo svolgimento delle seguenti attività:

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

Nel punto di coordinamento è 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...).E' altresì opportuno che siano assicurate le comunicazioni tra il personale del punto di coordinamento, quello delle squadre di ricerca e gli enti/autorità a terra (radio portatili, cellulari ecc...) da poter attivare alla bisogna ed in luoghi ritenuti sicuri.

Nel punto di coordinamento devono essere altresì disponibili: il presente piano, gli ulteriori piani nave ritenuti necessari, le localizzazioni dei punti di comunicazione fissa di bordo, nonché l'elenco dell'equipaggio presente a bordo e degli eventuali passeggeri/visitatori.

Per la registrazione delle più salienti attività, il comando di bordo valuterà l'opportunità di impiegare le allegate check list (Allegati 2 e 3) che potranno essere integrate dal bordo in base alle esigenze contingenti.

6.3.4.2 Sgombero dell'area ed evacuazione della nave

Lo sgombero delle persone dall'area interessata dall'eventuale rinvenimento dell'oggetto IED deve essere disposto dal personale che effettua la ricerca.

L'evacuazione delle persone dalla nave deve avvenire all'ordine del comando di bordo o di chi ha assunto la direzione delle operazioni.

Sarebbe opportuno che il personale di bordo sceso dalla nave rimanga a disposizione nei pressi della stessa fino all'arrivo delle forze dell'ordine per la realizzazione di un eventuale cordone di sicurezza.

Nel caso la scoperta dell'ordigno avvenga alla fonda o in navigazione, occorre stabilire dei punti di adunata su ponti esterni lontani dai locali interessati dal rinvenimento.

6.3.4.3 Rapportazione dell'allarme

Il comando di bordo dovrà prontamente rapportare alle autorità competenti che sono:

- con nave in porto, la Polizia di Stato;
- con nave in navigazione, la Polizia di Stato. Qualora il collegamento con il competente organo della PS non sia possibile, la comunicazione dovrà essere indirizzata all'IMRCC ovvero al MRSC o all'Autorità Designata.

6.3.5 Ricerca di IED

6.3.5.1 Prima ricerca

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

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

Si deve 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 o alloggiano nei locali interessati, in quanto più idonei alla rilevazione di eventuali oggetti estranei. Nell'esecuzione della ricerca il personale deve essere equipaggiato con le dotazioni di protezione individuali di cui al precedente punto 6.3.4.1, 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 4). La ricerca deve 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.

Oggetto di particolare attenzione deve essere quei luoghi che ben si prestano all'occultamento, quali ad esempio:

- carrugetti;
- carabottini;
- prese d'aria;
- spazi sovrastanti e retrostanti condotte d'aria, tubolature, fasci di cavi;
- attrezzature coperte da cappe.

Qualora in un locale, a seguito di una prima ricerca, non sia stata rilevata la presenza di oggetti sospetti, l'esecutore della ronda deve 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 deve essere interrotta anticipatamente (15 minuti prima dell'ora comunicata) per permettere l'eventuale evacuazione delle persone ed il completamento delle misure di difesa passiva tendenti alla riduzione dei danni, lasciando proseguire la ricerca al personale artificiere eventualmente intervenuto.

6.3.5.2 Scoperta

Qualora in un locale sia stata rilevata la presenza di un oggetto sospetto, l'esecutore della ricerca deve 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 ad interdirla gli accessi mediante nastro bicolore;
- lasciare aperte tutte le porte ed i portelli stagni 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 comando di bordo deve tempestivamente riportare il fatto alle autorità competenti di cui al precedente punto 6.3.4.3 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. Occorre 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.

Devono essere predisposti gli assetti antincendio e di evacuazione/abbandono nave più opportuni.

6.3.5.3 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 delle navi per verificare l'eventuale presenza di ulteriori IED.

6.3.5.4 Intervento di artificieri

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

6.4 Armi, munizioni ed esplosivi

6.4.1 Generalità

L'imbarco ed il trasporto degli esplosivi sulle navi nazionali sono vietati salvo che non vengano effettuati nel rispetto delle specifiche norme applicabili.

Ferme restando le disposizioni del Codice penale e del T.U.L.P.S., degli articoli 193 e 1199 del Codice della navigazione nonché 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.

6.4.2 Trasporto armi e munizioni

La Società e/o l'armatore devono sviluppare politiche coerenti con le finalità del presente documento. Qualora il trasporto a seguito dei passeggeri di armi e munizioni non sia escluso da tali politiche aziendali, la gestione delle armi e delle munizioni trasportate dai passeggeri deve essere improntata al rispetto delle indicazioni di seguito riportate.

Previa autorizzazione del comando di bordo, le armi proprie e le munizioni potranno essere trasportate dai passeggeri che posseggano le relative necessarie licenze/autorizzazioni di porto/possesso/trasporto rilasciate dalle competenti autorità di Pubblica Sicurezza.

I passeggeri all'imbarco dovranno consegnare per la custodia le armi "proprie" e le munizioni. La riconsegna dovrà avvenire allo sbarco. La nave dovrebbe destinare appositi idonei locali per l'esigenza della custodia.

Qualora alla nave, agli impianti portuali toccati ovvero nei tratti di mare interessati dai viaggi, sia applicabile il livello di security 2 o 3, il trasporto di armi proprie e munizioni da parte dei passeggeri non dovrebbe essere consentito anche in assenza di specifiche disposizioni da parte dell'ANSM o dell'Autorità designata.

Le precedenti indicazioni non si applicano nei confronti di appartenenti alle FF.AA. , agli organi di Polizia o dei servizi di sicurezza sussidiaria.

Onde consentire un'opportuna informazione dell'utenza, la Società e l'armatore dovrebbero individuare un'idonea forma di avviso (es.: cartellonistica ecc.) da esporre presso i punti individuati per la vigilanza e, per quanto possibile, presso le biglietterie.

6.4.3 Armi potenziali

La nave deve identificare e registrare ogni oggetto/dotazione di bordo che potrebbe essere impiegata come arma da parte di persone presenti a bordo. Nella lista delle potenziali armi sono da annoverare dotazioni quali pistole lanciarazzi, cannoncini lanciasagole, asce da pompieri e grossi coltelli da cucina.

Per quanto possibile le armi potenziali devono essere custodite e chiuse in luoghi non accessibili al pubblico. Quando ciò non sia possibile un membro dell'equipaggio deve essere incaricato di monitorare tali dotazioni per segnalare tempestivamente l'eventuale loro rimozione non autorizzata.

6.4.4 Rinvenimento armi e munizioni

La Società ed il comando di bordo devono assicurare che l'equipaggio della nave sia consapevole della pericolosità connessa con la presenza di armi e munizioni e della necessità di assicurare una discreta ma continua vigilanza.

Nel caso di rinvenimento di armi o munizioni, la nave deve avere 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 comando;
- l'allontanamento dall'area interessata delle persone non appartenenti all'equipaggio;
- 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 reportazione alla Polizia di Stato. Con nave in navigazione e qualora il collegamento con il competente organo della P.S. non sia possibile, la reportazione deve essere fatta all'Autorità designata.

6.5 Impossessamento, sequestro e rapina

6.5.1 Generalità

Scopo del presente paragrafo è quello di divulgare le "migliori pratiche" scaturite a seguito dell'esperienza maturata nell'industria marittima internazionale che si è dovuta confrontare con fenomeni quali il terrorismo e la pirateria caratterizzati da incidenti di security rilevanti come l'impossessamento, il sequestro, la presa di ostaggi, la rapina ecc...

Sebbene gli atti di pirateria non siano un fenomeno presente nei nostri mari e solo raramente essi siano stati registrati in passato (2003) nel mare Mediterraneo, l'esperienza maturata dal personale marittimo, vittima di questo fenomeno nelle altre parti del globo, porta a ritenere che le migliori pratiche individuate per questa specifica minaccia possano trovare utile impiego anche in altre situazioni di atti illeciti dolosi contro la sicurezza (security) delle navi, delle persone e dei beni presenti a bordo.

Si ritiene pertanto opportuno individuare pratiche applicabili nelle varie fasi temporali nelle quali un possibile attacco ad una nave può essere di massima suddiviso, posto che alcune situazioni operative sono sostanzialmente simili ancorché l'attacco abbia finalità diverse.

Nell'applicare gli indirizzi di seguito riportati, gli equipaggi devono essere consapevoli 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.

Il verificarsi di questa tipologia di incidente di security rilevante con nave in porto generalmente consente un tempestivo allertamento delle forze dell'ordine le quali potranno impartire le più opportune disposizioni. Si ritiene, quindi, di delineare di seguito quelle "migliori pratiche" che potrebbero essere seguite quando la nave si trovi in navigazione. Ciò non esclude il fatto che il comando di bordo, anche nel caso di nave in porto, in attesa dell'intervento delle autorità competenti, possa, in base al suo professionale giudizio, porre in essere attività mutate dall'altra situazione operativa (in navigazione) qualora le stesse siano ritenute utili a ridurre il livello del rischio.

6.5.2 Fase di pre attacco

La Società ed il comando di bordo delle navi che operano in acque nelle quali vi sia una maggiore possibilità d'attacco (Particolari situazioni geografiche, livelli di security superiori al SL1, ecc...), ciascuno per gli aspetti di propria competenza, devono:

- essere consapevoli della necessità di incrementare la vigilanza e di fare ricorso ad idonei supporti tecnologici di sorveglianza e scoperta, essendo consci del fatto che una precoce scoperta di un possibile attacco è il più efficace deterrente nei confronti dello stesso;
- prima di entrare in dette aree, accertarsi della funzionalità delle apparecchiature e dotazioni che potrebbero trovare un utile impiego nella prevenzione e gestione di un incidente di security rilevante (radar, apparati radio fissi e portatili, sistemi addizionali di sorveglianza e scoperta ecc...);
- per quanto possibile e ragionevole, tenersi distanti dalle aree nelle quali la minaccia è maggiore. Nel caso si renda necessaria una sosta in dette acque, sarebbe opportuno valutare la possibilità di non ancorare, preferendo un pendolamento a lento moto a situazioni nelle quali i tempi di ripristino delle capacità di spostamento ed evoluzione siano lunghi;
- essere in grado di poter contattare le competenti autorità (IMRCC, MRSC – Autorità designate ecc...) nel caso vengano individuate situazioni sospette che facciano presagire l'imminenza dell'attacco. Il comando di bordo dovrebbe considerare che eventuali "segnalazioni di pericolo" vanno impiegate solo in caso di "imminente pericolo". Tale ponderato apprezzamento consentirebbe di evitare a forme di allertamento generale che potrebbero sfociare in uno svilimento di tali segnalazioni che devono, invece, essere caratterizzate dalla necessità di immediata assistenza;

- per quanto compatibile con le altre esigenze, assicurarsi che lungo le murate non siano lasciate inutilizzate dotazioni e strutture che possano facilitare l'ingresso a bordo a persone non autorizzate (cime appennellate, biscaggine e scalandroni ammainati, bettoline e maone non presidiate ecc...). Vanno altresì tenute chiuse tutte quelle aperture di non immediato uso (Aperture a murata, portelloni di imbarco, boccaporte, porte esterne, oblò ecc...);
- considerare che, dall'analisi di molti eventi accaduti, è emerso che la cattura e la tenuta sotto minaccia di una persona è risultato essere il mezzo più utilizzato dagli attaccanti per guadagnare il controllo graduale dell'intera nave. Pertanto e in special modo nelle ore notturne e nelle zone a maggior rischio, le persone non impegnate in rilevanti attività di servizio che richiedano la loro presenza all'esterno, dovrebbero rimanere all'interno delle sovrastrutture. Coloro i quali devono invece operare all'esterno, dovrebbero essere muniti di mezzi di comunicazione con il personale di guardia. Nell'espletamento delle ronde tale circostanza deve essere tenuta nella massima considerazione;
- approntare manichette ed idranti antincendio sui ponti esterni. L'impiego di forti getti di acqua in alcuni casi si è rivelato utile per scoraggiare i tentativi di abbordaggio, in special modo nei confronti di piccoli battelli nei quali gli impianti elettrici dei motori possano essere danneggiati da tali getti;
- essere in grado di effettuare manovre evasive quali rapide, accentuate ed alternate accostate in abbinata con l'incremento della velocità a quella massima sostenibile. Gli effetti del moto ondoso provocato potrebbero, infatti, fungere da deterrente nei confronti di piccoli battelli attaccanti e rendere più difficoltoso l'eventuale uso di rampini. L'effettuazione di tali manovre evasive deve essere opportunamente valutata nel caso di aree di mare ristrette e congestionate;
- essere consapevoli che l'eventuale uso o dimostrazione di armi da parte delle persone a bordo è altamente sconsigliabile. L'impiego di armi non solo richiede una specifica "capacità ed addestramento" - fatto che, normalmente, non è riscontrabile negli equipaggi - ma potrebbe causare una "escalation" della violenza nell'attacco.

6.5.3 Fase di abbordaggio

In questa fase si dovrebbe far ricorso a vigorose manovre evasive ed all'impiego dei getti d'acqua. L'equipaggio eventualmente impiegato sui ponti esterni deve essere stato precedentemente indottrinato sulle segnalazioni significanti l'ordine di rientro all'interno delle sovrastrutture. Se non già in contatto con le autorità competenti (IMRCC, MRSC, Autorità designata e Polizia di Stato) ogni sforzo deve essere fatto per stabilire tale comunicazione.

6.5.4 Fase iniziale dell'impossessamento

Qualora gli attaccanti siano riusciti a salire a bordo, le azioni del comando di bordo e dell'equipaggio devono essere finalizzate a:

- per quanto possibile, chiudere le vie d'ingresso dall'esterno verso l'interno. Tale attività potrebbe essere effettuata in sequenza, con zone sempre più ristrette, per ritardare la presa di possesso completa;
- cercare di rimanere in posizione di controllo tecnico della navigazione (Ponte di comando, locali propulsione ed organi di governo);
- attivare, ove disponibili, tutti i sistemi di registrazione (CCTV ecc..) cercando di rendere il meno evidente possibile tale funzionamento.

Le opzioni disponibili al comando ed all'equipaggio dipenderanno dalle finalità e metodiche dell'attacco (terrorismo o azioni criminali d'altra natura) e dagli strumenti di pressione (ostaggi). Non dovrebbe essere presa in considerazione l'ipotesi di effettuare sortite ovvero di tentare la cattura di uno o più degli attaccanti.

Qualora venga deciso di far confluire le persone presenti a bordo verso specifici punti di raccolta, gli stessi dovrebbero essere scelti in base al requisito della presenza di una via di sfuggita alternativa alla principale.

Per quanto possibile, ogni sforzo deve 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..).

6.5.5 Fase finale dell'impossessamento

Qualora gli attaccanti abbiano guadagnato il controllo dei punti nevralgici della nave e/o abbiano catturato ostaggi, il comando di bordo e l'equipaggio dovrebbero cercare di mantenere la calma anche per assicurare gli eventuali passeggeri.

In assenza di esplicite istruzioni da parte delle autorità competenti, il comando dovrebbe tentare di instaurare un negoziato con gli attaccanti al fine di riportare sotto la gestione dell'equipaggio il controllo tecnico della navigazione e di agevolare il rilascio degli eventuali ostaggi.

Il comando di bordo 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 comando di

bordo e l'equipaggio dovrebbero 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.

CAPITOLO VII

RICHIESTA DI INFORMAZIONI E RAPPORTAZIONE DI INCIDENTI DI SECURITY

7.1 Generalità

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.

7.2 Liste punti di contatto

La nave deve poter contare su dati aggiornati dei vari punti di contatto delle autorità, degli enti e degli altri soggetti rilevanti, in materia di security, coerentemente ai tipi di viaggio effettuati.

La società ed il comando di bordo devono procedere alla redazione ed all'aggiornamento 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 5;
- integrate con altri dati ritenuti eventualmente necessari/opportuni;
- sufficientemente differenziate per le varie aree geografiche d'interesse. Ciò per tener in debito conto anche le varie competenze territoriali esistenti relativamente ai viaggi ed alle interfacce previste.

Le schede dei punti di contatto devono essere tenute costantemente aggiornate dalla nave 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.

7.3 Mezzo di comunicazione

Nell'individuazione del mezzo di comunicazione da impiegare per lo scambio di informazioni di security, il comando di bordo 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 dei "media" da utilizzare resta ovviamente salva la professionale valutazione del comando di bordo di fattori quali la necessità e l'urgenza che potrebbero giustificare l'impiego di qualsivoglia mezzo/sistema di comunicazione.

7.4 Tipologia della comunicazione

Anche a seguito delle valutazioni accennate nel precedente paragrafo 3, il comando di bordo 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.

**INFORMAZIONI DA RACCOGLIERE IN CASO DI COMUNICAZIONE
DI BOMBA A BORDO**

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

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

PROVA AD OTTENERE LE SEGUENTI INFORMAZIONI (poni le domande nel seguente ordine):
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?

COMPLETA CON:
MEZZO DI RICEZIONE
ORARIO DI RICEZIONE DELLA CHIAMATA
NOME \ COGNOME OPERATORE

DA CONSEGNARE IMMEDIATAMENTE AL RESPONSABILE DELLA SECURITY

CHECK LIST

MINACCIA BOMBA CON NAVE IN PORTO

MISURA DI SECURITY	NOTE
Allertare 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/soggetti: CP, AP, Vigili del Fuoco, PFSO o responsabile per la security dell'impianto.	
Sospendere le operazioni non essenziali.	
Approntamento degli impianti antincendio.	
Approntamento disalimentazione elettrica a zone.	
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 equipaggio non essenziale.	
Evacuazione generale.	
Altro.	

CHECK LIST

MINACCIA BOMBA CON NAVE IN NAVIGAZIONE O ALLA FONDA

MISURA DI SECURITY	NOTE
Allertare il personale usando il Public Address System o altro mezzo ritenuto idoneo.	
Rapportare alla Polizia di Stato (Qualora il collegamento con la PS non sia possibile, riportare a IMRCC ovvero MRSC o Autorità designata).	
Se non già fatto con la reportazione, informare IMRCC ovvero MRSC o Autorità designata.	
Sospendere le operazioni non essenziali.	
Approntamento degli impianti antincendio.	
Approntamento disalimentazione elettrica a zone.	
Se alla fonda, approntamento apparati propulsivi.	
Approntamento mezzi collettivi di salvataggio.	
Stabilire team e zone ricerca IED. Distribuire dotazioni.	
Inizio prima ricerca.	
In caso di rinvenimenti IED, sgombero e segnalazione dell'area interessata.	
Ripetizione ricerca.	
Evacuazione passeggeri.	
Evacuazione equipaggio non essenziale.	
Abbandono nave.	
Altro.	

**QUESTIONARIO RILIEVO CARATTERISTICHE
DEL POSSIBILE IED**

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

ORA RILIEVO

NOME / COGNOME OPERATORE

DA CONSEGNARE IMMEDIATAMENTE AL RESPONSABILE DELLA SECURITY

ALLEGATO 5

NUMERI UTILI PER RICHIESTA INFORMAZIONI E RAPPORTAZIONE SITUAZIONI PER LA
NAVE DURANTE LA NAVIGAZIONE O L'INTERFACCIA CON L'IMPIANTO PORTUALE DI

.....

Organizzazione	Nome	Telefono Ufficio	Cellulare	Altri tipi di contatto
Responsabile per la security della Società ed eventuale suo vice				
Referente per la security dell'impianto portuale ed eventuale suo vice				
I.M.R.C.C. Roma	Centrale Operativa			
M.R.S.C.	Sala Operativa			
Capitaneria di Porto a) <input type="checkbox"/> Autorità Designata b) <input type="checkbox"/> Autorità Marittima	Sala Operativa			
Autorità Portuale	Referente Security			
Polizia di Stato a) <input type="checkbox"/> Uff. Polizia Front. b) <input type="checkbox"/> Commissariato c) <input type="checkbox"/> Questura	Centralino			
Guardia di Finanza	Centralino			
Vigili del Fuoco	Personale di guardia			
Dogana	Centralino			
Servizi Tecnico Nautici a) <input type="checkbox"/> Piloti b) <input type="checkbox"/> Ormeggiatori c) <input type="checkbox"/> Rimorchiatori d) <input type="checkbox"/> Barcaioni				

Aggiornamenti a cura della nave

Data: _____

APPENDICE I

Scheda A

REG. (EC) 725/2004 Art.3.3 – APPLICAZIONE DI NORME DI MARITIME SECURITY ALLE ALTRE NAVI IN SERVIZIO NAZIONALE ED AI CONNESSI IMPIANTI PORTUALI

NAVI PASSEGGERI

N°	CATEGORIA (a)	PRESENZA DELLA COMPANY (Reg. 336/2006)	SHIP SECURITY al 1 LUGLIO 2007	PORT FACILITY SECURITY al 1 LUGLIO 2007
1	Ro – Ro	SI già prevista ai sensi del Reg.CE 3051/95 (ora abrogato dal 336/06)	<p>Alle navi PAX Ro-Ro in Navigazione Nazionale, diverse da quelle di classe A (98/18/CE) già coperte dalla SOLAS/ISPS, si applicherà un assetto di security identico a quello determinato per le altre navi PAX di cui ai punti 3, 4, 5 e 6 ricorrendo alla seguente assimilazione per quanto attiene ai limiti di navigazione:</p> <p>- Nazionale come HSC, DSC, ALISCAFI del punto 3 - Naz. Co. come classe B 98/18 - Naz. Li. come classe C 98/18 - Naz. Lo. come classe D 98/18</p>	Negli impianti portuali si adotteranno le misure previste nei rispettivi punti 3, 4, 5 e 6.
2	Altre navi PAX non 98/18/CE	SI dal 24.03.2008 ad eccezione di quelle che effettuano viaggi in tratti di mare assimilabili alle navigazioni di classe C e D (98/18/CE) per le quali non si applica il Reg. 336/2006.	<p>Alle altre navi PAX (non Ro-Ro), diverse da quelle 98/18/CE, si applicherà un assetto di security identico a quello determinato per le PAX di cui ai punti 3, 4, 5 e 6 ricorrendo alla seguente assimilazione per quanto attiene ai limiti di navigazione:</p> <p>- Nazionale come HSC, DSC, ALISCAFI del punto 3 - Naz. Co. come classe B 98/18 - Naz. Li. come classe C 98/18 - Naz. Lo. come classe D 98/18</p> <p>Per le NAVIGAZIONI SPECIALI, se le navi non hanno una già individuata collocazione nella Naz., Naz.Co., Naz.Li. o Naz.Lo., si seguirà un processo di assimilazione considerando il valore della distanza massima dalla costa.</p>	Negli impianti portuali si adotteranno le misure previste nei rispettivi punti 3, 4, 5 e 6.
3	<p>HSC } DSC } che effettuano navigazione oltre 20 mg dalla costa ALISCAFI }</p> <p>PAX Ro-Ro assimilate del punto 1 (Nav. Nazionale)</p> <p>Altre navi PAX assimilate del punto 2 (Nav. Nazionale)</p>	<p>SI già prevista dalla SOLAS</p> <p>SI già prevista dalla SOLAS</p> <p>SI dal 24. 03. 2008</p> <p>SI già prevista</p> <p>SI</p>	<p>1) se abilitate al trasporto di \geq 450 passeggeri: • ISTRUZIONI PESANTI fino al 23. 03. 2008; • ORGANIZZAZIONE DI SECURITY LEGGERA dal 24.03.2008.</p> <p>2) se abilitate al trasporto di $<$ 450 passeggeri: • ISTRUZIONI LEGGERE fino al 23. 03. 2008; • ISTRUZIONI PESANTI dal 24. 03. 2008.</p>	Negli impianti portuali si adotteranno pertinenti misure (istruzioni leggere, istruzioni pesanti e organizzazione di security leggera) coerenti con le previsioni imposte alle navi in base alla portata di passeggeri delle stesse così come riportata, per la stagione in corso, nei relativi certificati di abilitazione. Gli impianti portuali già muniti di un PFSP approvato potranno provvedere ad una sua integrazione mediante una sezione "ad hoc" per la gestione della specifica interfaccia.

Segue NAVI PASSEGGERI

4	<p>Classe B (98/18/CE)</p> <p>PAX Ro – Ro assimilate del punto 1 (Naz. Co.)</p> <p>Altre navi PAX assimilate del punto 2 (Naz. Co.)</p> <p>HSC</p> <p>DSC</p> <p>ALISCAFI</p> <p>che effettuano navigazione entro 20 mg dalla costa</p>	<p>SI dal 24. 03. 2008</p> <p>SI già prevista</p> <p>SI</p> <p>SI</p> <p>SI</p> <p>SI dal 24. 03. 2008</p>	<p>1) se abilitate al trasporto di \geq 450 passeggeri:</p> <ul style="list-style-type: none"> • ISTRUZIONI PESANTI; <p>2) se abilitate al trasporto di $<$ 450 passeggeri:</p> <ul style="list-style-type: none"> • ISTRUZIONI LEGGERE fino al 23. 03. 2008; • ISTRUZIONI PESANTI dal 24. 03. 2008. 	<p>Negli impianti portuali si adotteranno pertinenti misure (istruzioni leggere, istruzioni pesanti) coerenti con le previsioni imposte alle navi in base alla portata massima di passeggeri delle stesse così come riportata, per la stagione in corso, nei relativi certificati di abilitazione. Gli impianti portuali già muniti di un PFSP approvato potranno provvedere ad una sua integrazione mediante una sezione "ad hoc" per la gestione della specifica interfaccia.</p>
5	<p>Classe C (98/18/CE);</p> <p>PAX Ro – Ro assimilate del punto 1 (Naz. Li.)</p> <p>Altre navi PAX assimilate del punto 2 (Naz. Li.)</p> <p>HSC, DSC, ALISCAFI che effettuano navigazione entro 6 mg. dalla costa</p>	<p>Non applicabile</p> <p>SI già prevista</p> <p>Non prevista</p> <p>Non prevista</p>	<p>1) se abilitate al trasporto di \geq 450 passeggeri:</p> <ul style="list-style-type: none"> • ISTRUZIONI LEGGERE fino al 23. 03. 2008; • ISTRUZIONI PESANTI dal 24. 03. 2008. <p>2) se abilitate al trasporto di $<$ 450 passeggeri:</p> <ul style="list-style-type: none"> • ISTRUZIONI LEGGERE 	<p>Negli impianti portuali che servono unità abilitate, per la stagione in corso, a trasportare \geq 450 passeggeri si adotteranno pertinenti misure (istruzioni leggere, istruzioni pesanti) coerenti con le previsioni imposte alle navi.</p> <p>Negli impianti portuali che servono unità abilitate, per la stagione in corso, a trasportare $<$ 450 passeggeri è la nave che assicura la security durante l'interfaccia.</p> <p>Gli impianti portuali già muniti di un PFSP approvato potranno provvedere ad una sua integrazione mediante una sezione "ad hoc" per la gestione della specifica interfaccia.</p>
6	<p>Classe D (98/18/CE) ;</p> <p>PAX Ro – Ro assimilate del punto 1 (Naz. Lo.);</p> <p>Altre navi PAX assimilate del punto 2 (Naz. Lo.)</p> <p>HSC, DSC, ALISCAFI che effettuano navigazione entro 3 mg. dalla costa</p>	<p>Non prevista</p> <p>SI già prevista</p> <p>Non prevista</p> <p>Non prevista</p>	<p>ISTRUZIONI LEGGERE</p>	<p>La nave assicura la security durante l'interfaccia.</p> <p>Gli impianti portuali già muniti di un PFSP approvato potranno provvedere ad una sua integrazione mediante una sezione "ad hoc" per la gestione della specifica interfaccia.</p>

(a) Alla nave temporaneamente adibita ad una tipologia di viaggio diversa da quella indicata nel certificato di sicurezza si applicheranno i pertinenti assetti di maritime security richiesti per il tipo di viaggio effettivamente svolto.

NAVI DA CARICO ED ALTRI TIPI

TIPO	STAZZA	COMPANY (Reg. 336/2006) (a)	SHIP SECURITY al 1 LUGLIO 2007	PORT FACILITY SECURITY al 1 LUGLIO 2007
<p>NAVI CARICO</p> <p>comprese HSC, MODU o unità assimilabili ai sensi del D.P.R. n.886/1979</p>	<p>TUTTE</p> <p>unità con stazza ≥ 500 GT</p>	<p>SI dal 24. 03. 2008</p>	<p>1) Se: nave CISTERNA (SOLAS I-A / 2.h) nave PETROLIERA (SOLAS II-1 / 2.12) nave CHIMICHIERA (SOLAS VII-B / 8.2) nave GASIERA (SOLAS VII-C / 11.2)</p> <p>si applicheranno:</p> <ul style="list-style-type: none"> • ISTRUZIONI LEGGERE se impiegate esclusivamente in aree portuali; • ISTRUZIONI PESANTI fino al 23. 03. 2008; • ORGANIZZAZIONE DI SECURITY LEGGERA dal 24. 03. 2008. <p>2) Se altri tipi di navi da carico comprese HSC, MODU o unità assimilabili (886/1979) si applicheranno:</p> <ul style="list-style-type: none"> • ISTRUZIONI LEGGERE fino al 23. 03. 2008; • ISTRUZIONI PESANTI dal 24. 03. 2008. 	<p>Negli impianti portuali si adotteranno pertinenti misure (istruzioni leggere, istruzioni pesanti ed Organizzazione di security leggera) coerenti con le previsioni imposte alle navi in base alla diversa tipologia delle stesse. Gli impianti portuali già muniti di un PFSP approvato potranno provvedere ad una sua integrazione mediante una sezione "ad hoc" per la gestione della specifica interfaccia.</p>

(a) Ai sensi del punto (9) delle premesse del Reg. (CE) n.336/2006, spetta agli Stati membri decidere se applicare il Codice ISM alle navi che effettuano esclusivamente servizio in aree portuali.

SCHEMA SINOTTICO DELL'ESTENSIONE DELLA MARITIME SECURITY ALLE NAVI IN NAVIGAZIONE NAZIONALE ED AI CONNESSI IMPIANTI PORTUALI

ISTRUZIONI LEGGERE (ISLE)	1. PAX HSC, DSC ed Aliscafi in Nav.Nazionale (oltre 20 mg dalla costa) ed altre navi assimilate del punto 3 della Scheda A.	< 450 pass.	dall' 1. 07. 2007 al 23. 03. 2008 poi ISPE
	2. PAX B (98/18/CE), PAX HSC, DSC ed Aliscafi in Naz.Costiera (entro 20 mg dalla costa) e altre navi assimilate del punto 4 della Scheda A.	< 450 pass.	dall' 1. 07. 2007 al 23. 03. 2008 poi ISPE
	3. PAX C (98/18/CE), PAX HSC, DSC ed Aliscafi in Naz.Litoranea (entro 6 mg dalla costa) ed altre navi assimilate del punto 5 della Scheda A.	a) ≥ 450 pass.	dall' 1. 07. 2007 al 23. 03. 2008 poi ISPE
		b) < 450 pass.	dall' 1. 07. 2007 sempre ISLE (a)
	4. PAX D (98/18/CE), PAX HSC, DSC ed Aliscafi in Naz.Locale (entro 3 mg dalla costa) ed altre navi assimilate del punto 6 della Scheda A.		dall' 1. 07. 2007 sempre ISLE (a)
	5. CARICO (Cisterna, Petroliera, Chimichiera e Gasiera)	≥ 500 GT	SE IMPIEGATA ESCLUSIVAMENTE IN AREE PORTUALI dall' 1. 07. 2007 sempre ISLE
6. ALTRE NAVI DA CARICO, comprese HSC, MODU ed unità assimilabili (886/1979)	≥ 500 GT	dall' 1. 07. 2007 al 23. 03. 2008 poi ISPE	
ISTRUZIONI PESANTI (ISPE)	1. PAX HSC, DSC ed Aliscafi in Nav.Nazionale (oltre 20 mg dalla costa) ed altre navi assimilate del punto 3 della Scheda A.	a) ≥ 450 pass.	dall' 1. 07. 2007 al 23. 03. 2008 poi SELE
		b) < 450 pass.	dal 24. 03. 2008 in poi
	2. PAX B (98/18/CE), PAX HSC, DSC ed Aliscafi in Naz.Costiera (entro 20 mg dalla costa) ed altre navi assimilate del punto 4 della Scheda A.	a) ≥ 450 pass.	dall' 1. 07. 2007 in poi
		b) < 450 pass.	dal 24. 03. 2008
	3. PAX C (98/18/CE), PAX HSC, DSC ed Aliscafi in Naz.Litoranea (entro 6 mg dalla costa) ed altre navi assimilate del punto 5 della Scheda A.	≥ 450 pass.	dal 24. 03. 2008 in poi
4. CARICO (Cisterna, Petroliera, Chimichiera e Gasiera)	≥ 500 GT	dall' 1. 07. 2007 al 23. 03. 2008 poi SELE	
5. ALTRE NAVI DA CARICO, comprese HSC, MODU ed unità assimilabili (886/1979)	≥ 500 GT	dal 24. 03. 2008 in poi	
ORGANIZZAZIONE DI SECURITY LEGGERA (SELE)	1. PAX HSC, DSC ed Aliscafi in Nav.Nazionale (oltre 20 mg dalla costa) ed altre navi assimilate del punto 3 della Scheda A.	≥ 450 pass.	dal 24. 03. 2008 in poi
	2. CARICO (Cisterna, Petroliera, Chimichiera e Gasiera)	≥ 500 GT	dal 24. 03. 2008 in poi

(a) I connessi impianti portuali sono esentati da norme di security.

ARGOMENTI DA SVILUPPARE PER LE ISTRUZIONI E PER L'ORGANIZZAZIONE DI SECURITY LEGGERA

REGIME	ITEM PER LE NAVI	ITEM PER GLI IMPIANTI PORTUALI (a)
ISTRUZIONI LEGGERE (ISLE)	<ul style="list-style-type: none"> • Sorveglianza nave (b) (c) • Sorveglianza ingresso passeggeri / visitatori • Sorveglianza imbarco carico e provviste • Procedure per rinvenimento oggetti sospetti • Numeri utili per richiesta informazioni e reportazione situazioni 	<ul style="list-style-type: none"> • Sorveglianza aree interessate dall'interfaccia (b) (c) • Sorveglianza transiti persone • Sorveglianza transito e sosta materiali • Procedure per rinvenimento oggetti sospetti • Numeri utili per richiesta informazioni e reportazione situazioni
ISTRUZIONI PESANTI (ISPE)	<ul style="list-style-type: none"> • Vigilanza nave (d) (f) • Vigilanza ingresso passeggeri / visitatori • Vigilanza imbarco carico e provviste • Procedure per audit interni • Procedure per principali incidenti di security • Numeri utili per richiesta informazioni e reportazione situazioni 	<ul style="list-style-type: none"> • Vigilanza aree interessate dall'interfaccia (e) (f) • Vigilanza transiti passeggeri / visitatori / equipaggi • Vigilanza transito e sosta materiali • Procedure per audit interni • Procedure per principali incidenti di security • Numeri utili per richiesta informazioni e reportazione situazioni
ORGANIZZAZIONE SECURITY LEGGERA (SELE)	<ul style="list-style-type: none"> • Nomina di un responsabile per la security della società (g) (i) • Nomina di un responsabile per la security di bordo • Piano di sicurezza ridotto contenente: <ol style="list-style-type: none"> 1. Valutazione dei rischi 2. Struttura organizzativa per la security 3. Procedure per i 3 livelli Marsec relativamente a: <ul style="list-style-type: none"> - controllo accessi - controllo aree ad accesso limitato - controllo identità passeggeri / visitatori (se applicabile) - controllo operazioni di imbarco carico e provviste (se applicabile) 4. Procedure per audit interni 5. Procedure per principali incidenti di security 6. Numeri utili per richiesta informazioni e reportazione situazioni 	<ul style="list-style-type: none"> • Individuazione di un referente per la security dell'infrastruttura (h) (i) • Piano di sicurezza ridotto contenente: <ol style="list-style-type: none"> 1. Valutazione dei rischi 2. Struttura organizzativa per la security 3. Procedure per i 3 livelli Marsec relativamente a: <ul style="list-style-type: none"> - conterminazione dell'infrastruttura - controllo accessi - controllo aree ad accesso limitato - controllo passeggeri / visitatori / equipaggi (se applicabile) - controllo transito e sosta materiali (se applicabile) 4. Procedure per gli audit interni 5. Procedure per i principali incidenti di security 6. Numeri utili per la richiesta informazioni e reportazione situazioni

- (a) Per impianto portuale si intende quella porzione di area portuale direttamente ed immediatamente connessa con le attività di imbarco oggetto di tutela.
- (b) Le istruzioni ISLE, emanate dall'Autorità competente per la sicurezza marittima (ACSM), sono a carattere generale. Esse saranno diffuse dalle Autorità marittime che potranno integrarle con una specifica sezione inerente le eventuali esigenze / particolarità locali sentita, per quanto attiene gli impianti portuali, la competente Autorità portuale, ove istituita. Tale sezione consentirà un coerente e dinamico adeguamento a contingenti situazioni.
- (c) Per attività di sorveglianza si intende: tener d'occhio o sotto osservazione persone o cose, come misura di sicurezza, per assicurare un normale svolgimento delle attività.
- (d) Le istruzioni ISPE per le navi saranno rilasciate a ciascuna unità dell'Autorità marittima ove è registrata la nave. Tali istruzioni saranno preparate sulla base di linee guida, emanate dall'ACSM, che terranno in debito conto sia la tipologia delle navi sia la specificità dei servizi svolti.
- (e) Le istruzioni ISPE per gli impianti portuali saranno rilasciate dall'Autorità designata competente per territorio sentita l'Autorità portuale, ove istituita. Tali istruzioni saranno preparate sulla base di linee guida, emanate dall'ACSM, che terranno in debito conto la tipologia dei traffici.
- (f) Per attività di vigilanza si intende: attenta sorveglianza allo scopo di esercitare una più intensa attività di prevenzione.
- (g) L'attività di organizzazione e redazione del piano sarà svolta dal Responsabile per la security della società sulla base di linee guida emanate dall'ACSM.
- (h) L'attività di organizzazione e redazione del piano sarà svolta dal Referente per la security dell'infrastruttura sulla base di linee guida emanate dall'ACSM.
- (i) Per attività di controllo si intende: frequente attività di accertamento in seno ai fenomeni oggetto di vigilanza.

N.B.: 1) Le attività di sorveglianza, vigilanza e controllo dovranno essere poste in essere nel periodo temporale funzionale all'espletamento delle attività d'imbarco oggetto di tutela.

2) Le disposizioni riportate nel presente quadro di riferimento organizzativo (schede A, B, C e D) non si applicano alle unità ed agli impianti portuali già disciplinati in base all'art.3.2 del Reg. (CE) n.725/2004.