POLITEXT

Ricard Marí Sagarra

El código PBIP - 1

Operatividad en la interfaz buque-puerto

EDICIONS UPC

POLITEXT 174

El código PBIP - 1

Operatividad en la interfaz buque-puerto

POLITEXT

Ricard Marí Sagarra

El código PBIP - 1

Operatividad en la interfaz buque-puerto

EDICIONS UPC

Subvencionado por el Ministerio de Fomento

Primera edición: diciembre de 2006

Diseño de la cubierta: Manuel Andreu

Edicions de la Universitat Politècnica de Catalunya, SL
Jordi Girona Salgado 31, 08034 Barcelona
Tel.: 934 016 883 Fax: 934 015 885
Edicions Virtuals: www.edicionsupc.es
E-mail: edicions-upc@upc.edu

Producción: Ediciones Gráficas Rey
C/ Albert Einstein, 54 C/B nau 15
08940 Cornellà de Llobregat

Depósito legal: B-54112-2006
ISBN: 978-84-8301-895-8

Índice

Capítulo 4. Mejoras en la transferencia de mercancías

Capítulo 5. Procedimientos tecnificados a la identificación

Capítulo 6. Control de personas y cosas

Capítulo 7. Respuesta humana a situaciones del security

Introducción

El cumplimiento del Cap. XI-2 del Convenio SOLAS, conocido como el código PBIP, adoptado el 12.12.2002, en vigor desde el 1 Julio 2004, así como del Reglamento del Parlamento Europeo y del Consejo, adoptado el 31.03.2004, en vigor desde el 20.05.2004 (DOUE de 29.04.2004), en su aplicación de forma progresiva a los buques,

a) Tráfico marítimo nacional 01.07.2005 (pasaje)
b) Otras categorías de buques (2007)

ha creado un nuevo campo de relaciones operativas entre el buque y la instalación portuaria, en el marco de la voluntad única de la prevención de las situaciones delictivas (nivel 1) como objetivo prioritario, y de lucha abiertamente opositora, cuando se alcance o se supere el nivel 3 de protección.

La puesta en marcha de las normas de obligado cumplimiento, en la protección del entorno marítimo, supone un reto difícil de afrontar por parte de los responsables de seguridad. La principal preocupación es la protección de la interfaz buque – puerto y todos los procedimiento deben estar dirigidos a generar una barrera impermeable a todas las amenazas pasadas, presente y futuras.

Los nuevos sistemas de ataque terroristas y, el uso de nuevas tecnologías por parte de los atacantes dificultan enormemente el trabajo de seguridad que hasta ahora tenía una mínima influencia en los procedimientos portuarios.

Todos los estudios realizados hasta este momento por diferentes entidades son pesimistas respecto a la capacidad de evitar en tiempo real un atentado en una instalación portuaria. Los actos acaecidos hasta la fecha así lo demuestran. El puerto de Ashdod es un ejemplo claro de que frente a la determinación terrorista pocos son los sistemas de seguridad que aguantan.

En esta ocasión, dos suicidas hicieron explotar sus bombas, uno dentro del puerto junto a la cerca (del perímetro exterior) y otro fuera. Las explosiones, que se produjeron de forma casi simultánea y que en un principio fueron interpretadas como la explosión de algún depósito de combustible, causaron también unos quince heridos, tres de ellos en estado grave. Ashdod es uno de los dos puertos israelíes más importantes en el mar Mediterráneo. También está la principal base de la marina israelí en el sur del país y por esta razón cuenta con un alto nivel de seguridad, estando restringido el acceso mediante varios controles. Aun así los terroristas consiguieron en parte su objetivo.

Podemos concluir que el peso de la lucha contra el terrorismo se centra en la información muy lejos del puerto y más aún del buque. Pero tenemos la obligación de generar cuantas barreras podamos para

evitar que el problema llegue al buque, o a tierra desde éste, superando los procedimientos de la Interfaz. Todo esto sin romper o entorpecer la dinámica portuaria ni la actividad marítima.

Actualmente, la seguridad portuaria establecida por el Plan de Protección de Buques e Instalaciones Portuarias va generando en todo el mundo procedimientos, normas y actuaciones por parte de las fuerzas de seguridad, tanto pública como privada. No obstante, la tónica general es cubrir la seguridad con el mínimo presupuesto posible, y esta falta de presupuesto afecta por igual a los medios técnicos necesarios como al factor humano.

La única opción para suplir la falta de presupuestos adecuados es adaptarse de forma no convencional a la nueva situación, aplicando soluciones integradas en los procedimientos habituales del puerto. El control de mercancías y pasajeros existente deberá verse reforzado mediante el análisis de radioscopia, pero también mediante la detección de sospechosos por parte del personal de seguridad. Hoy en día contamos con métodos de protección adecuados para creas espacios estancos con un flujo constante de clientes sin paralizar la operativa del puerto. No podemos romper el funcionamiento del puerto con mejoras operacionales en materia de seguridad que supongan molestias excesivas y entorpezca el desarrollo normal de la actividad portuaria.

La necesidad de fuertes inversiones en la protección del puerto, con prioridad en la interfaz buque – puerto, marca una serie de fases en la implantación tanto de inversiones escalonadas como de adaptación a los nuevos procedimientos del personal de seguridad, empresas, tripulantes y usuarios.

Es evidente que con la implementación de los planes de protección en unos y otros, todos han pasado los requisitos para su verificación. No obstante, los planteamientos de protección (security) no pueden esquematizarse como si fueran las habituales respuestas a riesgos incluidos en el safety. Los planteamientos no están relacionados con variables físicas o químicas, con resistencias estructurales o de cualquier otro tipo medible *a priori*. Ahora el problema se amplia o se modifica sustancialmente la voluntad (maldad) humana de llevar a cabo un acto delictivo, con la enorme variabilidad de posibilidades que ello significa.

El proceso se complica cuando, además, el suceso o conflicto interacciona con fuerzas ajenas al buque, que generalmente conoce insuficientemente el medio en que se desarrolla la actividad marítimo-portuaria del transporte, aunque parta de mejores conocimientos en procedimientos técnicos y operativos de control en este tipo de amenazas.

Cabe decir que sin un sistema organizativo moderno, con una completa implantación del modelo de mando único poco se podrá hacer para reducir los riesgos de ataque terrorista y menos aún para reducir las pérdidas en caso de que el ataque se materialice. Esto quedó ampliamente demostrado en los últimos atentados masivos contra ciudades en todo el mundo llevados a cabo por Al Qaeda.

El estudio presenta un nivel de conocimientos especializados en los temas incluidos en el security, tanto en la metodología de procedimientos detectores de los riesgos relacionados con la intervención delictiva de humanos, como son la identificación de indicios, señales, acciones, pautas de conducta, respuesta a ciertos estímulos de control, etc., como desde el punto de vista del buque como unidad independiente y autónoma para controlar su seguridad integral.

El planteamiento de contenidos se hace teniendo en cuenta los tres grandes bloques que intervienen en el proceso de la seguridad (security), como son:

- El buque, sus tipos, diseño estructural y tráficos
- El puerto como filtro de las amenazas que intentan acceder al buque
- Las personas de unos y otros, además de los delincuentes que quieren hacer el daño.

El buque es el gran desconocido, y de alguna manera todo gira en torno a él, desde el propio código PBIP, que tiene su implementación para hacerlo seguro frente a este nuevo sentir de la amenaza de elevado riesgo y consecuencias. El puerto tiene un papel importante como primer filtro que impida el acceso de personas y substancias, dañinas al buque el buque; aplica las suyas, que son razonablemente inferiores en magnitud y medios, y finalmente las personas involucradas que pueden frenar las acciones delictivas, pero se enfrentan a unas acciones poco conocidas y con poca preparación.

El resultado de ese cóctel es incierto por naturaleza, muchos intermediarios, muchas formas de pensar y de hacer, y si bien el código pretende subsanar la falta de sincronización de todos los estamentos e instituciones que se ven involucrados en la amenaza, el contenido y desarrollo formativo queda en unas trazas de color muy débiles y poco consistentes para representar un verdadero muro de medidas eficaces en la prevención y en la resolución de las situaciones aquí consideradas.

Objetivos

Hasta prácticamente el día de hoy, la actividad marítimo-portuaria tenía como objetivos prioritarios la mayor observancia de las normativas y requisitos para alcanzar un nivel de seguridad (safety) aceptable, mientras que a partir de ahora, la inclusión firme y demoledora de la parte de protección (security) coge al sector del transporte marítimo con escasos conocimientos y nulas referencias bibliográficas, que quedan recluidas en las fuentes de las fuerzas y cuerpos de seguridad y los de ámbito militar.

En la extensa bibliografía dedicada al safety todavía se incorporan nuevos criterios, puntos de vista, mejoras organizativas, procedimientos y metodologías, el campo del security, en cambio aplicado a una actividad civil como es el marítimo, está vacío de contenidos, solo se muestran ideas, voluntades y principios, sin desarrollos de cómo hacerlo, con qué, de qué manera, sin presentar los límites máximos y mínimos de eficacia y de riesgo en la sobre valoración de cualquier aspecto.

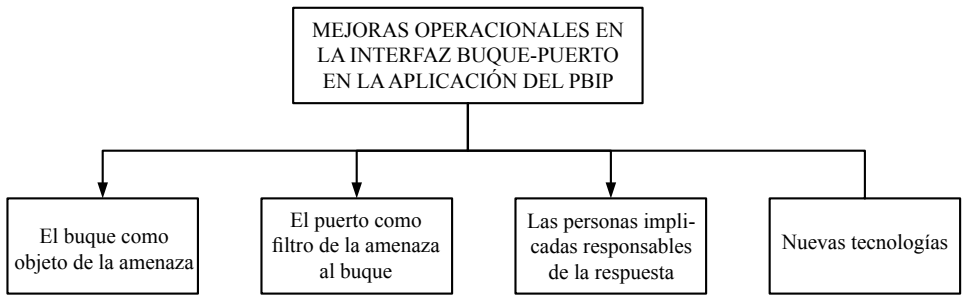
Es evidente, y por ello no es de extrañar, que en los próximos tiempos, deban surgir numerosas publicaciones, estudios, análisis, investigaciones y aportaciones de toda índole, en la nueva área de conocimientos que representa el security para su aplicación civil y por civiles, que en definitiva signifiquen una mejora de la prevención y protección de la vida ante actos extraños, ajenos a la actividad comercial, industrial y de servicios con la que se encuentra relacionada la actividad marítima.

El estudio persigue alcanzar los siguientes objetivos:

- ✓ Cubrir las lagunas operacionales en el control de situaciones de crisis por actos delictivos incluidos en el PBIP, tanto desde el buque como en la interfaz con el puerto.
- ✓ Mejorar el conocimiento de las acciones de control que pueden aplicarse en el amplio tema que está abarcado en la definición de protección (security).
- ✓ Detalle de los pormenores que producen, provocan y culminan una situación de protección en los buques y su relación con la seguridad portuaria en el transporte marítimo.

Desarrollo esquemático del estudio

La presentación y análisis de los distintos capítulos del trabajo será llevado a cabo conforme a los bloques descritos en el esquema 1.
Todas las partes, están estrechamente relacionadas entre sí en el denominador común de la figura del buque, para finalmente confluir en una línea de conclusiones.



Esquema 1

En su conjunto, cada uno de los bloques constituye un capítulo específico para tratar, en lo necesario y en la extensión que precise, las consideraciones, la identificación de las limitaciones y particularidades que condicionan los planes de emergencia en su aplicación en un buque determinado y en su interfaz.

Capítulo 1. El buque como objeto de la amenaza

1.1 Los medios organizativos

Los medios organizativos de un sistema de seguridad deben establecer los niveles de riesgo y la vulnerabilidad de la instalación a proteger. En el caso que nos atañe, la complejidad se acentúa al ser el entorno marítimo un espacio muy variado y cambiante, especialmente en la interfaz buque–puerto, ya que la variedad de buques y todas las diferentes acciones que pueden realizar en un puerto son enormes.

La valoración de los riesgos y de las vulnerabilidades es algo puntual, con procedimientos diferentes en cada caso. De esta forma, entendemos que el nivel puntual de riesgo de un "portacontenedores" cargando en el puerto de Algeciras con destino EE.UU. y el de un Crucero de pasaje atracando en el puerto de Barcelona procedente de un recorrido turístico por el Mediterráneo, con pasaje mayoritariamente americano, es muy diferente.

No obstante, los dos ejemplos citados anteriormente citados tienen un alto nivel de riesgo, pero los procedimientos empleados en su protección serán totalmente diferentes. Por supuesto, en caso de materializarse la amenaza, los procedimientos de reducción de pérdidas serán también muy diferentes.

Establecer un servicio de seguridad entorno a los diferentes procesos de estiva, de acceso a los buques de pasaje de vehículos, descarga de hidrocarburos, etc. requiere un estudio concreto con una planificación diaria de las tareas que el personal de seguridad desempeñará.

Mientras que la seguridad aeroportuaria permite una actividad plana de gestión, debido a que las variables son pasaje y carga, y además un tipo de carga muy "limpia", en un puerto esto no es así. Quien pretenda adaptar la experiencia de la seguridad aérea a la marítima fracasará estrepitosamente.

La seguridad marítima requiere soluciones que respetando la actividad, garanticen su seguridad adaptándose a las siguientes cuestiones básicas:

- El tipo de buque
- La carga
- El puerto clase y situación geográfica
- La operación a realizar, fondeo, atraque, recogida de pasaje, descarga de sustancias peligrosas, etc.
- Operaciones simultáneas en el tiempo y espacio con otros buques

1.2 Condicionantes relacionados con el buque

Dada la importancia que adquiere el buque, pues puede convertirse en arma, si se le da esa finalidad, o en vector de un arma de destrucción masiva, o en el medio de transporte inconsciente de una carga malévola, a menos que se tomen las medidas adecuadas en materia de protección marítima y control[1].

Así mismo, podemos establecer en la interfaz buque - puerto el punto de entrada de mercancías peligrosas en el país, como armas, explosivos, material radioactivo, etc. también de personas vinculadas a redes terroristas, inmigración ilegal, o delincuentes buscados por la policía que encuentran en la vía marítima la forma ideal de moverse entre países debido al actual bajo control ejercido.

Es necesario dedicar tiempo al estudio de la amenaza que representa el buque bajo el tratamiento y consideración aislada e independiente de su entorno, teniendo en cuenta la vulnerabilidad por tipo de buque, siguiendo el esquema nº 1.1 Esto nos dará una idea muy acertada del tipo riesgo que supone cada actividad portuaria con este tipo de buque, actividades que estableceremos y analizaremos más adelante.

Los contenidos enunciados permiten considerar cualquier planteamiento de protección que se pretenda implementar en un puerto, ya que pasa ineludiblemente por la consideración de la amenaza que representa el buque como objetivo directo o indirecto, principal o secundario, al tratar temas de orden público, delincuencia organizada, terrorismo, vandalismo, altercados, etc., porque de otro modo la acción delictiva podría ser aplicada indistintamente contra los diversos operadores terrestres de cualquier otra modalidad del transporte.

Considerar los aspectos del PPB que constituyen las medidas esenciales a partir de las cuales pueden determinarse los niveles de eficacia en términos de protección de un buque, tal como específicamente son detallados en el apartado 9.8 de la parte B del código[2]:

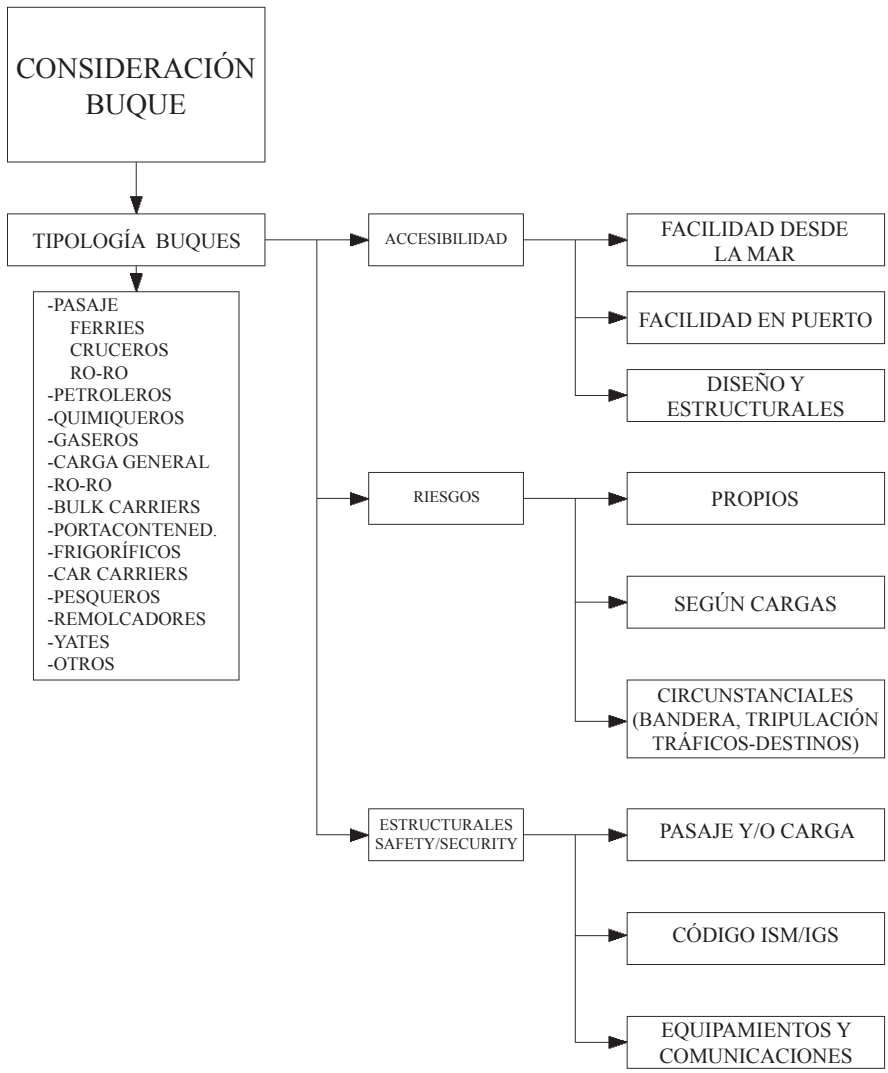
- ✓ Accesos
- ✓ Zonas restringidas
- ✓ Manipulación de la carga
- ✓ Entrega de provisiones
- ✓ Equipajes no acompañados, y
- ✓ Vigilancia de la protección del buque

Este esquema permite agruparlos según el grado de vulnerabilidad estructural (tipo de buque), operativa (tráficos) y grado de rigor de sus tripulaciones (especialidad), en las siguientes apreciaciones por bloque:

A. El buque de pasaje que en el esquema 1.1 incluye los buques ferries, cruceros y Ro-Ro, por el hecho de llevar personas a bordo distintas de las que forman la tripulación, en según que aspectos a considerar no podrán ser tratados por igual al existir marcadas diferencias entre los procedimientos y objetivos de cada tipo de transporte marítimo.

[1] Comunicado de la Comisión COM(2003)229 final, 2003/0089 (COD) para la propuesta de Reglamento del Parlamento Europeo y del Consejo, de mejora de la protección de los buques y las instalaciones portuarias. Bruselas, 2.5.2003

[2] Prácticamente obligatorias a nivel CE, bajo las prescripciones del reglamento, en el apartado 4.1.12 (Revisión de los planes de protección de los buques) del artículo 3.



Esquema 1.1

B. Los buques que habitualmente transportan cargamentos en tanques, como son los petroleros, quimiqueros y gaseros, constituirán un solo grupo de similares tratamientos y consideraciones.
C. Los buques de carga general, frigoríficos y bulkcarriers, también se agrupan en una categoría de planteamientos unificados.
D. Los buques Ro-Ro con transporte rodado sin chóferes ni pasaje, porta contenedores y car-carriers, forman un bloque de similar tratamiento.
E. Finalmente, los tipos de buques como pesqueros, remolcadores y embarcaciones de recreo serán considerados en un bloque de barcos de régimen portuario, con un tratamiento específico.

1.3 Buques del bloque "A"

Accesibilidad

En la mar y desde ella, la accesibilidad al ferry es difícil, dada la altura y la verticalidad de su obra muerta desde la línea de flotación. El acceso a través de las portas solo es posible si se efectúa desde el interior, y la apertura siempre se realiza en aguas resguardadas y con el buque parado.

El asalto desde la mar solo sería posible de existir una previa fuerza ocupante y de apoyo al abordaje en el interior del buque, de tal modo que el acceso a las cubiertas de intemperie se hiciera con el buque parado o a muy poca velocidad.

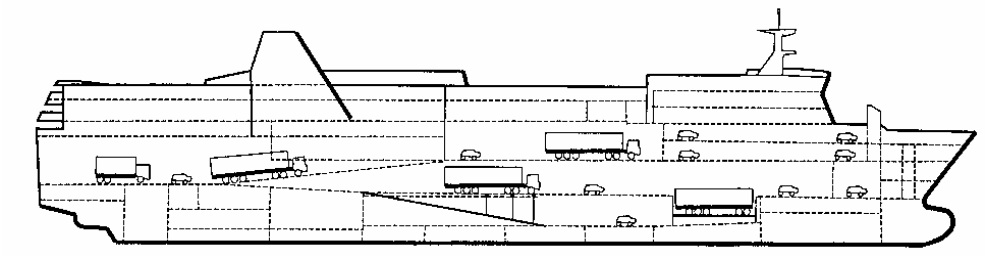


Fig. 1.1

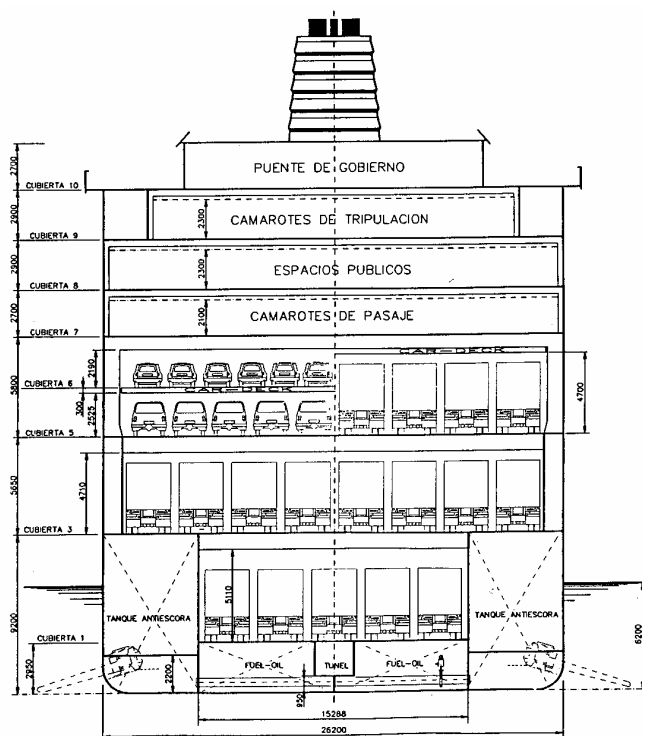


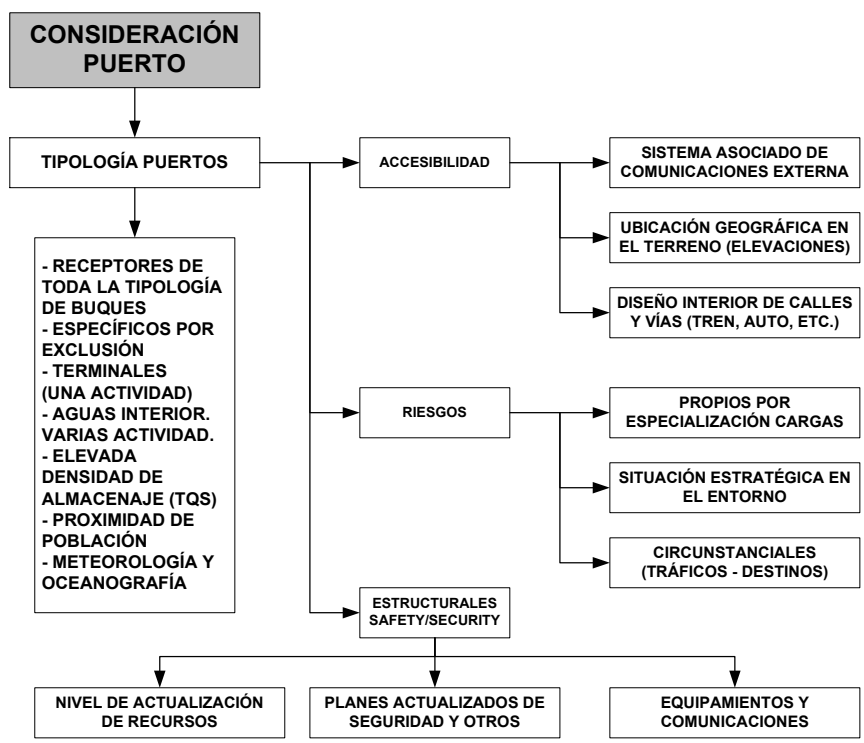
Fig. 1.2

Capítulo 2. El puerto como amenaza al buque

2.1 Condicionantes asociados al puerto

Los condicionantes asociados al puerto se desarrollan en el esquema 2.1, basado principalmente en la consideración de las variables, accesibilidad, riesgos y planteamientos estructurales.

Como la OMI no tiene la autoridad para decirles a los estados miembros cómo proteger sus puertos, creó el término *instalaciones portuarias* para referirse a las áreas donde recibe servicios de un buque que tiene la protección de la convención SOLAS.



Esquema 2.1

2.2 Filosofía y principios del control de accesos

Las instalaciones portuarias perdieron el control de accesos que antiguamente poseían como zona estratégica de una ciudad, al abrir sus puertas en la segunda mitad del siglo XX. De esta forma, las ciudades próximas encontraron un área de esparcimiento donde los ciudadanos podían pasear y realizar diferentes actividades lúdicas. La situación actual crea la necesidad de volver al estatus quo de zona estratégica que poseían. No obstante, en algunos casos la gestión del puerto permitirá establecer una zona de libre tránsito para no romper con la situación actual de forma traumática.

El principal factor diferenciador y multiplicador del riesgo en una instalación portuaria lo constituye la característica esencial de su actividad en términos de continuidad en el tiempo: 24 horas al día, 365 días al año. Por si esto fuera poco, establecer un perímetro seguro creando una burbuja protectora es prácticamente imposible con los medios técnicos actuales, eso sin contar con la falta de presupuesto, bastante común a la mayoría de los puertos. Esto nos lleva en muchas ocasiones a una falta de personal que desconoce en general los conceptos relacionados con la seguridad, una limitada utilización en términos de cantidad y calidad de sistemas de seguridad física y, por último, la escasez de los recursos dedicados a estos conceptos.

Si las instalaciones constituyen el sistema motriz del puerto, debe iniciarse su protección, al menos indirecta, desde el perímetro externo, donde se establece un área segura primaria antes del vallado o el control de acceso al puerto. De esta forma, se realizan sistemas de control activos tan pronto como sea posible sin que éstos afecten a las zonas de explotación; por ejemplo, a partir de las calles colindantes.

De lo anterior se deduce que los accesos constituyen puntos sensibles y deben ser reducidos en número al mínimo indispensable:

A. Acceso de pasajeros y acompañantes con o sin vehículo.
B. Entrada de vehículos transportando mercancías para su embarque.
C. Acceso de empleados del puerto, tripulaciones con permisos de tierra, mantenimiento o abastecimiento de buques.

En principio, es poco apropiado limitar cualquier tipo de acceso dentro de la zona dedicada al esparcimiento de los ciudadanos de la ciudad. Incluso potenciar esta área, a modo de las zonas de duty free de los aeropuertos, puede tener grandes beneficios, al no justificar en modo alguno la permanencia en las zonas de seguridad de personas ajenas a las mismas. Estas áreas de esparcimiento deben ser protegidas mediante controles aleatorios y vigilancia mediante CCTV.

Un tema muy diferente lo constituyen los accesos que comunican la zona de explotación (con la excepción de que resulten comunes en las vías de evacuación) con la zona de servicios. De cualquier forma, donde las medidas de seguridad deben ser extremadas al máximo es en el acceso a esas zonas en donde se encuentran las instalaciones vitales, y este control debe efectuarse a través de diferentes sistemas físicos de protección.

A partir de una configuración de una instalación portuaria determinada se presentan las siguientes necesidades mínimas a efectos de la obtención de una eficacia mínima en el control de los accesos a la misma:

1. Vallado perimetral de los servicios portuarios a partir del punto donde sea posible realizarlo con objetividad, con plena evaluación de las alternativas que puedan ser aplicadas en cuanto a la naturaleza física y material de dicha valla.
2. Establecimiento de las zonas restringidas en la instalación para acceso al buque, bien sea considerado por concesión, línea de atraque, tráfico de mercancías especializado, o bien por cualquier otra consideración relacionada con el riesgo y la vulnerabilidad de cada zona relacionada con buques.

El primer punto está condicionado por la configuración superficial del dominio público, la proximidad de los límites exteriores a las zonas operativas del puerto con los buques, las que vengan determinadas por la población a la que posiblemente se vea inmediatamente relacionada (fagotizada) y por la disponibilidad actual de los accesos a la instalación portuaria.

El vallado debe marcar e indicar claramente la línea de responsabilidades, y a su vez establecer condicionantes de paso, y en especial su relación objetiva con la interfaz buque-puerto. En la Figura 2.1, correspondería a "P".

En la figura 2.1, se esquematiza una configuración portuaria para el control de accesos, donde se representan:

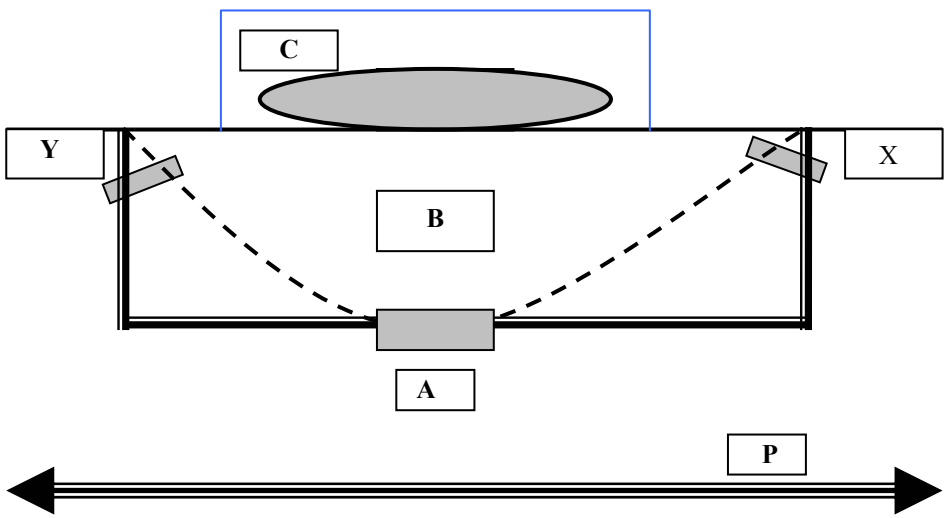


Fig. 2.1

Por su parte, el segundo punto constituye el objetivo fundamental de este estudio, ya que, independientemente de la existencia o no del vallado exterior, definitorio de la propia instalación portuaria, el control de la protección solo será posible si queda bien definido el anillo principal de seguridad donde puedan implementarse medidas de filtro y disuasorias.

a. A partir de una línea de atraque donde el buque se encuentre amarrado con seguridad, debe existir una zona restringida de accesos y salidas que envuelva en tierra la eslora del buque con la suficiente holgura para abarcar la explanada de operaciones y movimientos internos, así como los puntos de amarre (norays) al que el buque se encuentre sujeto.

Capítulo 3. Amenazas y riesgos del buque

3.1 El buque como receptor de las amenazas

Conforme a los contenidos de las tablas de análisis de los apartados anteriores, el buque como amenaza indirecta sobre el puerto deberá sufrir inicialmente las primeras consecuencias para pasar a ser objetivo, medio y objeto de la agresión ilícita que se está perpretando contra las instalaciones portuarias, al utilizar el buque para introducirse en ellas.

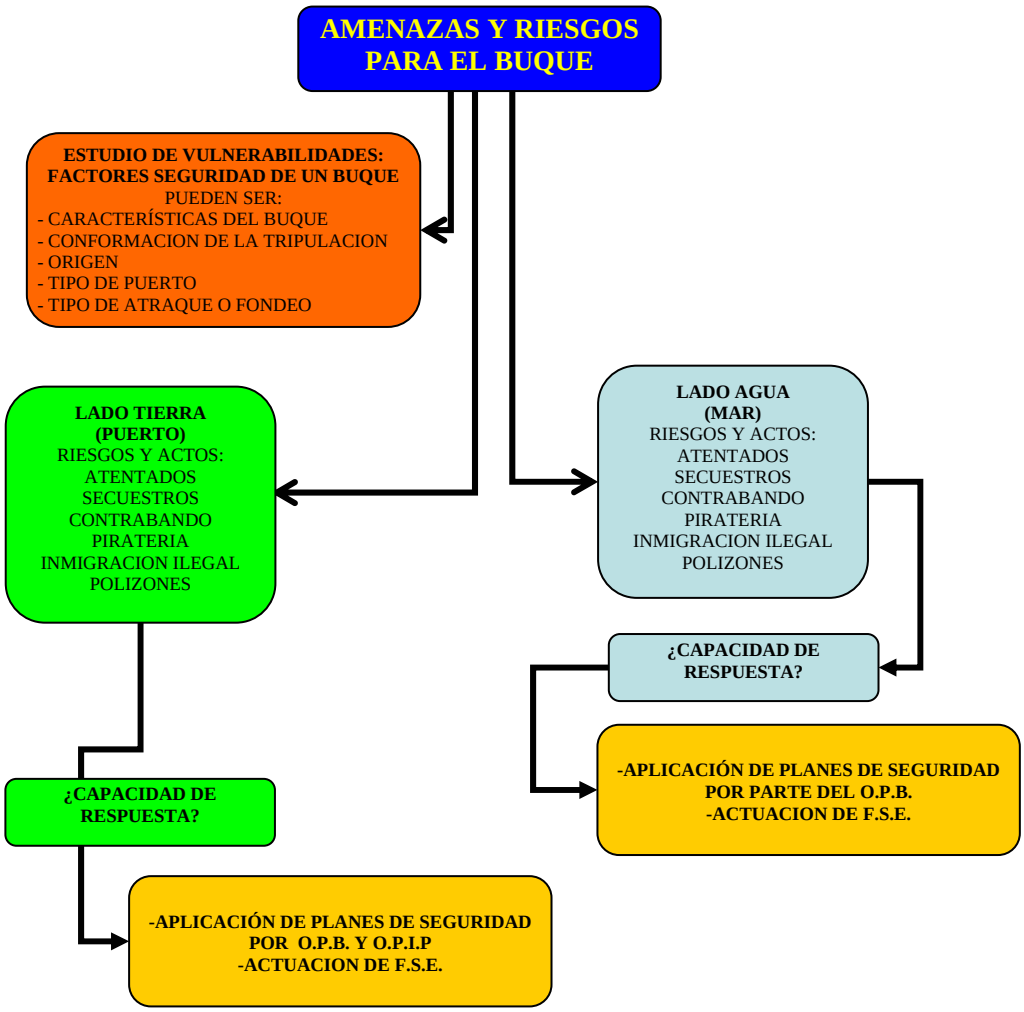
En el esquema 3.1 se encuentran referenciados los aspectos y variables que van a condicionar al buque.

En esta etapa, el buque adquiere un papel fundamental en la seguridad global del sistema portuario, debiendo regirse por el plan de protección del buque (PPB) las ayudas externas que pueda recibir de las fuerzas de seguridad del Estado (FSE) y el apoyo logístico que pueda proporcionarle el puerto.

No obstante, el buque no puede quedar solo a expensas de sus posibilidades de protección en unas aguas que no le son conocidas, ni tan siquiera amigables, ya que de todos es conocido que siempre constituirá el punto débil de toda la seguridad global que quiera implementarse en la actividad marítima portuaria, puesto que es el elemento menos controlable, aún siendo cada día mayor el número y la eficacia (SIA, Control de Tráfico, etc.) de los medios que se están implementando a bordo.

La expresión *solo a expensas* viene a significar el apoyo que en todo momento pueda y deba recibir desde tierra, y el puerto así debe admitirlo, ya que su mayor interés se basa en que el buque no padezca problemas ni en sus aguas ni en sus instalaciones. Por un lado, se debe impermeabilizar el puerto y por otro haciendo más seguros los buques que vaya a recibir.

Tal como se analizará en el capítulo de protección del puerto, la adopción de medidas preventivas, disuasorias y de control sobre la amenaza que representa el buque sobre el puerto solo serán eficaces si parten de un buen conocimiento de los riesgos intrínsecos que cada tipo de los mismos significa en la cadena de la protección, siendo más eficaz en la medida que se ajuste a la realidad de cada buque, a la evaluación de las probabilidades y a la naturaleza de las circunstancias y condiciones en que se produce la relación entre ellos.



Esquema 3.1

Mientras tanto, una vez consumados los actos delictivos en el buque y a partir de dicho momento, éste pasa a ser el último eslabón antes de que los objetivos finales sobre el puerto puedan darse lugar.

En el esquema 3.2, continuación del esquema anterior, se distinguen las consecuencias, así como la determinación de responsables afectados en la toma de decisiones.

Se observa que el peso de la responsabilidad recae prácticamente en el puerto, a través de sus planes de protección de instalaciones (PPIP) y su plan de protección del puerto (PPP), ya que conocida o advertida la posibilidad de que la amenaza sea real, la aplicación de los correspondientes niveles de

protección se desencadenan de forma lógica, independientemente del nivel de garantías que pueda ofrecer el plan de protección del buque (PPB).

Si el PPB es bueno y desde el buque se ha hecho todo lo humanamente posible para impedir que el buque sea el objeto del delito, la amenaza habrá sido ralentizada en la medida de lo posible y existirán fundadas esperanzas que ambos esfuerzos (puerto y buque) obtengan un resultado positivo en la operativa de la protección o representen una reducción de las consecuencias finales.

Mientras tanto, una vez consumados los actos delictivos en el buque y a partir de dicho momento, éste pasa a ser el último eslabón antes de que los objetivos finales sobre el puerto puedan darse lugar.

En el esquema 3.2, continuación del esquema anterior, se distinguen las consecuencias, así como la determinación de responsables afectados en la toma de decisiones.

Se observa que el peso de la responsabilidad recae prácticamente en el puerto, a través de sus planes de protección de instalaciones (PPIP) y su plan de protección del puerto (PPP), ya que conocida o advertida la posibilidad de que la amenaza sea real, la aplicación de los correspondientes niveles de protección se desencadenan de forma lógica, independientemente del nivel de garantías que pueda ofrecer el plan de protección del buque (PPB).

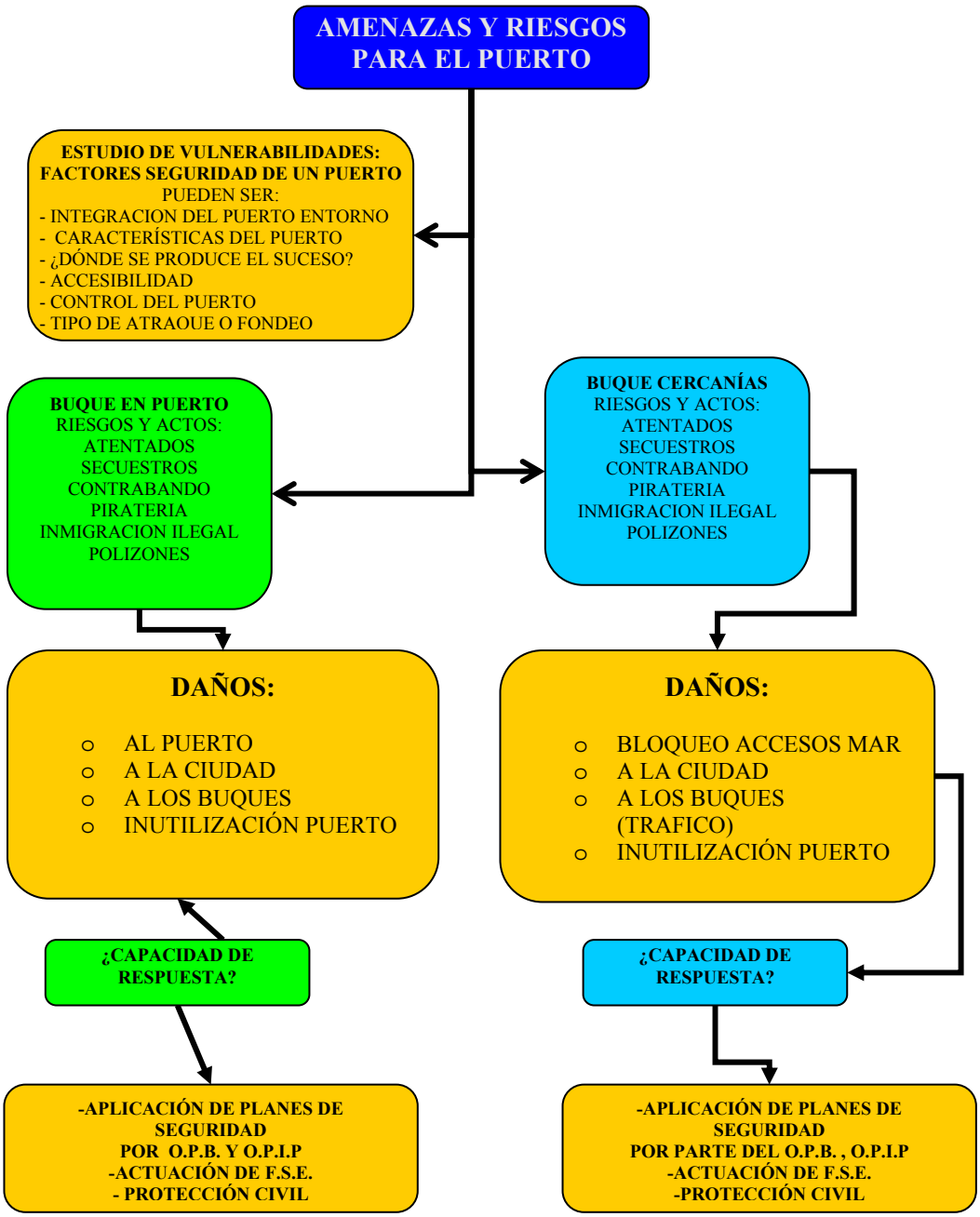
Si el PPB es bueno y desde el buque se ha hecho todo lo humanamente posible para impedir que el buque sea el objeto del delito, la amenaza habrá sido ralentizada en la medida de lo posible y existirán fundadas esperanzas que ambos esfuerzos (puerto y buque) obtengan un resultado positivo en la operativa de la protección o representen una reducción de las consecuencias finales.

Conocidas la vulnerabilidad del buque y las consecuencias previsibles que puede ocasionar a las instalaciones portuarias, el PPIP deberá considerarlas en la medida equilibrada que cubran las necesidades de protección.

Otro factor a tener en cuenta son los sistemas de control de la carga de los buques. Los principios de eficacia establecen que nada se quede sin mirar y nada se mire dos veces. Es por esta razón que la inspección de buques que tienen un origen seguro no debería ser necesaria. Es más, establecer orígenes seguros es lo que permitirá al tráfico marítimo no paralizarse, teniendo en cuenta que hará innecesarias las inspecciones exhaustivas de buques en las zonas de fondeo, acción mucho más complicada que la inspección de la carga en el puerto.

3.2 Controles de protección en contenedores de carga

En la mayoría de los casos, el problema será exterior a la interfaz buque-puerto y por tanto más relacionado con el PPP que con el PPIP. No obstante, conocida la intermodalidad del transporte y la elevada influencia de los contenedores como iniciadores de un incidente en la protección, se considera necesario aportar criterios y alternativas de mejora en el control y en su identificación.


AMENAZAS Y RIESGOS PARA EL PUERTO
ESTUDIO DE VULNERABILIDADES: FACTORES SEGURIDAD DE UN PUERTO
PUEDEN SER:
- INTEGRACION DEL PUERTO ENTORNO
- CARACTERÍSTICAS DEL PUERTO
- ¿DÓNDE SE PRODUCE EL SUCESO?
- ACCESIBILIDAD
- CONTROL DEL PUERTO
- TIPO DE ATRAOUE O FONDEO
BUQUE EN PUERTO
RIESGOS Y ACTOS:
ATENTADOS
SECUESTROS
CONTRABANDO
PIRATERIA
INMIGRACION ILEGAL
POLIZONES
BUQUE CERCANÍAS
RIESGOS Y ACTOS:
ATENTADOS
SECUESTROS
CONTRABANDO
PIRATERIA
INMIGRACION ILEGAL
POLIZONES
DAÑOS:
AL PUERTO
A LA CIUDAD
A LOS BUQUES
INUTILIZACIÓN PUERTO
DAÑOS:
BLOQUEO ACCESOS MAR
A LA CIUDAD
A LOS BUQUES (TRAFICO)
INUTILIZACIÓN PUERTO
¿CAPACIDAD DE RESPUESTA?
¿CAPACIDAD DE RESPUESTA?
-APLICACIÓN DE PLANES DE SEGURIDAD
POR O.P.B. Y O.P.I.P
-ACTUACIÓN DE F.S.E.
- PROTECCIÓN CIVIL
-APLICACIÓN DE PLANES DE SEGURIDAD
POR PARTE DEL O.P.B. , O.P.I.P
-ACTUACIÓN DE F.S.E.
-PROTECCIÓN CIVIL

Esquema 3.2

Capítulo 4. Mejoras en la transferencia de mercancías

4.1 Introducción

La escalada de acciones terroristas así como de otra tipología de delitos asociados a la actividad del mar (contrabando, piratería, sabotaje, abordajes, inmigración ilegal,.etc.) ha hecho que la Asamblea Internacional de la I.M.O., llevada a cabo en noviembre de 2001, decidiera por unanimidad la adopción de nuevas medidas en materia de seguridad de las instalaciones portuarias y de los buques, que debían ser adoptadas por los países firmantes del convenio SOLAS 1974 a partir de la decisión en firme sellada en diciembre de 2002. En ella se fijaban nuevas prebendas respecto al SOLAS 1974, así como la implantación del código PBIP.

Estos nuevos requisitos sirvieron de fundamento para la nueva estructura internacional, en la cual buques e instalaciones portuarias debían cooperar para la detección y neutralización de riesgos que pudieran amenazar la seguridad del sector del transporte marítimo.

Teniendo en cuenta que en la actualidad la totalidad de las instalaciones portuarias de primera categoría de los países que adoptaron el SOLAS 1974 tienen un sistema de transporte multimodal (al menos cuatro de los siguientes: tráfico aéreo, autopista, ferroviario, red vial pública, tubería y marítimo) y que un incremento de la seguridad supone indefectiblemente un ascenso de los costes (tal y como se ha reflejado en la aplicación tras los sucesos del 11 de septiembre de 2001 de los nuevos procedimientos de seguridad en el transporte aéreo), se deben adoptar medidas encaminadas a optimizar la relación coste-beneficio y que sean de fácil adaptación a este sistema multimodal para que ese incremento en seguridad beneficie las actividades marítimas en la reducción de las acciones delictivas asociadas a esta actividad.

Con la aparición de los actuales sistemas intermodales de transporte, que se encuentran integrados dentro de las infraestructuras portuarias, se crea una problemática de permeabilidad. Todo procedimiento de traslado de un modo de transporte a otro exige una comprobación del proceso para evitar riesgos durante la manipulación. Si se han cumplido debidamente los preceptos marcados en la descarga y carga de las mercancías, se tiene un nivel de seguridad sensiblemente bueno. A pesar de ello, y para recibir o trasladar la mercancía de/a cualquier otro modo de transporte, se realizarán de nuevo comprobaciones de los listados de mercancía. Siempre que sea posible, la mercancía estará lo menos dispuesta a granel como sea posible. El empleo de continentes aumenta la seguridad en su manipulación, aunque dificulta su revisión mediante procedimientos no electrónicos, y sin violar los precintos de seguridad.

Del mismo modo deben ser medidas que acepten una implantación en un breve periodo de tiempo, sin que ello incremente los costos. La implementación de los procesos requiere de la cooperación efectiva entre todos los elementos relacionados con la actividad, tales como usuarios, navieras, astilleros,

autoridades portuarias, cuerpos y fuerzas de seguridad del Estado, personal embarcado, personal del lado tierra, pasajeros, gestores y todo aquel que en uno u otro modo intervenga en actividades que confluyan con procesos de seguridad marítima. De ese modo, se establecen responsabilidades que deben de ser adquiridas obligatoriamente por parte de empresas del sector de modo que se integren dentro de los planes comunes de seguridad, tal y como marca el PBIP.

Los procesos ya en uso deben de pasar por un proceso de estudio y revisión, sustituyendo o actualizando aquellos que no aporten el nivel de seguridad requerido.

El objeto del presente documento es, dentro de la implantación de PBIP en las instalaciones de las autoridades portuarias de puertos del Estado, la presentación de procedimientos y la propuesta de sistemas que mejoren el actual nivel de seguridad existente en la transferencia de mercancías entre las instalaciones portuarias y los buques, entendiendo dentro de los procedimientos realizados en las instalaciones portuarias incluso la receptación de mercancías del exterior.

Entre ellos se presentan protocolos de actuación en chequeos de documentación, reconocimiento de sospechosos, control de contenidos de contenedores, aseguramiento de la identidad de los propietarios de los fletes, transparencia en la identidad de las empresas navieras, creación de registros de empresas autorizadas y la identificación de los medios de transporte mediante un código IMO (que igualmente deberían ir pintados en las bandas de los buques), bases de datos para garantizar la trazabilidad del buque, sistemas de identificación automática, mejoras e implementación de sistemas antipánico en los buques para una rápida alerta a los equipos de primera intervención, reducción de los tiempos de estancia con la optimización de los procesos de estiba y desestiba.

Para ello se desglosarán los procedimientos de entrada de mercancía al puerto entre los de lado tierra y los de lado mar, aplicando en cada caso los procedimientos específicos.

Se trata, pues, de potenciar, en los distintos controles de accesos (tomando la inspección del buque incluso como uno de ellos) la detección de sospechosos y la implantación de procesos de mejora en la identificación de personal y mercancías; no tanto de la detección de elementos peligrosos en las mercancías, que pasarían a un segundo nivel de prioridad.

4.2 Registros de empresas autorizadas dentro de las IP

Uno de los puntos críticos en la seguridad portuaria es la existencia de prestaciones de distintos servicios por empresas externas a la autoridad portuaria y sobre las que salvo el cumplimiento de los contratos específicos con cada una de ellas y de la ley en materia de seguridad laboral, no se aplicaban procedimientos de captación de formación o de control de sus operaciones, en concreto las del personal que desarrolla los servicios contratados.

En materia de seguridad aeroportuaria se ha demostrado en numerosas ocasiones que el principal riesgo procede del personal interno de gestión y de contrata.

Es por ello que encaminado a mejorar los sistemas de control e información del personal en las actuaciones portuarias (estiba y desestiba, operaciones marítimas, aprovisionamientos, transportes

Capítulo 5. Procedimientos tecnificados a la identificación

5.1 Fundamentos de la autenticación biométrica

La autentificación biométrica (AB) consiste en la verificación de la identidad de un individuo, tomando como parámetros de identificación ciertos elementos morfológicos animales, y por tanto humanos, y con una mínima probabilidad de repetición de un individuo a otro, de modo que prácticamente se puede decir que sólo se dan en ese sujeto.

A través de la AB nos proponemos tomar información acerca de un rasgo distintivo de una persona (su voz, su huella dactilar, su iris, su retina, olor ...) para más tarde comparar ese registro introducido en una base de datos con otro tomado en el momento de querer realizar la identificación, y poder averiguar si se trata del mismo individuo. Del mismo modo, los animales reconocen a otros animales, incluidos los seres humanos, por características biométricas tales como el olor o la voz.

La dificultad de la AB estriba en el desarrollo de la tecnología que pueda realizar esas identificaciones, de modo que lo hagan de forma rápida y libre de errores. Igual que ocurre con otras capacidades humanas, tales como el lenguaje, dotar a las máquinas de la capacidad de llevar a cabo la AB con efectividad se ha revelado como una tarea muy compleja.

Funcionamiento de la AB

El parámetro determinante es la elección de los rasgos distintivos que identifican sin lugar a error a cada persona. Aunque la autenticación de usuarios mediante métodos biométricos es posible utilizando cualquier característica única y mesurable del individuo (esto incluye desde la forma de teclear ante un ordenador hasta los patrones de ciertas venas, pasando por el olor corporal), hace décadas que se acepta comúnmente que rasgos como la huella digital, el iris del ojo o la voz son únicos para cada persona y completamente válidos para la automatización de la AB.

Otros rasgos menos conocidos comúnmente o que implican mayores dificultades para las máquinas son el sistema venoso de la retina, los rasgos de la cara o la forma de la mano.

Lo óptimo para un sistema de AB es focalizar aquellos rasgos que, además de ser distintos en cada persona, no sufren variaciones a lo largo del tiempo por causas como el proceso natural de envejecimiento o los cambios en la masa corporal. De este modo, los tres primeros rasgos (huella digital, iris y voz) son los que aglutinan la mayor parte de los esfuerzos investigadores actuales.

Tras decidir qué rasgo va a utilizarse en el proceso de autentificación, para lo cual es importante ver la actividad o sector al que va destinado el sistema en cuestión, es necesario buscar los parámetros

cuantificables y/o caracterizables. De ese modo, se sabe que todas las huellas digitales humanas tienen una serie de puntos (intersecciones, extremos de líneas, etc.) distribuidos de distintas formas en cada persona. Al comparar por tanto dos huellas digitales, no se compara la totalidad de la huella, sino únicamente la situación de esos puntos y sus posiciones relativas.

El análisis de los patrones formados por esos puntos constituye en sí el proceso de autentificación biométrico.

En esta línea, existen ya aplicaciones comerciales de la AB en forma de lectores de huellas digitales incorporados a ordenadores portátiles que sustituyen o complementan la tradicional protección por contraseña. Controles de huellas o de iris se están usando también en sistemas de control de acceso a instalaciones. Los lectores de huellas o los reconocedores de voz pueden, a medio plazo, sustituir a los PIN de nuestros teléfonos móviles o a las llaves de nuestros coches.

No obstante, la AB por sí sola no puede resolver todas las necesidades de autentificación y seguridad, sino que hemos de considerarla una herramienta más dentro de nuestro repertorio, y en el caso concreto de los controles de accesos para mercancías que lleguen a puerto por tráfico rodado, la combinación idónea será con las técnicas de detección de sospechosos. Un sistema de AB puede ser el refuerzo perfecto para presionar a un individuo y para aumentar la seguridad en las credenciales individuales de identificación del personal portuario. De hecho, no solo serviría dentro del ámbito del control de accesos de mercancías, sino que de cara a mejorar la protección de datos en los equipos de oficina, un sistema de reconocimiento de huella dactilar podría sustituir a los clásicos lectores de tarjeta tanto para el control de fichajes como en los distintos equipos informáticos de la empresa, que podrían ser dotados también de reconocedores de huellas dactilares, de tal forma que sólo los usuarios autorizados puedan utilizar cada equipo.

Del mismo modo, estos sistemas instalados en los ordenadores portátiles pueden el acceso a la información sensible de la empresa de robo o extravío. De esta forma, la empresa tiene la absoluta certeza de que sólo su personal accede a sus instalaciones maneja su información y, además, de que los fichajes se realizan de forma correcta.

Si la empresa dispone de una infraestructura de clave pública (PKI) para asegurar la confidencialidad de sus comunicaciones, la AB puede jugar un papel importante a la hora de incrementar los niveles de confianza en dos de las características más importantes de la PKI: la irrefutabilidad y la confidencialidad. Es decir, cuando un empleado vaya a enviar un mensaje firmado y cifrado digitalmente, utilizará su lector de huellas digitales para autorizar la firma del mensaje. Cuando el destinatario reciba el mensaje y trate de descifrarlo, habrá de proporcionar también su autentificación por medio del sistema AB. Así, ambos pueden estar seguros de que el mensaje ha sido emitido por quien dice haberlo emitido y, además, sólo su destinatario podrá leerlo. Si la firma digital es el código OMI de empleado, cuya creación se recomienda en este documento, así como el código OMI de emergencias, utilizable en caso de secuestro, se autenticaría el código con un parámetro biométrico o dos.

Todas estas operaciones basadas en la AB eliminan dos elementos que hasta ahora han sido claves en todos los sistemas de seguridad informáticos: contraseñas y tarjetas.

La AB erradica, pues, toda la problemática derivada del extravío o robo de tarjetas de identificación o de la utilización de contraseñas simples o fáciles de averiguar o robar e incluso de olvidar. Tienen la

ventaja de que los patrones no pueden perderse o ser sustraídos, ni pueden ser usados por otros individuos en el caso de que lleguen a tener acceso a nuestra tarjeta personal y/o PIN.

A diferencia de los antiguos sistemas, en los que había que portar algo, los sistemas de biometría hacen que los parámetros de identificación ya vayan "incorporados" en el individuo. Se aumenta así a niveles muy altos la seguridad informática en la empresa, al mismo tiempo que se facilitan muchas operaciones diarias.

Estos sistemas pueden aumentar la cadencia de flujo de los controles de accesos.

Al igual que se están realizando estudios previos a la creación de un DNI digital basado en AB, se estima que sería optimo su empleo para la creación de la mencionada credencial de identificación de trabajador de empresa autorizada.

De hecho, en la actualidad se encuentra en fase de ultimación un proyecto a gran escala para la emisión en Suiza de casi 100.000 pasaportes biométricos cada año, entre 2005 y 2010. Para pasar la frontera de los E.E.U.U. sin visa, a partir del 26 de octubre del 2005, el personal que quiera hacerlo deberá estar dotado de un pasaporte con lectura óptica (2003). Es decir, de un nuevo pasaporte con datos biométricos. El antiguo pasaporte (1985) comenzará a quedar fuera de uso desde el 26 de octubre del presente año.

Los norteamericanos han fijado, además, otra exigencia. Para aprovechar el programa de entrada sin visa, los países firmantes del convenio deberán al menos trabajar seriamente en la preparación de un pasaporte que contenga dichos datos biométricos. Se estima que esa exigencia va seguramente a imponerse a escala internacional y especialmente en la Unión Europea. El nuevo pasaporte, al igual que la credencial propuesta, llevará una pastilla electrónica con contenidos biométricos. Hay que precisar que el pasaporte actual (2003), que puede ser controlado por lectura óptica, seguirá siendo expedido, si bien se empezarán a hacer los registros de sus datos biométricos en una de las oficinas repartidas en el país (Tabla 5.1).

La validez de la credencial o del pasaporte deberá igualmente reducirse de 10 a 5 años, por razones relacionadas con la duración de vida técnica de la pastilla electrónica.

Los dispositivos biométricos tienen tres partes principales; por un lado, disponen de un mecanismo automático que lee y captura una imagen digital o analógica de la característica a analizar. Además disponen de una entidad para manejar aspectos como la compresión, almacenamiento o comparación de los datos capturados con los guardados en una base de datos (que son considerados válidos), y también ofrecen una interfaz para las aplicaciones que los utilizan.

El proceso general de autenticación sigue unos pasos comunes a todos los modelos de autenticación biométrica: *captura* o lectura de los datos que el usuario a validar presenta, *extracción* de ciertas características de la muestra (por ejemplo, las minucias de una huella dactilar), *comparación* de tales características con las guardadas en una base de datos, y *decisión* de si el usuario es válido o no. Es en esta decisión donde principalmente entran en juego las dos características básicas de la fiabilidad de todo sistema biométrico (en general, de todo sistema de autenticación): las tasas de falso rechazo y de falsa aceptación.

Por tasa de *falso rechazo* (*False Rejection Rate*, FRR) se entiende la probabilidad de que el sistema de autenticación rechace a un usuario legítimo porque no es capaz de identificarlo correctamente, y por

Capítulo 6. Control de personas y cosas

6.1 Control de pasajeros y revisión de equipajes

Elaboración de lista de pasajeros, cotejando los datos del billete con D.N.I. o pasaporte. El empleado de la compañía completará los datos adjuntos para proceder a etiquetar el equipaje del pasajero antes de su revisión (tabla 6.1).

La revisión del equipaje se realizará en zona oculta en presencia del pasajero. Estas revisiones serán aleatorias siguiendo las indicaciones del personal de control del área común de la terminal de pasajeros que mediante las técnicas anteriormente expuestas de detección de sospechosos marcarán los pasajeros que deben ser controlados.

Debido a la peculiaridad del transporte marítimo, los procedimientos seguidos en la aviación civil carecen de eficacia, ya que es muy frecuente el embarque de pasajeros que portan bultos muy voluminosos y gran número de maletas que por su tamaño dificultan la revisión automática. Esto obliga a tener que habilitar una línea de revisión paralela que ejecute la inspección de forma manual.

La velocidad de inspección dependerá de la especialización del personal de seguridad y de los medios técnicos disponibles.

Cuestionario para la aceptación de pasajeros

Nº 0000	**CONTROL DE PASAJEROS (DATOS DEL BUQUE)**	FECHA: 00/00/00
		OBSERVACIONES
NOMBRE		
1º APELLIDO		
2º APELLIDO		
SEXO		
EDAD		
NACIONALIDAD		
Nº D.N.I. / PASAPORTE		

EQUIPAJE	ETIQUETADO DE SEGURIDAD	OBSERVACIONES
1º	Nº XXXXXX/YYYY	Descripción
2º		
3º		
4º		
5º		

Tabla 6.1

6.2 Zona de control de billetes y revisión de equipajes

Una vez entregada la tarjeta de embarque, todo el equipaje de pasajero procederá a entrar en la zona de preembarque por el control de acceso siguiendo los protocolos de seguridad oportunos. Una vez dentro de la zona segura, le será entregado su equipaje (fig. 6.1).

El refuerzo de las medias de seguridad de los niveles 2 y 3 estarán marcadas por la revisión sistemática de todo el equipaje, incluso se procederá a la entrega en destino del mismo en las travesías inferiores a 4 horas.

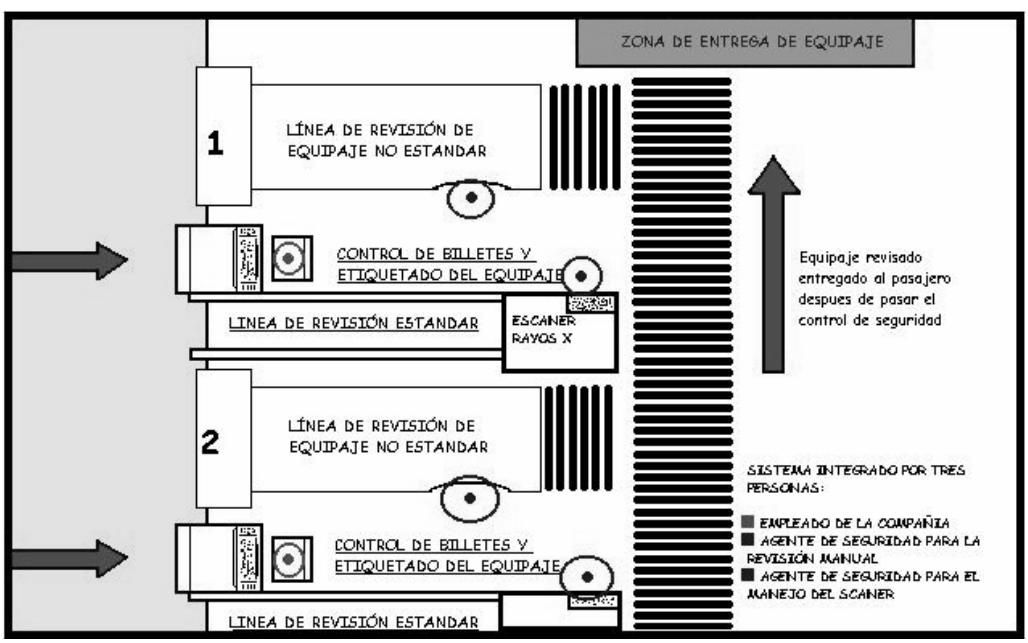


Fig. 6.1

Capítulo 7 Respuesta humana a situaciones del *security*

7.1 Conducta humana bajo presión

Aun afectando a todas las personas y tipo de buques, debe considerarse como especiales a los buques de pasaje, al cumplir un objetivo muy diferente a cualquier otro tipo de barco. En él existe una concentración de personas que desean ser atendidas y que en su gran mayoría desconocen el medio. Por otro lado, la tripulación se ve afectada por la necesidad de añadir, a las responsabilidades propias de la navegación, todas aquellas tareas propias de los servicios que demanda el pasaje. Al comportamiento de tripulación y pasaje debe añadirse el de posibles agresores, fuerzas de segunda intervención y familiares de todas las personas implicadas en una posible crisis a bordo.

El tema debe tratar la conducta humana, no solamente bajo presión, sino también en rutina.

El desencadenante de muchas de las situaciones críticas que se viven a bordo tiene origen en la falta de prevención, al ignorar que las personas implicadas en estos actos están sometidas a altos niveles de stress. Este hecho facilita la detección de los agresores y permite prevenir conductas en la tripulación que pueda desencadenar acciones negativas.

La complejidad del comportamiento humano exige rigor en la exposición de sus múltiples dificultades tratada según los aspectos básicos de la conducta individual y de la colectiva, se consideran que el *comportamiento* es toda aquella actuación de una persona que tiene unas consecuencias, tanto para él mismo como para otras personas o entorno físico. La base de esta actuación tiene muchos condicionantes o factores psicológicas, ambientales, sociales, biológicos, de aprendizaje, perceptivos, cognitivos, etc., es decir, es un fenómeno único pero con múltiples causalidades.

7.2 Conducta individual

El conocimiento del comportamiento de las personas individualmente permitirá conocer los mecanismos que obran en el comportamiento de la masa en situaciones de crisis. El comportamiento espontáneo no existe, ya que cada una de las acciones posee un desencadenante que de alguna forma obliga a la persona a responder estableciendo una cadena de acción–reacción. Y es esta misma cadena y sus consecuencias lo que modifica la conducta de las personas en sus relaciones, así como en el medio. En el caso de una situación de emergencia, diferentes personas reaccionarán de distintas maneras. Este comportamiento puede tener un resultado adaptado a la situación o completamente erróneo.

La experiencia enseña que en la mayoría de eventos críticos, se dan numerosas reacciones individuales que salvan la situación cuando todos los sistemas de intervención previstos fracasan. ¿Qué tuvieron en común las personas que sobrevivieron a situaciones de crisis?

Ante cualquier situación en la que aparece una amenaza sobre una persona, y ésta puede sufrir un daño, sea éste del tipo que sea, se está ante una situación de presión. Es una situación que produce un determinado nivel de stress.

Muchos factores intervienen en el resultado al lidiar con el stress producido por la situación de crisis y además variará mucho de una persona a otra. Pero existen una serie de parámetros que son comunes a todas las personas.

Estos parámetros configuran una gráfica que sirve para valorar las situaciones críticas y el comportamiento de las personas involucradas.

Por un lado, el tiempo que va transcurriendo segundo a segundo y que puede ser un percusor de stress si no cumple con la tarea requerida en el plazo establecido.

Existen situaciones en las que el tiempo no es un factor importante, otras veces es el factor decisivo.

Otro factor que marca la escala en relación al tiempo es el nivel de actividad de la persona sometida al evento crítico. Este nivel de actividad consta de varias zonas que muestran el nivel de stress soportado, así como los niveles normales de actividad y la línea de desastre (Fig. 7.1)

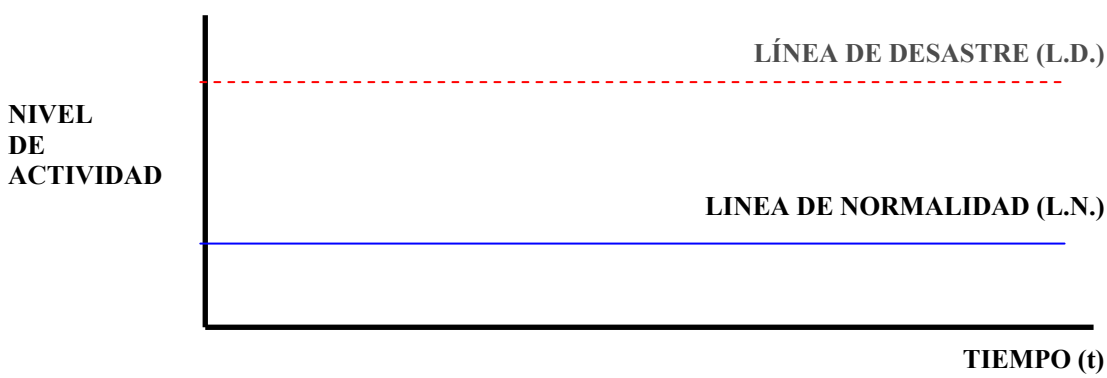


Fig. 7.1

El nivel de desastre se alcanza en lo cotidiano en todos los órdenes de la vida, suceden cosas extraordinarias a las que no se encuentra una explicación lógica, pero el análisis en la perspectiva del tiempo permite objetivizar el suceso.

Las situaciones que generan presión son muy variadas y, como se ha dicho anteriormente, configuran gráficas muy diferentes. Por ejemplo:

a) Presión de tiempo

El tiempo establece una prioridad en la resolución de la crisis. Esto rompe el equilibrio disparando los niveles de stress, en función de los requerimientos de la tarea a ejecutar, la imposibilidad de

cumplirlos en el tiempo marcado y siendo mayor el nivel de desequilibrio cuanto mayor sea la pérdida que sufrirá la persona. Existen muchos tipos de presión, pero éstas son las más habituales.

b) Presión social (éxito-miedo al fracaso)

El tiempo no marca de una forma especial la resolución de estas crisis. El nivel de presión viene determinada por el entorno y la pérdida de apoyos familiares, sociales, etc. El nivel de presión es acumulativo y la línea de desastre se alcanza cuando la persona se colapsa, principalmente por conflictos de rol.

c) Presión interna acumulada (frustración)

El stress generado por la frustración es acumulativo y requiere de un tiempo más o menos largo para saturar las capacidades resolutivas de la persona y precipitarla a la línea de desastre.

d) Presión por miedo físico

La presión por miedo físico establece una necesidad de resolver la situación en el mínimo tiempo posible. Esto, unido a que lo que se encuentra expuesto es la integridad física, genera un pico de stress muy alto enviando a la persona a las inmediaciones de la línea de desastre y rebasándola en muchas ocasiones.

7.3 Reacciones de shock y de pánico

La presión por miedo físico es la más útil para el control del orden público y el posterior conocimiento de acciones grupales y de masa. La posible reacción de todas las personas es la misma. No existe ningún ser humano que no cumpla este principio, tan sólo hay diferencias entre unos y otros en la intensidad de las reacciones. Bajo presión, la reacción oscila entre el shock y el pánico (Fig. 7.2).

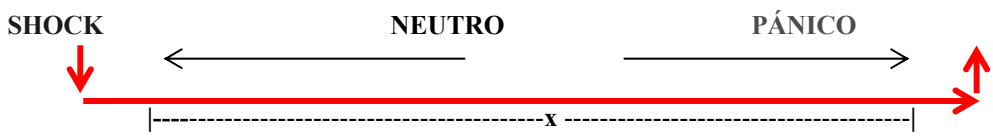


Fig. 7.2

El shock se caracteriza por lentitud de movimientos o ausencia de los mismos, sudoración fría, lividez, silencio, posturas cerradas de barrera y protección incluso fetales. El canal de comunicación de salida se encuentre cerrado no así el de entrada (Fig. 7.3).

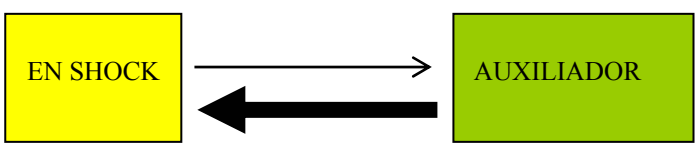


Fig. 7.3

El pánico es lo contrario al shock; la persona muestra hiperactividad, sudoración caliente, rubor en el rostro, alaridos y tono de voz elevada, posturas abiertas. El canal de comunicación de salida está abierto, pero tan saturado que bloquea el canal de entrada (Fig. 7.4).

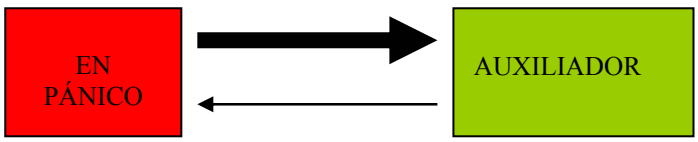


Fig. 7.4

Por lo tanto, no se puede determinar que todo el mundo pasa por un periodo de shock más o menos duradero, para luego entrar en una fase de Pánico más o menos profunda.

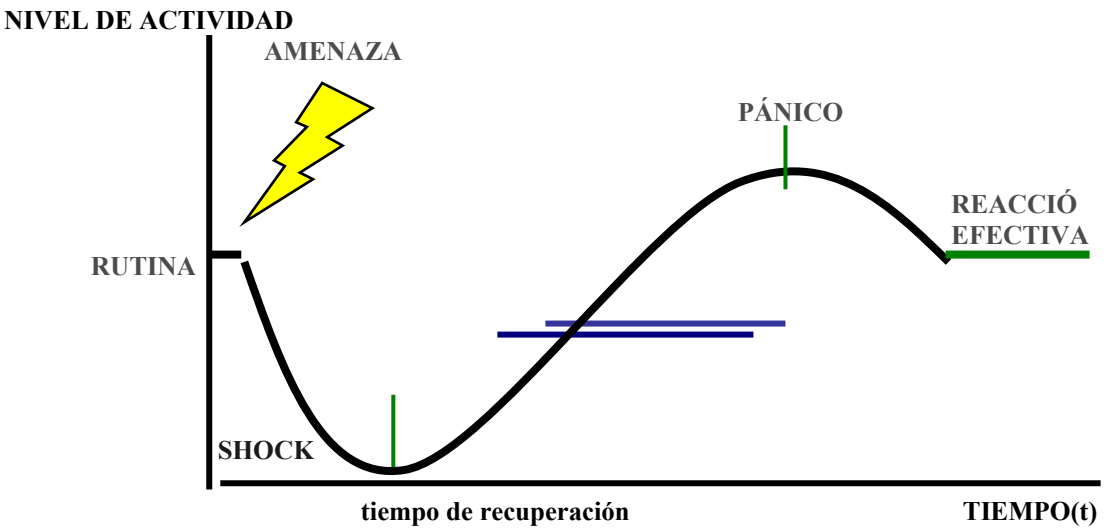


Fig. 7.5

Más tarde se llega a la reacción efectiva, que es lo que se pretende, ya que solamente esta fase es la que puede generar la acción que solucione la crisis (figura 7.5).

El tiempo que transcurre desde la amenaza hasta la reacción efectiva se denomina tiempo de recuperación. Este es el tiempo que debemos acortar para conseguir aumentar nuestras posibilidades de sobrevivir. Entre los métodos para lograr este propósito están los ejercicios de simulación, que pretenden generar las experiencias y el conocimiento necesario para superar las situaciones límite a las que nos enfrentamos en una crisis.

En la reacción efectiva, a la que se le concede tanta importancia, se crean las acciones que evitan la amenaza y hacen que el alcance de los daños sean aceptables, necesitándose que las acciones sean ejecutadas en el tiempo, intensidad y lugar adecuados.