Artículo de Investigación. Revista Ciencia e Ingeniería. Vol. 35, No. 2, pp. 85-94, abril-julio, 2014.
ISSN 1316-7081. ISSN Elect. 2244-8780 Universidad de los Andes (ULA)

Revisión del estado del arte de la evaluación de riesgos en instalaciones portuarias

Review of the state of the art of risks assessment in port facilities

Romero Faz, David *[1] y Camarero Orive, Alberto [2]
[1] Dpto. Ingeniería Civil: Infraestructura del Transporte. Universidad Politécnica de Madrid. 28014. Madrid-España
[2] Dpto. Ingeniería Civil: Transportes. Universidad Politécnica de Madrid. 28040. Madrid-España
*david.romero@upm.es

Resumen

La evaluación de la seguridad en puertos comerciales es un tema de plena actualidad, si bien se sigue investigando la mejor manera de valorar el riesgo existente en una instalación frente a posibles ataques terroristas. En este sentidola Organización Marítima Internacional (OMI) en el año 2001, tras el ataque a las Torres Gemelas de Nueva York, amplió su concepto de la seguridad, incluyendo desde entonces la seguridad física, tanto de instalaciones portuarias como de buques. Estos cambios en el concepto de la seguridad fueron incorporados a partir de 2001 mediante la Resolución A.924 en la que se apela a un término más global, la "Protección Marítima", como parte de las enmiendas realizadas a los capítulos V y XI del Convenio Internacional de Seguridad para la Vida Humana en el Mar (SOLAS), incorporándolas al nuevo Código sobre Protección de Buques e Instalaciones Portuarias (ISPS). Así pues, la OMI creó un grupo de trabajo con el fin de desarrollar una metodología específica para la evaluación de riesgos en instalaciones portuaria, denominada Matriz de Análisis de Amenaza y Riesgo MAAR. Algunos países como España o EEUU han realizado su propia metodología acorde con sus necesidades e idiosincrasias. El presente artículo analiza el estado del arte de las principales o más extendidas metodologías de evaluación de riesgos en instalaciones, comparando las aportaciones de cada una frente a la propuesta por la OMI.

Palabras Claves: Riesgos, gestión, puerto, instalaciones, amenaza, daño**.**

Abstract

The assessment of security at commercial port is a current issue, although much remains to be learned especially in defining the best way to properly assess the risk on facilities against possible terrorist attacks. In this sense, the scope of interest and therefore work of IMO had always been the vessel, and not the port issues, but in 2001, after the attack on the twin towers in New York occurred a change of mind moving towards a broader concept of security, including physical security in the same standards both of port facilities and vessels. These changes in the concept of security were incorporated from 2001 through the resolution A.924 in which it appeals to a broader term, "maritime protection", as part of the amendments to chapters V and XI of the International Convention of human in the sea life safety (SOLAS), incorporating the new code about protection of ships and port facilities (ISPS) operational security in port activity concerns traditionally they covered the prevention or combat illegal such as trafficking in arms, narcotic drugs and, in general, smuggling of all kinds of goods. Thus pue, the International Maritime Organization (IMO) created a working group to develop a specific methodology for the evaluation of risks in port facilities, called MAAR. Some countries like Spain or the US carried out its own methodology in accordance with their needs and idiosyncrasies. This article analyzes the state of the art of main or most common methodologies for risk assessment at port facilities by comparing the contributions of each one against the original from IMO.

Key words: Risk, management, port, facilities, threat, damage.

1 Introducción

Los autores han realizado una revisión del estado del arte respecto de la evaluación de riesgos para la protección en instalaciones portuarias en base a la metodología descrita en origen por la Organización Marítima Internacional (OMI) y a las desarrolladas por en países como España, EEUU, y otros (Comisión de las Comunidades Europeas, 2003).

La evaluación de la protección en instalaciones portuarias fue promovida por la Organización Marítima Internacional (OMI), a partir de 2003 mediante una metodología propia aplicable a todos los países pertenecientes a la OMI, y por tanto con infraestructuras portuarias, si bien, como luego se verá, algunos países como España o Estados Unidos, han creado su propia metodología en paralelo, basada, en algún caso en las directrices marcadas por la OMI (Organización de las Naciones Unidas, 2006).

2 Desarrollo del trabajo

Para la evaluación se han analizado las diferentes metodologías propuestas por la OMI y las variantes a la misma desarrolladas por países en los que su seguridad nacional puede verse amenazada y que por tanto a su juicio, juega un papel importante en sus puertos y por tanto en la garantía de protección de sus instalaciones y sus ciudadanos.

La evaluación de la seguridad o protección es fundamentalmente un análisis de riesgos de todos los aspectos relacionados con las operaciones y elementos asociados a una instalación, para determinar así que elemento o elementos de estas son más susceptibles y/o tienen más probabilidades de sufrir un incidente ante la acción de agentes internos/externos.

Se puede definir el riesgo como la medida de la pérdida económica y/o daños para la vida humana, resultante de la combinación entre la frecuencia del suceso y la magnitud de las pérdidas o daños (consecuencias) en un plazo de tiempo (Cabeza y Cabrita, 2007).

$$R=f\,(f,c) \qquad (1)$$

2.1 MAAR. Organización Internacional del Trabajo (OIT) y Organización Marítima Internacional (OMI), 2003

Hasta el año 2003 solo existían los planes de seguridad que cada puerto aplicaba a su manera y sin criterios unificados internacionalmente, si bien con elementos de juicio comunes. La Conferencia de Gobiernos Contratantes del Convenio Internacional para la Seguridad de la Vida Humana en el Mar, 1974 (SOLAS Conferencia, Londres, 9-13 de diciembre de 2002), aprobó las enmiendas a la Convención Internacional para la Seguridad de la Vida Humana en el Mar (SOLAS), 1974. La seguridad general de las zonas portuarias se dejó para un trabajo conjunto posterior entre la Organización Internacional del Trabajo (OIT) y la Organización Marítima Internacional (OMI). Un grupo de trabajo conjunto de la OMI / OIT desarrolló en julio de 2003 un documento donde se describe la finalidad de las medidas de protección, los niveles de protección, los contenidos de la evaluación de la protección portuaria, etc. Asimismo, en él se propone un modelo para la evaluación de riesgos que deberá ser la base de las diferentes metodologías a desarrollar posteriormente por cada país. El modelo es del tipo simplificado, y propone una definición de los conceptos de riesgo, amenaza, vulnerabilidad e impacto, asignándoles unos valores cuantitativos preestablecidos de forma cualitativa, creando con estos conceptos una matriz denominada "matriz de análisis de amenaza y riesgo", MAAR.

Su propósito es identificar las amenazas con el fin de adoptar y recomendar medidas para detectar, detener, y reducir las consecuencias de cualquier incidente potencial, que pueda producirse.

El objetivo del código de buenas prácticas es comparar y evaluar las medidas de seguridad que reduzcan, de manera independiente, la vulnerabilidad o el impacto y por ende, la puntuación total del riesgo (OMI-IMO, 2004). Hay que tener en cuenta que la introducción de una medida de seguridad respecto de una amenaza puede aumentar el riesgo de otro.

El riesgo viene determinado por la ecuación:

$$\text{Riesgo} = \text{Amenaza} \times \text{Vulnerabilidad} \times \text{Impacto} \qquad (2)$$

El procedimiento que se debe seguir para la determinación de los diferentes riesgos en las instalaciones portuarias es el siguiente. En primer lugar se debe generar una tabla separada para cada objetivo potencial, identificando a través de funciones y operaciones, zonas vulnerables, puntos clave o personas en el puerto y en el entorno inmediato que pueden, actuando ilegalmente, incidir negativamente sobre la seguridad, la seguridad del personal o la actividad de la terminal. Asimismo se debe identificar la "propiedad" del objetivo; operador, Autoridad Portuaria, etc. Se debe establecer si existen medidas de seguridad existentes, tales como un cerco perimetral, control de acceso y/o patrullas de vigilancia objetivo potencial. Si es así, ¿son efectivas, o son las mejores?

Situación de amenaza Se deben considerar la posibilidad de supuestos de amenazas internas y externas a las que el objetivo identificado pueden ser vulnerables (la información por parte de la policía, de seguridad y los servicios de inteligencia es esencial).

Tabla 1. Matriz de amenaza y riesgo

Escenario nº	Escenario de Amenaza	Amenaza	Vulnerabilidad	Impacto	Total	Acción prioritaria
A	B	C	D	E	F	G
1 2						

Amenaza. La probabilidad de un suceso ocurrido debe evaluarse con la siguiente escala: Seguridad en los puertos; 3 = Alto; 2 = Medio; 1 = Bajo. La asignación de la puntuación de la amenaza puede estar basada en información específica obtenida o debido a características conocidas del objetivo potencial.

Vulnerabilidad. La vulnerabilidad del objetivo para cada amenaza puede evaluarse de la siguiente manera;4 = No existen medidas de seguridad o las existentes no son eficaces (p.e.: el acceso sin restricciones a los destinatarios);3 = medidas de seguridad mínimas (por ejemplo, las zonas restringidas no claramente identificados, procedimientos inadecuados de control de acceso, vigilancia esporádica; ningún programa de capacitación en seguridad formal, objetivo susceptible a determinados tipos de daños);2 = medidas de seguridad satisfactorias (p.e: zonas restringidas claramente identificadas y acceso controlado; programa de seguridad de capacitación formal, la vigilancia adecuada y el conocimiento amenaza; destino no muy vulnerable); 1 = medidas de seguridad plenamente eficaces (p.e: ser: capaz de pasar rápidamente a un nivel de protección superior si es necesario; objetivo difícil de dañar).

Impacto. Evaluar el impacto (o consecuencias) de cada incidente potencial que se produzca sobre el objetivo y en la terminal, caso de producirse. Se puede evaluar de la siguiente manera: 5 = Perjudicial para la seguridad y vigilancia (probabilidad de causar la pérdida de vidas, lesiones graves y/o crear un peligro general para la salud pública y la seguridad);4 = Perjudicial para la seguridad pública y/o la imagen del país (que puedan causar daños ambientales significativos y / o de salud pública localizada y de seguridad);3 = Perjudicial para el medio ambiente y/o para la función económica del puerto (Probabilidad de que todo el puerto se vea sometido a interrupción continuada de su actividad y/o pérdidas económicas importantes y/o daños a la imagen del país.);2 = Perjudicial para los bienes, la infraestructura de servicios públicos y la seguridad de la carga (Probabilidad de una interrupción temporal de un determinado bien, infraestructura u organización); 1 = Perjudicial para la confianza de los clientes o de la comunidad portuaria.

Puntuación del Riesgo. El resultado de los efectos será: riesgo = amenaza x vulnerabilidad x impacto. En la evaluación de escenarios probables, la historia y el modus operandi de los grupos ilegales más probable que operan en el área deben ser considerados al determinar los objetivos, y determinar y evaluar las medidas de seguridad más adecuadas.

2.2 RBDM. Navigation and Vessel Inspection.Servicio de Guarda Costas (EEUU), 2003

En 2003 Estados Unidos diseñó su propia metodología de aplicación sobre la base de los preceptos del Código ISPS, mediante el Título 33 del Código de Regulaciones Federales (CFR), Partes 101 a 107, y de la Circular N° 11-02 (NVIC 11-02) "Navigation and VesselInspection", 2003, del Servicio de Guarda Costas de los EEUU.

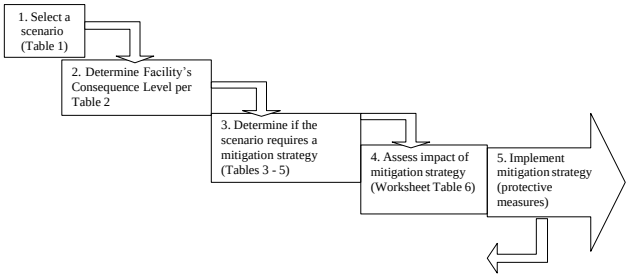

Fig. 1. Diagrama de flujo de la evaluación de la seguridad basada en el riesgo

Risk-based decision-making, RBDM, es un proceso sistemático y analítico para considerar la probabilidad de que una violación de la seguridad ponga en peligro un activo, individuo o función e identificar las acciones que reducirán la vulnerabilidad y mitigarán las consecuencias. Las evaluaciones pueden identificar vulnerabilidades en las operaciones de una Instalación, seguridad del personal y seguridad física y técnica (Servicio Guardacostas EE.UU. 2003).

Identificación de posibles amenazas

Una vez identificados los activos que pueden ser objeto de sabotaje o actos terroristas, se identifican las posibles amenazas existentes asociadas a las instalaciones en estudio y de forma implícita a las operaciones que en una terminal se efectúen. Asimismo se debe identificar en qué modo se podrían producir dichos ataques con el fin último de valorar la vulnerabilidad de las infraestructuras descritas anteriormente. Una vez definidas las amenazas se estará en condiciones de establecer las convenientes medidas de protección. Para evaluar de forma completa las posibles amenazas es necesario establecer una serie de escenarios de ataque posibles cuyo resultado sea una amenaza potencial para la seguridad de la instalación.

Estimación del nivel de consecuencia

Una vez definidos los escenarios posibles y por tanto las amenazas probables para una terminal se estima el nivel de consecuencia que tendrá la instalación en función de la actividad que en ella se desarrolla; valor 3 para instalaciones que transfieran, almacenen o manipule mercancías peligrosas, valor 2 para instalaciones que reciben buques certificados para más de 150 pasajeros o que operan buques que realiza viajes internacionales, y valor 1 instalaciones distintas de las anteriores.

Estimación de la vulnerabilidad de la terminal

La vulnerabilidad de una instalación portuaria se determina en base a los posibles ataques que pueda sufrir la misma, así como las estrategias de protección a instrumentar, adoptándose las medidas adecuadas para su instrumentación y de esa forma reducir la vulnerabilidad de la instalación portuaria. La evaluación de la vulnerabilidad se efectuará de forma cuantitativa para cada escenario descrito, y en base a cuatro criterios; disponibilidad, accesibilidad, seguridad orgánica y dificultad del objetivo. La evaluación

se debe realizar para cada bien e infraestructura a proteger, y éste a su vez en cada escenario estudiado. La ponderación de la vulnerabilidad será; 3 para instalaciones sin disuasión en accesos y con sistemas de seguridad sin capacidad de disuasión, 2 para instalaciones con regular disuasión en accesos y con regulares sistemas de seguridad disuasorios, 1 para instalaciones con buena disuasión en accesos y con buenos sistemas de seguridad disuasorios.

Matriz de Vulnerabilidad y Consecuencia

Antes de determinar que escenarios deben contar con medidas correctoras. Para ello se crea la matriz de la tabla 2 que a continuación se presenta y que recoge la suma de los indicadores evaluados de consecuencia y vulnerabilidad para cada amenaza o escenario planteado previamente.

Tabla 2. Matriz de Vulnerabilidad y Consecuencia

		Puntuación total de Vulnerabilidad		
		2	**3-4**	**5-6**
Nivel de consecuencia	**3**	Considerar	Corregir	Corregir
	2	Documentar	Considerar	Corregir
	1	Documentar	Documentar	Considerar

De esta manera se definen tres situaciones posibles en el estudio y consideración del riesgo: Corregir: se deben desarrollar medidas correctoras, tales como medidas protectoras de seguridad, para reducir el riesgo del escenario. Considerar: se deben desarrollar medidas correctoras caso a caso. Documentar: significa que el escenario puede no necesitar una medida correctora y por lo tanto sólo necesita ser documentado.

Determinación de escenarios que requieren medidas de protección

Para determinar qué escenarios requieren medidas de mitigación, se emplea la Tabla 3.

Tabla 3. Tabla para determinación de escenarios con medidas correctoras

Nº	**Escenario**	**Nivel de Consecuencia**	**Vulnerabilidad**			**Acción**
			Accesibilidad (a)	**Seguridad Orgánica (b)**	**Total (a+b)**	
1						
2						
3						

Por otra parte, la mayoría de los países hispanoamericanos, cuyo tráfico de mercancías marítimo hacia Estados Unidos es elevado, o cuya influencia económica por parte de éste en relevante sobre aquel, han asumido, de forma general, su metodología de análisis de riesgo con el fin de facilitar el movimiento de las mercancías hacia el mismo.

2.3 CARVER (Criticality, Accessibility, Recoverability, Vulnerability, Effect on Population, Recognizability). Ejército de los EE.UU.

La metodología CARVER es un método de análisis que se centra en la evaluación del riesgo de objetivos específicos dentro de las instalaciones.

CARVER fue desarrollada originalmente por el ejército de EE.UU. para identificar áreas dentro de las infraestructuras clave, civiles o militares, que pudieran ser vulnerables a un ataque de las Fuerzas Especiales de EE.UU

Se trata de un método de análisis muy potente si se utiliza junto con buena información sobre la amenaza, y se puede utilizar para subrayar las fortalezas y debilidades en la seguridad, especialmente en infraestructuras (Masse, 2007).

CARVER define seis factores para la evaluación en cada sitio o punto dentro de una instalación, ocupa estos seis factores en una escala de 1 (bajo) a 10 (más alto) y proporciona un rango lista ordenada de los puntos fuertes y débiles. El concepto de CARVER es aplicar un número objetivo de un presupuesto algo subjetivo. Esto proporciona un sistema para establecer el peso relativo de cada elemento entre cualquier número de sitios. Es importante reconocer las limitaciones de los sistemas como éste, y utilizarlos en consecuencia. Los elementos específicos de análisis CARVER son:

Criticidad: es la importancia de un sistema, subsistema o elemento. Un objetivo es crítico cuando su destrucción o daño tiene un impacto significativo en el funcionamiento del sistema, subsistema o elemento y, al más alto nivel, en la capacidad de la amenaza de realizar o mantener los ataques. También se basa en el impacto que sobre la opinión pública tendría un ataque terrorista y la percepción que de este ataque tendría la sociedad.

La criticidad depende de varios factores:

- Tiempo. ¿Con que rapidez afecta el impacto de la destrucción del objetivo a las operaciones?
- Cantidad. ¿Qué porcentaje de la producción se ve afectado por la destrucción del objetivo?
- La existencia de un relevo para la salida del producto o servicio.
- El número de objetivos y su posición en el sistema o diagrama de flujo del elemento

Accesibilidad: es la facilidad con que puede ser un objetivo alcanzado, ya sea físicamente o mediante enfrentamiento con fuego. Un objetivo es accesible cuando un elemento terrorista puede infiltrarse en el objetivo, o si el objetivo puede ser alcanzado por métodos directos o indirectos. La accesibilidad varía con la infiltración, la supervivencia y el escape potencial de la zona de destino, la situación de seguridad en ruta y en el objetivo, y la necesidad de la penetración de la barrera en éste. El uso de armas como los vehículos bomba siempre debe tenerse en cuenta al evaluar la accesibilidad. La supervivencia del terrorista o atacante no siempre se correlaciona con la accesibilidad de un

objetivo.

Recuperación del funcionamiento y la propiedad: es una medida del tiempo requerido para remplazar, reparar o evitar la destrucción o el daño infligido al objetivo, y varía en función de las fuentes y las edades de los componentes seleccionados, y con piezas de repuesto o capacidades redundantes.

Vulnerabilidad: es una medida de la capacidad de los terroristas para dañar el objetivo con los activos disponibles (tanto a las personas como a los bienes materiales).

Un objetivo es vulnerable si el terrorista tiene los medios y conocimientos para que el ataque tenga éxito. La vulnerabilidad depende de:

- La naturaleza y construcción del objetivo,
- La cantidad de daño necesaria / deseada;
- Los activos disponibles:
- Mano de Obra, experiencia y mentalidad;
- Transporte, armas, explosivos y equipos

Efecto sobre la población: se define como la influencia positiva o negativa sobre la población como resultado de las medidas adoptadas. El efecto no solo considera la reacción del público en las cercanías del objetivo, sino que también considera la reacción nacional e internacional de este.

Objetivos reconocibles: intenta valorar el grado en que un objetivo se puede reconocer sin confusión con otros objetivos o elementos. Los factores que influyen en él incluyen el tamaño y la complejidad del objetivo, la existencia de marcas distintivas, la sofisticación técnica y la capacitación de los atacantes.

Los objetivos fácilmente reconocibles servirán siempre mejor a los propósitos de un terrorista. Los objetivos serán reconocibles con diferentes condiciones climatológicas, y no serán confundidos por el agresor con otros elementos similares pero de menor importancia.

El Método CARVER ha sistematizado el modo de evaluar las amenazas de una acción terrorista o criminal, en forma de una serie de parámetros o indicadores, que se consideran los más idóneos para la medición de los factores de riesgo frente a este tipo de actos, así como la vulnerabilidad de las instalaciones.

El sistema de calificación usado en los análisis CARVER para medir el grado de amenaza y vulnerabilidad se efectúa mediante el empleo de los seis elementos explicitados anteriormente y consiste en la valoración numérica de la trascendencia de cada uno de ellos con la siguiente asignación:

- Nivel grave de trascendencia: 5
- Nivel alto de trascendencia: 4
- Nivel considerable de trascendencia: 3
- Nivel general de trascendencia: 2
- Nivel bajo de trascendencia: 1

La amenaza compuesta se calcula mediante la suma de las puntuaciones o calificaciones para las seis categorías del análisis CARVER, de modo que el mayor nivel o calificación de amenaza es, por tanto, de treinta. (Otros sistemas diferentes desarrollados en la actualidad establecen baremos de valoración distintos, tomando en consideración un número menor de factores o multiplicando la valoración de cada uno de ellos para obtener un índice representativo, con lo cual se obtienen otros indicadores distintos, lo que conceptualmente no modifica el método).

Adicionalmente, se puede considerar un séptimo factor o categoría directamente ligado al denominado "Efectos", que se denomina Shock. Contempla aspectos psicológicos, ligados a la acción terrorista y pretende medir las sinergias generadas por la suma de destrucción real de infraestructuras y el ánimo de la población.

El Método CARVER necesita a su vez ser complementado con otros procedimientos de valoración habituales en los análisis de Riesgos, tales como la evaluación de las Probabilidades o Frecuencia de Presentación y la determinación de las Consecuencias del ataque terrorista, de manera que se puedan evaluar los Riesgos de cada uno de los supuestos analizados.

De una manera simplificada, puede concluirse que el Método incorpora a los elementos convencionales de un Análisis de Riesgos (probabilidad y consecuencia), un tercer bloque formado por seis o siete factores que cuantifican de un modo más preciso las amenazas terroristas y la vulnerabilidad de la instalación, que es una buena aproximación al requerimiento del Código Internacional para la Protección de los Buques y las Instalaciones Portuarias PBIP.

Las actividades para la evaluación de riesgos que contemplan los factores descritos anteriormente serán los siguientes, bien entendido que este "diagrama de flujo" es genérico y no específico para escenarios concretos:

- Caracterización del sistema
- Identificación y valoración de la amenaza
- Identificación y valoración de la vulnerabilidad
- Determinación de los parámetros de control
- Establecimiento de probabilidades
- Análisis de impacto
- Determinación de riesgos
- Recomendaciones para controles de seguridad
- Documentación de los resultados y elevación del pertinente informe a la organización competente

2.4 RAM (Risk Assessment Methodology).Sandia National Laboratories. (EEUU)

Los Laboratorios Nacionales Sandia (EEUU) redefinieron una metodología de evaluación del riesgo para evaluar el riesgo en varios tipos de infraestructuras de los EE.UU, incluidas instalaciones portuarias. La metodología se basa en la ecuación de riesgo tradicional:

$$Riesgo = PA * (1 - PE) * C \quad (3)$$

Siendo:

PA	la probabilidad de un ataque
PE	la efectividad de los sistemas de seguridad
1 – PE	probabilidad de éxito del ataque o de fallo de los sistemas de seguridad
C	es la consecuencia de la perdida ante un ataque.

La metodología consta de siete etapas, que a continuación se describen y que se muestran debidamente en la correspondiente figura 2 mediante un diagrama de flujo:

1. Caracterización de las instalaciones

El primer paso es la caracterización de los sistemas de seguridad y su estado de funcionamiento y condiciones, para ello se requiere el desarrollo de una descripción detallada de la instalación en sí; límites de la instalación, la ubicación de edificaciones, puntos de acceso, etc.

2. Los eventos no deseados

Identificación de activos críticos. Eventos no deseados: los eventos no deseados deben ser definidos. Serán el resultado de consecuencias no deseadas. Son específicos y tienen efectos adversos para la salud pública y la seguridad, el medio ambiente, los activos, etc. Activos Críticos: el enemigo puede provocar que cada evento no deseado se produzca de varias maneras distintas, por ello es necesario un enfoque estructurado para identificar los componentes críticos para la prevención de eventos no deseados. La aplicación de un modelo lógico, como por ejemplo un árbol de fallas, se puede emplear para identificar los componentes críticos.

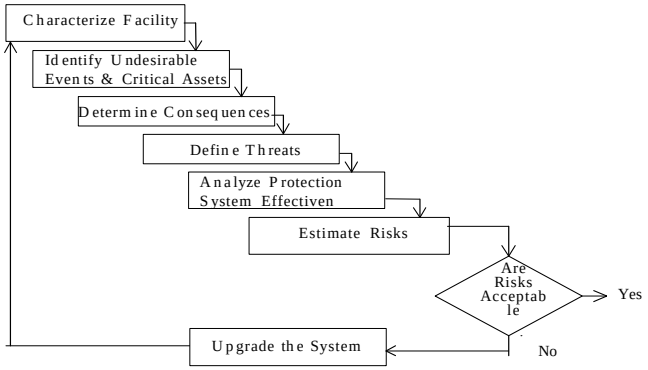

Fig. 2. Análisis metodológico

3. Determinación de las Consecuencias

Los componentes críticos y su ubicación se convierten así en el activo fundamental a proteger.

Tabla 4. Categoría de las consecuencias y valores asociados

Categoría de la Consecuencia	Valor de la Consecuencia
Catastrófica- daños con resultado de muerte(s), perdida de la misión o daño ambiental	Muy alta
Crítica- daños con lesiones graves o enfermedad, pérdida de la misión prinipal o daños ambientales importantes	Alta
Marginal-resultan en lesiones o enfermedad leves, pérdida de la misión en menor medida, o daño ambiental menor	Media
Insignificante-los resultado inferior a lesiones leves o enfermedad, inferior a la pérdida misión, o menos que el daño ambiental mínimo	Baja

4. Definición de amenaza

Es necesaria una descripción de la amenaza, esta descripción incluye el tipo de enemigo, tácticas y capacidades, información sobre la amenaza para estimar la probabilidad de que se puede intentar llevar a cabo los eventos o situaciones no deseadas. El tipo específico de amenaza a una instalación que se conoce como la amenaza base de diseño (DBT). Los tipos de organizaciones que pueden estar en contacto durante el desarrollo de la descripción de una DBT incluyen a las locales, estatales, y organismos relacionados con la inteligencia (Sandia National Laboratories, 2002).

Riesgo de ataque. Una vez descrita la amenaza, la información se puede utilizar junto con las estadísticas de sucesos pasados y la percepción de sitios específicos para clasificar las amenazas en términos de probabilidad de que cada tipo de amenaza que pueda producir un suceso no deseado.

5. Análisis de la Eficacia del Sistema de Protección

La Figura 3 resume el esquema del proceso de diseño y de análisis que puede ser utilizado al estimar la eficacia del sistema de protección física. Las características de la protección física deben ser descritas en detalle antes de la evaluación de la eficacia del sistema de seguridad.

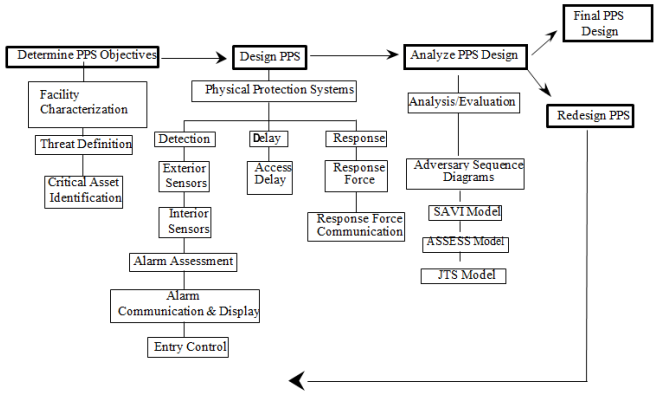

Fig. 3. Diseño y esquema del proceso de evaluación

6. Estimación del riesgo

Evaluación del riesgo mediante la fórmula ya enunciada; Riesgo = PA * (1 - PE) * C.

7. Actualizaciones e Impactos

Actualizaciones del Sistema. Si el riesgo estimado para el ámbito de la amenaza descrita se considera inaceptable, habrá que considerar mejoras en el sistema. El primer paso es revisar todas las suposiciones que se hicieron y que afectan el riesgo. Todas las suposiciones sobre eventos no deseados, la identificación de objetivos, definición de consecuencias, la descripción de la amenaza, la estimación de la probabilidad de ataque, y las funciones de las salvaguardas deben ser revaluadas con cuidado. La actualización del sistema se puede analizar para calcular los cambios en el riesgo debido al cambio en la probabilidad de ataque, la efectividad del sistema, o los valores de las consecuencias. Si el riesgo estimado para la actualización del sistema se considera aceptable, la actualización se ha completado. Si el riesgo sigue siendo inaceptable, el proceso de actualización y la mejora del sistema se debe repetir hasta que el riesgo se considere aceptable.

Actualización de Impacto. Una vez que la actualización del sistema ha sido definida, es importante evaluar el impacto de la actualización del sistema en la misión de la instalación y el costo. Si las actualizaciones del sistema suponen una pesada carga para el funcionamiento normal, habrá que considerar la posibilidad de una compensación entre el riesgo y las operaciones. Se deberá tener en cuenta un equilibrio entre el riesgo y el coste total. Cuando el equilibrio se alcanza en el nivel de riesgo y el impacto en el coste de la actualización, la misión, y el calendario, la actualización del sistema está lista para su aplicación. En este punto, se puede afirmar que el diseño y proceso de análisis han sido completados.

2.5 SECUREPORT, 2004. Puertos del Estado (ESPAÑA)

En España Puertos del Estado, como organismo autónomo responsable de la coordinación de las actividades en los puertos comerciales españoles, y en dependencia directa del Ministerio de Fomento, desarrolló una metodología para la evaluación de la protección y posterior elaboración de los planes de protección de las instalaciones portuarias (Gobierno de España, 2007), que incluye el diseño de una herramienta informática, denominada "SECUREPORT".

La Comisión Europea legisla la seguridad en puertos a través de la Directiva 2005/65/CE de 26 de octubre de 2005 sobre mejora de la protección portuaria (Unión Europea, 2005).

El sistema de valoración del riesgo seguido en España se resume a continuación, así como los criterios de aceptación del mismo. El cálculo del riesgo que cada uno de los supuestos a estudiar ocasiona en cada uno de los elementos a analizar, se realiza mediante la expresión siguiente:

$$IR = ID \times IV \times IC \quad (4)$$

donde:

IR Índice de Riesgo, que se define como la estimación cuantitativa del Riesgo existente en el caso que se analiza. ID Índice de Verosimilitud, IV Índice de Vulnerabilidad, IC Índice de Consecuencias. Cada uno de los índices globales anteriores se aplica mediante una batería se índices y subíndices.

La verosimilitud se determina mediante:

- Índice de Probabilidad General (IPG), se trata de un índice que valora de forma global las posibilidades de un ataque terrorista a las instalaciones y cuyo valor lo determina la autoridad en materia de seguridad (Guardia Civil).
- Índice de Carácter Simbólico (lAS), valora el incremento de la probabilidad de presentación de un suceso que se produce en relación con el nivel general definido en el apartado anterior, debido al carácter simbólico de la instalación o elemento que se analiza, que pudiera hacerle convertirse en un blanco preferente del ataque. Se entenderá que un bien tiene carácter simbólico cuando se trata de una instalación portuaria o elemento de la misma que está considerado en el ámbito nacional, regional o local como un referente significado del puerto o de la ciudad o del entorno en que se encuentra, de manera que la repercusión social de cualquier siniestro que se produzca en él pudiera hacerle convertirse en un blanco preferente.
- Índice de Trascendencia para la Protección (lTP), valora el incremento de la probabilidad de presentación de un suceso que se produce debido al hecho de que el elemento o instalación que se considera deba tener reforzado su integridad ante un ataque, ya sea por tratarse de elementos que controlen o realicen las funciones de protección (p.e. centros de control de seguridad), o por que tengan que desarrollar acciones posteriores al suceso que minimicen las consecuencias del mismo (p.e. instalaciones de bomberos). Tendrán está consideración todas las instalaciones o elementos que tengan encomendado el control o el desarrollo de las funciones de protección, ya se trate de instalaciones gubernamentales o de otras que no tengan esa consideración.

La vulnerabilidad se valora mediante:

- Índice de Accesibilidad a la Instalación (IAI), valora cuantitativamente la facilidad con la que las personas o los medios de que se valgan para ocasionar una amenaza a la instalación portuaria o al elemento que se considere, puedan introducirse o aproximarse a ellos. A efectos de este apartado se considerarán medios las mercancías, equipajes, vehículos y cualquier otro procedimiento que pueda ser utilizado para facilitar la intrusión.
- La valoración de la accesibilidad se realizará utilizando

una escala que tendrá los cuatro niveles siguientes: 4 Accesos sin control o con controles inoperativos. 3 Existencia de defensas perimetrales y de sistemas de control de accesos permanentemente operativos. 2 Existencia de defensas perimetrales y de sistemas de control de accesos permanentemente operativas.1 Todas las medidas descritas en el Nivel 2 (Ministerio del Interior) y además existencia de patrullas armadas permanentemente operativas, con posibilidad de intervención rápida en caso de intrusión.

- Índice de susceptibilidad a la Destrucción (ISD), valora cuantitativamente la susceptibilidad del elemento que se considera a su destrucción ocasionada por la amenaza que se analiza. La valoración tomará en consideración la tipología de las amenazas, ya se trate de un ataque convencional con explosivos, de un ataque bioquímico o similar, o de un ataque cibernético o de otras características cuyo objetivo sea generar daños sin producir destrucción física de elementos. Se consideran ataques bioquímicos, cibernéticos o convencionales con explosivos. La puntuación varía entre 4-1 puntos.
- Índice de Ineficiencia Operativa (lIO), valora cuantitativamente la ineficiencia de los procedimientos operativos establecidos para hacer frente a la amenaza que se considera, incluidas las consecuencias que se deriven de ella. La valoración se realizará en relación con las características, funciones o servicios prestados por la instalación o elemento que se valora. La puntuación oscila entre 4-1 puntos
- Los índices utilizados para la cuantificación de las consecuencias son:
- Índice de daños a la Vida Humana (IDV), valora cuantitativamente los daños a la vida humana, ya sea con resultado de muerte o de lesiones, que se puedan producir tanto en el recinto de la instalación portuaria como en su entorno, a consecuencia de los sucesos que se consideren, la valoración tomará en consideración los daños ocasionados directamente por el suceso VRD, como los que se produzcan por siniestros ocasionados por el suceso (p.e. hundimiento de estructuras, incendio de productos almacenados, liberación de productos tóxicos, etc.), VRI, como los debidos a efecto dominó en otras instalaciones, VRDO. La valoración de los daños se efectuará determinando los espacios de influencia de los diferentes sucesos, en términos de alcance e intensidad con lo que se manifiestan, tomando en consideración los factores geográficos, climáticos y otros que afecten a la instalación portuaria y al elemento que se analice.
- Se clasifican los daños a la vida humana y posteriormente se valoran entre 5-1 punto, y se evalúa las muertes o daños producidos en una superficie alrededor de la zona atacada.
- Índice de Daños Económicos (IDE), Valora cuantitativamente las repercusiones económicas por reconstrucción de todos los elementos dañados, ya sean de la instalación portuaria o ajenos a ella incluyendo los de cese o afección de las actividades económicas que se realicen en ellas, CDR, así como los ocasionados por cese o afección de las actividades económicas relacionadas con las instalaciones que hayan sufrido daños directos, CRI.
- El costo CRD es el de la inversión de las obras de reconstrucción de los elementos dañados de la instalación portuaria incluyendo en ambos casos los costos por cese o afectación de las actividades económicas que se realicen en las instalaciones directamente dañadas.
- El costo CRI es el de repercusiones económicas por cese o afección de las actividades económicas relacionadas con la instalación portuaria que hayan sufrido daños directos, ya sean actividades oferentes o demandantes de servicios creados cuando las instalaciones estaban operativas. La valoración de CRI se efectuará en términos de pérdida de Valor Añadido Bruto (VAB).
- Índice de Redundancia de Elementos que aseguren la Funcionalidad (IRD), Valora cuantitativamente la posibilidad de que la instalación portuaria que se analiza pueda seguir funcionando sin los bienes que resulten afectados por el suceso que se considera. El análisis tomará en consideración la posibilidad de que la función afectada pueda ser suplida por otra instalación portuaria similar existente en el mismo puerto. La valoración de la incidencia se determinará por el porcentaje en que las funciones afectadas queden cubiertas por otras instalaciones propias o ajenas.
- Índice del plazo de Recuperabilidad (IRP), Valora cuantitativamente el plazo de tiempo necesario para que la instalación portuaria recupere íntegramente las capacidades funcionales y operativas que tenía previamente al ataque que se analiza, si esa recuperación es posible. La valoración de la incidencia se determinará por el plazo necesario para que la instalación portuaria recupere sus funciones.
- Índice de Repercusión Social y Ambiental (ISA).
- Para la determinación del subíndice de repercusión en el medio ambiente, se asignarán los siguientes valores en función de las consecuencias que el suceso analizado pueda presentar en el medio ambiente, desde repercusión muy alta (5 puntos) hasta muy baja (0 puntos).
- Para el cálculo del subíndice de repercusión en el patrimonio artístico se asignaran los siguientes valores en función de las consecuencias que el suceso analizado pueda presentar en dicho patrimonio. La puntuación varía desde 5 a 1 punto.
- Para el cálculo del subíndice de alarma social se asignaran los siguientes valores en función de la alarma social generada por el suceso que se analiza. La puntuación varía desde 5 a 1 punto.
- El índice de riesgo puede tomar valores comprendidos entre 1 y 20 ambos inclusive, para el supuesto de que el Índice de Vulnerabilidad sea 1, valores comprendidos entre 2 y 40, ambos inclusive, para el supuesto de que el Índice de Vulnerabilidad sea 2 y valores comprendidos entre 3 y 60, ambos inclusive para el caso de que el Índice de Vulnerabilidad sea 3.

La evaluación del riesgo se efectúa mediante la compa-

ración del Índice del Riesgo obtenido para cada uno de los supuestos analizados con los criterios de aceptación de riesgo establecidos en este apartado (Sanchidrian, 2004). Los niveles de riesgo se definen como inadmisible, admisible, corregible, para los cuales se han establecido los valores siguientes:

Inadmisible: (N), IR ≥15,
Admisible: (A), IR < 10
Corregible: (C); 10 ≤ IR<15

3 Conclusiones

Del análisis de las diferentes metodologías aquí expuestas se deduce que la evaluación del riesgo, en términos de cuantificación del mismo, presenta diferencias importantes entre unas y otras, si bien se mantiene siempre el formato de; Riesgo = Amenaza x Vulnerabilidad x Impacto con leves variantes.

Así, la metodología RBDM introduce una variación en el concepto de consecuencia o impacto, discriminando el puerto por zonas en función de las características de la carga del buque; mercancías peligrosas, pasaje, etc., diferenciando así la importancia de las consecuencias de un ataque a una zona con personas o con mercancía normal o peligrosa. Además define tres parámetros para valorar ésta; disponibilidad, accesibilidad, seguridad orgánica y dificultad del objetivo.

Por su parte la metodología RAM denomina los conceptos de forma similar, si bien el significado es el mismo que el propuesto por la OMI y el formato es el mismo en conceptos y forma de proceder.

SECUREPORT es la metodología más compleja y novedosa de todas ellas, en tanto que considera hasta ocho subíndices para valorar los tres índices globales clásicos de amenaza (aquí verosimilitud), vulnerabilidad y consecuencias. En ese sentido, los índices definidos para la evaluación de la verosimilitud son tres y recogen cuantitativamente aspectos clave como la probabilidad de un ataque terrorista específico, así como la probabilidad de incremento de dicho riesgo debido al carácter simbólico de la instalación y el incremento de probabilidad de ataque, debido a que los sistemas de seguridad o de control puedan estar reforzados en una instalación concreta, lo que indicaría que la amenaza aquí es mayor. Además la vulnerabilidad se evalúa considerando la adecuación de las medidas de control de acceso y la susceptibilidad de destrucción del elemento a la amenaza en estudio, considerando tres tipos de ataques; ataques bioquímicos, cibernéticos o convencionales con explosivos. Respecto al IDV discrimina éste en varios tipos de afección. Igual sucede con el IDE, el cual diferencia daños económicos por cese de actividad económica y por reconstrucción. Se introducen dos conceptos nuevos para valorarla posibilidad de que la instalación pueda seguir funcionando sin los bienes que resulten afectados y el plazo de tiempo necesario para que la instalación portuaria recupere íntegramente las capacidades funcionales. Por último se considera un índice que valora la repercusión social del atentado, valor o contemplado en las anteriores formulaciones.

Referencias

Cabeza M, Cabrita E, 2007. La planificación estratégica del análisis de riesgo cuantitativo de procesos, Ciencia e Ingeniería Vol. 28 Nº. 2

Comisión de las Comunidades Europeas, 2003. Proposal for a Regulation of the European Parliament and of the Council on Enhancing Ship and Port Facility Security.

Gobierno de España, 2007. Real Decreto 1617/2007, de 7 de diciembre, por el que se establecen medidas para la mejora de la protección de los puertos y del transporte marítimo. Boletín Oficial del Estado, núm. 34, pp. 52395-52405.

Masse T, O'Neil S, Rollins John, 2007. The Department of Homeland Security's risk assessment methodology: Evolution, issues, and options for Congress, DTIC Document.

Sanchidrián C, 2008. La seguridad, el código ISPS y la legislación comunitaria.

Sandia National Laboratories, 2002.A Scalable Systems Approach for Critical Infrastructure Security.

Servicio de Guarda Costas de los Estados Unidos de América, 2003. Navigation and Vessel Inspection. Circular N° 11-02 (NVIC 11-02).

Oficina Internacional del Trabajo (ILO) y Organización Marítima Internacional (OMI-IMO), 2004. Security in Ports. ILO and IMO code of practices.

Organización de las Naciones Unidas, 2006.Maritime security: elements of an analytical framework for compliance measurement and risk assessment.

Unión Europea, 2005. DIRECTIVA 2005/65/CE del Parlamento Europeo y del Consejo de 26 de octubre de 2005 sobre Mejora de la Protección Portuaria. Diario Oficial de la Unión Europea.

Recibido: *04 de octubre de 2013*

Revisado: *15 de marzo de 2014*

Romero Faz, David: *Ingeniero de Caminos, Canales y Puertos. Experto Universitario en Transporte Marítimo y Gestión Portuaria. Profesor Asociado de la Universidad Politécnica de Madrid. Consultor de Ingeniería Marítima y Transportes en Isdefe.*

Camarero Orive, Alberto: *Doctor Ingeniero de Caminos, Canales y Puertos. Licenciado en Economía. Licenciado en Administración y Dirección de Empresas. Profesor Titular de la Universidad Politécnica de Madrid. Asesor en Logística, Transporte Marítimo y Puertos. Correo electrónico: alberto.camarero@upm.es .*