UNIVERSIDAD POLITÉCNICA DE MADRID

Escuela Técnica Superior de Ingenieros de Caminos,
Canales y Puertos

Metodología para la Evaluación del Riesgo en Instalaciones Portuarias

Tesis Doctoral

David Romero Faz

Ingeniero de Caminos, Canales y Puertos

Noviembre 2017

DEPARTAMENTO DE INGENIERÍA CIVIL: TRANSPORTE Y
TERRITORIO

Escuela Técnica Superior de Ingenieros de Caminos,
Canales y Puertos

Metodología para la Evaluación del Riesgo en Instalaciones Portuarias

David Romero Faz

Ingeniero de Caminos, Canales y Puertos

Director: Alberto Camarero Orive

Dr. Ingeniero de Caminos, Canales y Puertos

Licenciado en Economía

Licenciado en Administración y Dirección de Empresas

Noviembre 2017

Tribunal nombrado por el Sr. Rector Magnífico de la Universidad
Politécnica de Madrid, el día de de 2017.

Presidente:

Secretario:

Vocal:

Vocal:

Vocal:

Suplente:

Suplente:

Realizado el acto de defensa y lectura de Tesis el día de
de 2017 en la Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos
de Madrid, habiendo obtenido la calificación de:

EL PRESIDENTE

LOS VOCALES

EL SECRETARIO

A Miriam, Rodrigo y Gonzalo, por todo el tiempo que les he quitado de estar juntos.

A mis padres, por su amor y apoyo incondicional.

El éxito es la suma de pequeños esfuerzos, repetidos día tras día.

Robert Collier.

Agradecimientos

La decisión de realizar el doctorado supone un esfuerzo personal muy importante, sobre todo si se realiza cuando ya se tienen responsabilidades profesionales y familiares.

En mi caso personal, la decisión surgió hace años, cuando comencé mi carrera profesional como profesor de Puertos en la Escuela de Ingeniería Civil de la Universidad Politécnica de Madrid, como una necesidad para mi desarrollo como profesor y como investigador.

El desarrollo del doctorado en mi caso, ha resultado un camino largo lleno de obstáculos derivados de periodos en blanco por carga de trabajo, cambio de programa de doctorado o problemas administrativos al final, que con buena voluntad se solventaron. En definitiva, ha sido mucho el esfuerzo y el tiempo dedicado para su consecución, tiempo que he dejado de dedicar a mi familia y que sin embargo esta ha aceptado con buen ánimo.

Toda mi gratitud por tanto es para ellos, para mi mujer, Miriam, y para mis hijos, Rodrigo y Gonzalo, sin duda el motor de mi vida. Todo este esfuerzo es por ellos.

Agradecerles asimismo a mis padres, Fernando y Pilar, su cariño y amor incondicional siempre y sus ánimos para emprender esta empresa con éxito.

Agradecerle a mi Director de Tesis, el profesor D. Alberto Camarero Orive, por dedicarme sus esfuerzos tanto tiempo a pesar de las muchas vicisitudes que han surgido durante estos años.

A la profesora Dña. Nicoletta González Cancelas, por sus consejos y orientaciones en el desarrollo de los mis publicaciones durante el desarrollo de la Tesis Doctoral y por sus consejos.

A todos aquellos compañeros docentes que, habiendo pasado ya por ello, me han dado ánimos durante estos años para acabar el doctorado con éxito.

A mis compañeros y amigos, Luis y José María, por su apoyo y ánimos permanentes y en especial a Luis por su ayuda en la revisión del inglés de algunos artículos.

Mi agradecimiento sincero también para el profesor D. Andrés Valiente, por sus eficaces gestiones con el Vicerrectorado de Investigación para poder leer esta Tesis Doctoral después de muchas trabas administrativas.

Y gracias en definitiva a todos aquellos que me pueda olvidar y que habéis estado a mi lado durante todo este tiempo.

Resumen

A raíz de los atentados de Nueva York en 2001, el sector aeroportuario inicialmente y posteriormente otros, comenzaron a tomar medidas para protegerse de atentados futuros. Posteriormente se desarrolló el concepto de infraestructuras críticas en EUA y en Europa, considerándose entre estas las infraestructuras asociadas al transporte; carreteras, aeropuertos, ferrocarriles y puertos.

En la actualidad existen numerosas metodologías para la evaluación del riesgo en infraestructuras críticas, si bien en el ámbito de las infraestructuras portuarias no existen a penas metodologías específicas y las existentes ofrecen resultados claramente mejorables. Uno de los problemas, constatado en la literatura científica, es la existencia de discrepancias importantes entre los resultados de evaluación del riesgo en las metodologías desarrolladas, algunas muy teóricas, y los riesgos reales que se dan en las infraestructuras portuarias.

Esta Tesis Doctoral intenta aportar una solución a la carencia de metodologías para puertos, desarrollando una específica para este tipo de infraestructuras, centrada en las amenazas para la infraestructura y las personas, apoyándose para ello en las ya existentes, y mejorando aquellos aspectos no considerados hasta la fecha en la evaluación del riesgo mediante el empleo de encuestas al sector portuario español. Asimismo dicha aportación mejora la credibilidad de las amenazas a considerar al emplearse datos estadísticos de incidentes contra la seguridad en puertos comerciales españoles.

Asimismo la propuesta metodológica elaborada permite evaluar el nivel de riesgo de una instalación dada en su conjunto y permite tener una idea cualitativa del nivel de riesgo global que tiene un puerto.

Abstract

Following the attacks in New York in 2001, the airport sector initially and subsequently others began to take measures to protect against future attacks. Later, the concept of critical infrastructures was developed in the USA and in Europe, considering the infrastructures associated with transport; Roads, airports, railways and ports.

Nowadays there are many methodologies for risk assessment in critical infrastructures, although in port infrastructures there are only a few and the existing ones do not offer completely reliable results. One of the problems observed in the scientific literature is the existence of important discrepancies between the results of risk assessment in the existing methodologies (some are very theoretical), and the real risks that occur in port infrastructures.

This Doctoral Thesis tries to provide a solution to the lack of methodologies for ports, developing an specific one for this type of infrastructures focusing specifically on the threats to infrastructure and people, relying on existing ones and improving those aspects not considered to date in the risk assessment through the use of surveys of the Spanish port sector. Likewise, this contribution improves the credibility of the threats to be considered when using statistical data on security incidents in Spanish ports.

In addition the elaborated methodology allows evaluating the level of risk of a given facility as a whole and allows having an approximate idea of the existing level of global risk in the port.

1. INTRODUCCIÓN.....	1
1.1. Motivación de la Tesis Doctoral	2
1.2. Objetivo de la Tesis Doctoral.....	4
1.3. Estructura del documento.....	5
2. ANTECEDENTES	9
2.1. Las amenazas para la seguridad en los puertos.....	11
2.1.1. Los polizones y el tráfico ilegal de personas	11
2.1.2. El contrabando marítimo	12
2.1.3. La piratería	13
2.1.4. El Terrorismo	15
2.1.5. El Bio-terrorismo	17
2.1.6. El Ciberterrorismo	19
2.2. El Marco Regulatorio.....	19
2.2.1. Código Internacional para la Protección de los Buques y las Instalaciones Portuarias (PBIP)	20
2.2.2. Reglamento (CE) nº 725/2004.....	23
2.2.3. Directiva 2005/65/CE	25
2.2.4. Real Decreto 1617/2007	28
2.2.5. Directiva Comunitaria 2008/114/CE	30
2.2.6. Ley 8/2011 de Infraestructuras Críticas	32
2.2.7. Organización Internacional del Trabajo y Organización Marítima Internacional (OIT/OMI)	33
3. ESTADO DEL CONOCIMIENTO.....	37
3.1. Métodos de evaluación del riesgo	37
3.1.1. Métodos simplificados de evaluación del riesgo	38
3.1.2. Métodos complejos.....	43
3.1.3. Otros métodos	72
3.2. Evaluación de riesgos en infraestructuras	73

Índice

3.2.1.	Conceptos básicos de la evaluación de riesgos.....	73
3.2.2.	Gestión del riesgo.....	78
3.2.3.	Metodologías de evaluación de riesgos en infraestructuras críticas.....	79
3.3.	Análisis de riesgos en puertos.....	81
3.3.1.	Riesgos medioambientales y ante desastres naturales	82
3.3.2.	Riesgos económicos	85
3.3.3.	Riesgos asociados a la mercancía.....	88
3.3.4.	Riesgos asociados a la operación	92
3.3.5.	Riesgos asociados a variables políticas de seguridad.....	95
3.3.6.	Nuevas metodologías de evaluación de riesgos	97
4.	METODOLOGÍA.....	101
4.1.	Introducción	101
4.2.	Etapas de la metodología de la investigación	102
4.3.	Métodos y herramientas de investigación.....	104
4.3.1.	Recopilación y revisión bibliográfica	105
4.3.2.	Método deductivo.....	106
4.3.3.	Método comparativo	106
4.3.4.	Encuesta al Sistema Portuario Español	107
4.3.5.	Análisis de las estadísticas de seguridad	108
4.3.6.	Método inductivo.....	108
4.3.7.	Método Delphi	109
4.3.8.	Aplicación a una instalación portuaria.....	111
4.4.	Desarrollo de las etapas de la metodología.....	111
4.4.1.	Etapas 1. Definición de criterios y selección de metodologías a considerar ..	111
4.4.2.	Etapas 2. Análisis y evaluación comparativa de las metodologías seleccionadas	112
4.4.3.	Etapas 3. Identificación de nuevos parámetros.....	113

4.4.4.	Etapa 4. Elaboración de la Propuesta Metodológica	115
5.	RESULTADOS	119
5.1.	Etapa 1. Definición de criterios y selección de metodologías a considerar	119
5.1.1.	Criterios propuestos	119
5.1.2.	Metodologías seleccionadas	119
5.2.	Etapa 2. Análisis y evaluación comparativa de las metodologías seleccionadas	121
5.2.1.	AERONÁUTICA CIVIL (Colombia)	121
5.2.2.	CARVER (EUA)	122
5.2.3.	RBDM. Navigation and Vessel Inspection (Servicio de Guarda Costas de EUA)	122
5.2.4.	SECUREPORT. Puertos del Estado (España)	123
5.2.5.	TRAM (IMO-ILO)	124
5.2.6.	Resumen de la evaluación	124
5.2.7.	Evaluación comparativa de parámetros	125
5.3.	Etapa 3. Identificación de nuevos parámetros	135
5.3.1.	Resultado de la Encuesta al Sistema Portuario Español	135
5.3.2.	Análisis de estadísticas de seguridad	139
5.3.3.	Principales amenazas a considerar	143
5.3.4.	Identificación preliminar de parámetros	145
5.3.5.	Propuesta preliminar de coeficientes de ponderación de los parámetros... 145	
5.3.6.	Aplicación del Criterio Experto	146
5.4.	Etapa 4. Elaboración de la Propuesta Metodológica	149
5.4.1.	Propuesta metodológica	149
5.4.2.	Criterios de valoración de los coeficientes	159
5.4.3.	Criterios de evaluación del riesgo	161
5.4.4.	Evaluación del riesgo	163
6.	APLICACIÓN A LAS INSTALACIONES DE UN PUERTO	167

Índice

6.1. Objeto.....	167
6.2. Amenazas evaluadas	167
6.3. Evaluación del riesgo.....	168
6.4. Resultados	175
6.5. Análisis de sensibilidad de los coeficientes	177
7. CONCLUSIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN	187
7.1. Conclusiones.....	187
7.2. Futuras líneas de investigación	189
BIBLIOGRAFÍA.....	193

ANEXO 1 METODOLOGÍAS CONSIDERADAS

ANEXO 2 ENCUESTA AL SISTEMA PORTUARIO ESPAÑOL

ANEXO 3 CRITERIO EXPERTO

ÍNDICE DE FIGURAS

Figura 1. Esquema metodológico de la Tesis. Fuente: Elaboración propia.....	6
Figura 2. Método Dow. Procedimiento de cálculo.....	55
Figura 3. Esquema de cálculo del índice DOW. Factores de penalización	58
Figura 4. Esquema de cálculo del índice DOW. Factores de bonificación.....	58
Figura 5. Ejemplo de árbol de fallos.....	60
Figura 6. Simbología básica utilizada en diagramas	70
Figura 7. Símbolo de toma de decisión adjunta.....	71
Figura 8. CFD de seguridad del puerto.....	97
Figura 9. Etapas de la metodología de la investigación.	103
Figura 10. Preguntas y objetivos que determinan las actividades y herramientas aplicadas. .	104
Figura 11. Métodos y herramientas. Fuente: Elaboración propia	105
Figura 12. Panel de expertos. Actividades y herramientas.	146

ÍNDICE DE TABLAS

Tabla 1. Niveles de riesgo en función de la probabilidad y las consecuencias	39
Tabla 2. Cuadros de cualificación de riesgos.....	41
Tabla 3. Grado de peligrosidad	42
Tabla 4. Formato de recogida del HAZOP	47
Tabla 5. Contenido de las columnas.....	48
Tabla 6. Formulario de trabajo para análisis FMECA	49
Tabla 7. Símbolos utilizados para la representación del árbol de fallos	61
Tabla 8. Curva híbrida de exceso de pérdidas.....	84
Tabla 9. Relaciones cualitativas entre parámetros de las metodologías seleccionadas.....	130
Tabla 10. Resumen de parámetros considerados en cada metodología	131
Tabla 11. Resumen de estadísticas de seguridad en Sistema Portuario Español	139
Tabla 12. Matrices de riesgo específico	160
Tabla 13. Matrices de riesgo específico	162
Tabla 14. Evaluación del riesgo	163
Tabla 15. Resultados para el riesgo específico.....	175

Capítulo

1

Introducción

1. INTRODUCCIÓN

El transporte marítimo ha sufrido un incremento espectacular desde los años cincuenta, fecha en la que la economía mundial comienza su crecimiento sucesivo y en la que se comienza a gestar una clase económica que se denominará media, rompiéndose así las grandes diferencias entre pobre y ricos en el mundo occidental y en especial en Europa. Esta nueva clase media resultará ser la gran consumidora.

Dicho crecimiento económico supondrá unos cambios importantes, y en especial el denominado “desarrollismo económico”, que implica la industrialización de aquellos países tradicionalmente agrícolas para poder competir en términos de producción y exportación con aquellos más desarrollados económicamente. Estos cambios se manifiestan asimismo en los puertos comerciales de dichos países, de forma que estos van modificando su estructura, modelo de gestión y objetivos, transformándose con el tiempo en lo que actualmente son, empresas, públicas o privadas cuyo objetivo principal es el de dar soporte al denominado comercio marítimo a través del uso y explotación de su superficie suministrando una serie de servicios a la mercancía y al pasaje que por ellos discurren.

Desde el punto de vista de la mercancía y por ende del usuario, cada vez más el cliente, esta modernización en su modelo de gestión a un sistema moderno de un puerto en red orientado a los mercados y que se rige por su eficiencia, supone que el cliente es quien manda y por tanto exige garantías importantes para sus productos en su paso por el puerto, incluyendo la seguridad e integridad de sus mercancías (riesgo de ataques, robos, etc.). Esta transformación se produce a partir de los años cincuenta y aún sigue sucediéndose día a día.

Si bien el mundo se dividió en dos grandes bloques políticos a partir de los años cincuenta, es a partir de los años setenta cuando con los grandes movimientos migratorios debidos a los diversos conflictos políticos que asolan el mundo, comienzan a producirse actos delictivos de relevancia, principalmente localización de polizones en buques con travesías internacionales, si bien también se producen robos de mercancía en puerto y/o en el buque, así como daños a los buques y a sus tripulaciones en alta mar debidos a la piratería, la cual se incrementa en especial con las diferencias económicas entre países desarrollados y países en desarrollo o países en desarrollo.

Durante los años ochenta y sucesivos este fenómeno continúa creciendo con diferentes grados de desarrollo, y si bien se ha combatido desde entonces, su erradicación supone una tarea compleja en origen, dado que en muchas ocasiones

existen evidentes vínculos entre los piratas y los gobiernos de los países que los albergan. Asimismo su estructura se ha transformado desde pequeños grupos actuando de forma desorganizada y anárquica a estructuras mafiosas bien organizadas y pertrechadas para efectuar asaltos en alta mar o en el propio puerto.

El resultado de dicho problema, junto con otros nuevos, especialmente el Islamismo radical o también denominado Yihadismo a partir de los años noventa, o los problemas políticos existentes desde hace décadas en Europa del Este entre el pueblo checheno y Rusia, o los existentes entre el denominado Kurdistán y los países que albergan poblaciones de dicho origen, e incluso el problema entre palestino e israelíes, incrementan la inseguridad en las instalaciones portuarias de numerosos puertos comerciales en todo el mundo.

La ejecución de numerosos ataques terroristas en las últimas décadas (RAND, 2009) ha puesto de manifiesto la fragilidad de los sistemas de transporte. Dichos ataques pueden romper la cadenas de suministro (Greenberg, Chalk, Willis, Khilko, & Ortiz, 2006), interrumpiendo así el comercio internacional, lo que provoca no sólo pérdidas de vidas humanas, sino también impactos económicos y políticos significativos.

Esta situación condujo a los puertos a mostrar su interés por la evaluación de la seguridad de sus terminales y por parte de los gobiernos al deseo de conocer el riesgo para la seguridad de las personas que transitan o trabajan por un puerto a diario.

Conocido dicho interés, manifestado en 2003 a través de la Organización Marítima Internacional mediante la propuesta de una metodología de evaluación de la seguridad, surge la necesidad diez años después de su elaboración y de la de otras metodologías similares, de evaluar e intentar recoger aquellos aspectos que no han sido descritos aun o simplemente se consideran de manera inadecuada a la vista de los años de aplicación de estas metodologías.

La necesaria mejora en las metodologías empleadas en la evaluación se inicia en el presente capítulo en base a la investigación para el desarrollo de una nueva propuesta metodológica para la evaluación de la seguridad en instalaciones portuarias, que constituye el motivo de esta Tesis Doctoral y que continua en capítulos posteriores, en los cuales se desarrolla el estado del arte, la metodología de la investigación y se enuncian los resultados obtenidos que dan respuesta a los objetivos de ésta.

1.1. Motivación de la Tesis Doctoral

La presente Tesis Doctoral se desarrolla como resultado del acercamiento de su autor en fase previa pre-doctoral al sector de la evaluación de la seguridad en instalaciones portuarias, a través del estudio del Código sobre Protección de Buques e Instalaciones Portuarias (PBIP) y su aplicación en instalaciones portuarias españolas.

En los últimos años, ha habido un reconocimiento internacional creciente de que el rendimiento de la seguridad en la industria marítima debe ser revisado con carácter

urgente. Un gran número de medidas opcionales de control de seguridad marítima se han propuesto a través de diversos reglamentos y publicaciones con posterioridad al 11 Septiembre de 2001, (Z. L. Yang, Wang, Bonsall, & Fang, 2009). Aunque las medidas llevadas a cabo y las regulaciones en seguridad han mejorado en gran medida el rendimiento de la seguridad portuaria, las experiencias en las últimas décadas indican la necesidad actual de fortalecer el marco regulatorio de la seguridad, que a menudo carece de una estrategia integrada. Por ejemplo, mientras que el Código PBIP exige a las autoridades competentes llevar a cabo las evaluaciones de protección de la instalación portuaria, éste no prescribe ninguna metodología aceptada de forma general para implementarlo. Asimismo, el Código PBIP sugiere utilizar tres niveles de seguridad para hacer frente a los diferentes riesgos a los que se enfrentan los puertos en entornos operativos dinámicos, sin embargo, no incorpora ningún análisis de riesgos en la definición de los tres niveles de seguridad. En el caso de los puertos, esto se complica por el hecho de que las responsabilidades de la protección portuaria están en manos de los gobiernos, quienes tienen el poder final en la toma de todas las decisiones, incluyendo la aprobación del Plan de Protección de las Instalaciones Portuarias (PIIP) y la designación de los Oficiales de Protección de la Instalación Portuaria (OPIP). Así pues las voces que requieren una mayor justificación de la eficiencia por parte de los usuarios marítimos son aun importantes, tal y como se reflejó por parte de muchos participantes en el *Annual Total Port Security Forum (ATPSF) 2012*, (Z. Yang, Ng, & Wang, 2014).

Además, la evaluación de la seguridad tiene hoy en día una finalidad imprescindible en el contexto del funcionamiento óptimo de cualquier puerto comercial, dado que el valor de un puerto son sus clientes y con ellos la seguridad de sus mercancías. Se puede afirmar sin miedo a equivocarnos que la seguridad es un indicador neto de la eficiencia de un puerto comercial, vinculándose ésta a una óptima gestión del mismo, y dentro del puerto es igualmente aplicable esta definición a la seguridad a nivel de la terminal.

Este indicador resulta de tal interés e importancia que muchos clientes pueden llegar a optar por mover sus mercancías, entre otros motivos, por el grado de seguridad de un puerto o de una terminal concreta, y por tanto el adecuado conocimiento y valoración de los riesgos resulta vital para las partes implicadas, puerto y cliente.

Se trata por tanto de un factor de competitividad y por ello su desarrollo, en términos de aproximación a la realidad y del conocimiento del riesgo preciso que las terminales sufren frente a las amenazas a la seguridad de sus instalaciones resulta del máximo interés para el explotador portuario.

Se constató así la necesidad real de seguir investigando y mejorando la evaluación de los diferentes escenarios de amenaza que pueden darse para la seguridad en instalaciones portuarias en busca de una metodología más acorde con la realidad de la seguridad.

La escasa existencia de formulaciones específicas para el análisis de la seguridad en puertos fue asimismo otra de las motivaciones importantes para su tratamiento, dado

que si bien existen numerosas formulaciones generalistas para la evaluación de la seguridad en las denominadas “infraestructuras críticas” (entre las que se encuentran estos) con diferentes orígenes y antecedentes de aplicación, las metodologías particularizadas para puertos son muy reducidas.

Por ello resulta motivadora la obtención de nuevos parámetros para mejorar la evaluación de los riesgos para la seguridad en instalaciones portuarias ajustada a situaciones reales y en base a datos actualizados.

Así pues se considera justificada y motivada la elección de este tema como objeto de desarrollo a través de la presente Tesis Doctoral.

1.2. Objetivo de la Tesis Doctoral

El objetivo principal de esta Tesis Doctoral es la propuesta de una nueva metodología de evaluación del riesgo en instalaciones portuarias con el fin de ofrecer otra opción más de evaluación del riesgo al explotador de la instalación portuaria, apoyándose en datos reales de seguridad y considerando la experiencia actual en los puertos españoles.

Dada la amplitud de riesgos potenciales en una instalación portuaria; informáticos, seguridad, operacionales, laborales, etc., se consideran aquí solamente aquellos riesgos asociados a la seguridad de las mercancías y de las personas. Para ello se consideran fundamentalmente amenazas que supongan un deterioro de la infraestructura y los servicios del puerto, es decir la operación portuaria.

Para ello se prevé la obtención de nuevos parámetros que contemplen aspectos no considerados hasta la fecha en la evaluación de riesgos contra la seguridad en puertos, configurando una nueva propuesta metodológica de evaluación del riesgo. Esta permitirá a los explotadores de las terminales una determinación de los riesgos de atentados o acciones criminales contra la seguridad en sus instalaciones más ajustada a la realidad, dado que actualmente algunos riesgos están aparentemente sobrevalorados y otros, por el contrario, resultan infravalorados.

Asimismo se pretende obtener una evaluación del riesgo global de la instalación portuaria mediante la evaluación de las amenazas más relevantes obtenidas previamente.

Para alcanzar estos objetivos se plantean otros previos que han de cumplirse y que conducirán al principal. Dichos objetivos son:

- Conocer y analizar las principales metodologías existentes aplicables a infraestructuras críticas y a portuarias en particular.
- Definir un criterio para seleccionar las metodologías más adecuadas para el estudio.
- Realizar un análisis comparativo entre las metodologías seleccionadas

- Determinar aspectos novedosos para el análisis del riesgo.
- Proponer nuevos parámetros de relevancia para la evaluación de la seguridad.

El establecimiento de estos objetivos previos corresponde al procedimiento lógico y necesario para la consecución del objetivo principal, dado que cada uno de ellos colabora en la consecución del objetivo principal.

1.3. Estructura del documento

La estructura del documento de esta Tesis Doctoral es la siguiente:

PARTE 1: INTRODUCCIÓN

- Introducción: motivación y razones para la propuesta, objetivos de la Tesis Doctoral y su alcance.
- Estudio de antecedentes: se describen las diferentes situaciones de amenaza que se dan en el entorno portuario, así como el marco regulatorio que afecta a la seguridad en instalaciones portuarias.

PARTE 2: ESTADO DEL CONOCIMIENTO

- Se describen los métodos de evaluación del riesgo existentes, así como la evaluación del riesgo en infraestructuras, describiéndose las principales metodologías de evaluación en infraestructuras críticas. Además se realiza una revisión bibliográfica del estado del arte respecto del marco regulatorio conforme a cinco perspectivas diferentes del riesgo en instalaciones portuarias: riesgos medioambientales y por desastres naturales, riesgos asociados a la mercancía, riesgos asociados a la mercancía, riesgos asociados a la operación y riesgos asociados a las variables políticas de seguridad. Asimismo se describen nuevas metodologías para la evaluación del riesgo en puertos.

PARTE 3: METODOLOGÍA

- Realización por etapas de una propuesta metodológica para la evaluación de la seguridad en instalaciones portuarias, definiéndose asimismo aquellas herramientas y métodos empleados para su consecución.

PARTE 4: RESULTADOS Y CONCLUSIONES

- Se muestran los resultados de la Tesis y se desarrolla un caso de aplicación de la propuesta metodológica a un puerto español.
- Conclusiones y futuras líneas de investigación

Figura 1. Esquema metodológico de la Tesis. Fuente: Elaboración propia

Capítulo 2

Antecedentes

2. ANTECEDENTES

Al término de la Segunda Guerra Mundial el mundo se divide en dos bloques, políticamente hablando, situación que perdura hasta finales de los años ochenta. En esta época se mantiene una situación de continuo ajuste y medida de fuerzas por ambas partes, por la cual los temas de seguridad eran de preocupación fundamentalmente nacionales y su solución se definía por medio de políticas internas y acuerdos interinstitucionales entre las organizaciones de los países.

En la década de los noventa, ciertos temas sociales que involucraban al transporte marítimo, fueron agudizándose, entre ellos, el tráfico ilícito de drogas, armas, y desechos; el contrabando de mercancías fraudulentas, objetos de arte y especies forestales, animales y vegetales protegidas; el tráfico de indocumentados, polizones y personas en peligro rescatadas en alta mar; crecientes actos de piratería y asaltos a tripulantes y pasajeros; enormes pérdidas por mercancías robadas desde los puertos; y otros variados actos ilícitos. Los que antes eran hechos aislados, fueron convirtiéndose en actividades programadas por organizaciones criminales de alta sofisticación y que vinculaban entre sí los tráficos de drogas y armas, con grupos y actos terroristas, lavado de dinero, etc. (Sánchez, García, Manosalva, Rezende, & Sgu, 2004).

Durante los siguientes años noventa, se produjeron múltiples regulaciones internacionales y medidas preventivas, lideradas por organizaciones internacionales, como la Organización Marítima Internacional (OMI), y regionales, como la Organización de Estados Americanos (OEA). Sin embargo, y a pesar de ello el incremento de las actividades delictivas en el ámbito marítimo-portuario continuó en esta década.

Un aspecto importante a considerar es la definición entendida por el término “seguridad”. Para la Organización Marítima Internacional (OMI), el término seguridad marítima corresponde a todos aquellos aspectos relacionados con la “seguridad de la vida humana en el mar”, implicando con ello los aspectos técnicos de construcción de buques, operación y equipamiento de estos, entrenamiento de sus dotaciones, estiba de las cargas a bordo, ayudas a la navegación, cartografía, faros y balizas, servicios de tráfico marítimo de buques, etc. En general, son todos aquellos aspectos que pueden garantizar, dentro de lo posible, una navegación segura de los buques por las áreas de responsabilidad jurisdiccional de los respectivos países. (Sánchez et al., 2004).

El ámbito de interés y por tanto de trabajo de la OMI había sido siempre el buque, y no

los temas portuarios, a excepción hecha de los temas relacionados con mercancías peligrosas, seguridad en la gestión de contenedores, e instalaciones de recepción de residuos provenientes de buques en puertos. Durante los años noventa, la OMI comienza a considerar de interés la interfaz buque-puerto. Esto llevó al desarrollo de un conjunto de recomendaciones, directrices y resoluciones, directa o indirectamente relacionadas con la seguridad y la protección marítima.

Después de los atentados del 11 de septiembre en Nueva York se produjo un cambio en dichos intereses, avanzándose hacia un concepto más amplio de la seguridad, incluyendo en la misma normativa el tema de 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 (22) 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 (PBIP), (INTERNATIONAL MARITIME ORGANIZATION, 2002d).

En materia de seguridad operativa en la actividad portuaria las preocupaciones tradicionalmente abarcaban la prevención y/o el combate de actos ilícitos tales como el tráfico de armas, estupefacientes y, en general, el contrabando de todo tipo de mercancías. Sin embargo, actualmente es necesario prestar atención a otros temas, como por ejemplo el terrorismo, la piratería, etc., algunos de los cuales han entrado dramáticamente en escena en los últimos tiempos, sin que por ello pierdan relevancia los problemas antes mencionados.

A raíz del 11-S la Organización Internacional del Trabajo (OIT) y la OMI crearon un grupo de trabajo con el fin de desarrollar una metodología específica para la estimación del riesgo contra la seguridad en instalaciones portuarias. Este fue el primer paso para que los Estados miembros de dichas organizaciones internacionales dispusieran de una herramienta de estimación del riesgo, desde entonces diferentes países han ido desarrollando su propia metodología y hoy en día se sigue intentando obtener mejoras al resultado que estas ofrecen.

La importancia de la protección del transporte marítimo está determinada por la alta vulnerabilidad de este modo de transporte a los ataques terroristas, dadas las rutas extremadamente diversificadas y el enorme volumen y amplia gama de bienes embarcados, cuyo origen, descripción y propiedad no son siempre perfectamente trazables. Además, cualquier interrupción de la cadena de transporte marítimo debido a las acciones hostiles internacionales puede afectar en gran medida a la economía mundial (Papa, 2013).

Por todas las razones anteriormente mencionadas, la regulación de la seguridad marítima ha pasado a ser uno de los principales temas en la agenda política. En todo el mundo, las organizaciones internacionales, los gobiernos, y el sector privado han

cambiado sus esfuerzos hacia la gestión de los problemas de seguridad, tratando al mismo tiempo de salvaguardar la eficacia operativa. Sin embargo, los esquemas regulatorios heterogéneos que se han introducido, a veces se han superpuesto o incluso han entrado en contradicción entre sí.

Con el objeto de desarrollar los temas correspondientes a los antecedentes expuestos en los párrafos anteriores, el capítulo se centra en dos cuestiones, por una parte la descripción de las principales amenazas para la seguridad en el ámbito de la infraestructura portuaria, y por otra en la descripción del marco regulatorio nacional e internacional para la seguridad en instalaciones portuarias.

2.1. Las amenazas para la seguridad en los puertos

2.1.1. Los polizones y el tráfico ilegal de personas

Este es un problema complejo con un claro trasfondo social y económico. La condición de polizón abarca a aquellos individuos que utilizando el medio de transporte marítimo, buscando mejorar sus condiciones de vida, tratan de emigrar ilegalmente hacia otros destinos, escondidos en el buque o en su carga, sin la autorización del Capitán o del Armador del buque. Otra actividad que lleva a confusión con la anterior, es la práctica insegura asociada al tráfico o transporte deliberado e ilícito de personas indocumentadas. La principal diferencia entre polizones e inmigrantes ilegales, es que en esta última es necesaria participación de terceros, miembros de la tripulación o propietarios del buque o embarcación, quienes se lucran con el transporte ilegal de personas (Sánchez et al., 2004).

El Alto Comisionado de las Naciones Unidas para los Refugiados, (ACNUR), ha indicado la conveniencia en ciertos casos de dar (o al menos considerar) a los polizones el Estatus de Refugiados, con las protecciones correspondientes a la Convención de las Naciones Unidas. En la actualidad el tema, de acuerdo a las estadísticas existentes, ha aumentado su relevancia debido al incremento de los incidentes con polizones a bordo (Sánchez et al., 2004).

Los organismos internacionales relacionados con la materia, han venido instando a las autoridades públicas, administraciones y autoridades marítimo-portuarias, armadores y tripulaciones, a aunar esfuerzos de cooperación, con el fin de que, de la manera más extensa posible y en orden de prever los incidentes que involucren polizones, resolver los casos que los involucren de manera expedita y segura para que las repatriaciones se realicen de la manera más rápida posible, evitando aquellas situaciones en las cuales los polizones deben permanecer a bordo indefinidamente.

En este sentido, la OMI, por medio de su Comité de Facilitación, ha incluido enmiendas al Convenio Internacional sobre Facilitación del Tráfico Marítimo (FAL), donde se indican algunas prácticas y estándares recomendados internacionalmente,

las que fueron aprobadas y entraron en ejecución en el 2003 y que tienen relación con:

- Medidas preventivas a bordo y en tierra;
- Tratamiento de polizones a bordo;
- Recomendaciones sobre desvíos de rutas;
- Desembarco y repatriación de polizones;
- Costos de retorno y gastos de manutención de polizones, entre otros.

Como complemento a las disposiciones del Convenio FAL, la OMI adoptó las Directrices sobre la asignación de responsabilidades para tratar de resolver con éxito los casos de polizones (Resolución A.871 (20) de 1997, y la Resolución A.920 (22) de 2001: “Examen de las medidas de seguridad y los procedimientos de actuación con las personas rescatadas en el mar” (INTERNATIONAL MARITIME ORGANIZATION, 1997, INTERNATIONAL MARITIME ORGANIZATION, 2002).

El tráfico ilegal de personas es de interés en el caso de nuestro país, debido particularmente a la posición geo-política y estratégica que tiene España en el contexto de la Unión Europea. Este es un problema que afecta de forma general a los principales puertos de muchos países occidentales.

Los traficantes generalmente intentan introducir a las personas de forma ilegal en el país mediante su camuflaje en camiones o en contenedores, muchas veces escondidos en dobles fondos. Así se localizaron inmigrantes ilegales en los últimos años. En Enero de 2005, 32 ciudadanos chinos se encontraron en dos contenedores de embarque en el Puerto de Los Ángeles. En general quienes viajan en contenedores los hacen en condiciones miserables. En 2001, la policía irlandesa encontró un contenedor de carga con 8 muertos y 5 inmigrantes enfermos. Del mismo modo, en 2000, la policía británica descubrió 58 ciudadanos chinos en un camión que viajó a Inglaterra en un barco al borde de la muerte por asfixia. Sin embargo el nivel de desesperación de estas personas, dadas las condiciones de vida en sus países de origen es tal, que no parece que el alto riesgo de muerte les disuada de intentar su entrada ilegal a países más desarrollados.

2.1.2.El contrabando marítimo

El contrabando es una de las actividades delictivas más antiguas que existen y que se viene dando en el transporte marítimo desde hace siglos.

La lucha contra el contrabando por parte de los estados viene de lejos y a ella se destinan muchos recursos económicos y humanos. Sin embargo los contrabandistas suelen ir siempre un paso por delante de los agentes de la ley, en el caso español por delante de la Guardia Civil, responsable principal de la lucha contra el contrabando y quien de una forma muy eficiente suele desmontar todos los mecanismos que los

traficantes emplean, si bien en muchas ocasiones los delincuentes consiguen sus objetivos durante un tiempo hasta que son desmontados sus procedimientos (Sánchez et al., 2004).

Si bien el contrabando puede ser de cualquier bien de consumo del cual no es legal su venta en el país o si lo es no paga los pertinentes impuestos al entrar ilegalmente, y por tanto se debe perseguir su entrada al país, en general el tipo de contrabando más perseguido y en el que más esfuerzos se pone por parte del Estado es de forma general el contrabando de drogas, y en especial el de las drogas más duras como la cocaína y la heroína. También se persigue, por su gran demanda, el contrabando de drogas más blandas, si bien, igualmente ilegales como la marihuana o el hachís.

España cuenta con aproximadamente 8.000 km de costa, la entrada de estas drogas se produce mayoritariamente por vía marítima a través de nuestros puertos. Asimismo su proximidad al Magreb y su ubicación estratégica en el Mediterráneo permiten un mejor acceso a la droga en su camino hacia el resto de Europa, que cuenta con múltiples posibilidades de entrada al país.

El contrabando de tabaco supuso por su parte en 2014, solamente en Andalucía, unas pérdidas estimadas de aproximadamente 1.000 millones de euros en impuestos no ingresados y en ventas que se perdieron en los estancos de tabaco legal. Se estima que en el conjunto del Estado las pérdidas por contrabando ascienden a los 1.000 millones de euros.

Una de las mayores dificultades de la lucha contra esta actividad delictiva radica en los ilimitados fondos de que disponen los narcotraficantes y que les permite reponer inmediatamente las pequeñas embarcaciones o conseguir nuevos barcos que trasladen la droga oculta en ellos así como la continua innovación en mecanismos nuevos para ocultarla. Los nuevos contrabandistas son grandes empresarios con formación en comercio internacional y con vínculos mafiosos a lo largo de todo el planeta.

2.1.3. La piratería

La existencia de la piratería se remonta a los inicios del comercio marítimo con plena vigencia en el transporte marítimo en algunas regiones del mundo.

Existe una cooperación mínima entre las naciones para combatir la piratería, y cada país es responsable de hacer cumplir la ley en sus aguas territoriales. Los piratas tienen un buen conocimiento de su entorno operativo. Por lo general, eluden a los funcionarios marítimos cruzando las fronteras marítimas nacionales y aprovechando las vulnerabilidades debido a la falta de intercambio de información y cooperación internacional (Bakir, 2007).

Tanta seriedad reviste este tema que de acuerdo a los estudios realizados por OMI la existencia de estos incidentes se ha incrementado desde mediados de los años

setenta y por ello, conjuntamente con la *International Chamber of Shipping*, se realizaron investigaciones que permitieron destacar que entre 2000 y 2002 fueron 1.270 los reportes de buques atacados por piratas, mientras que en los quince años anteriores se habían reportado 1.587 casos. No obstante, es posible que la cantidad de incidentes sea aún mayor dado que muchos buques no los reportan por razones de pérdida de imagen para el capitán, la compañía y el Estado ribereño, pérdidas de tiempo por investigaciones de las autoridades marítimas y posteriores multas al Capitán del buque, y posible incremento en las primas de los seguros, entre otros (Sánchez et al., 2004).

Según los estudios realizados se ha podido determinar que las zonas de mayor ocurrencia de incidentes de este tipo son las siguientes:

- África Occidental;
- Estrecho de Malaca;
- Mar de la China Meridional e Indonesia y,
- Sudamérica y Caribe.

En África Occidental, los actos de piratería detectados e informados, correspondían a asaltos a buques anclados en puerto, cuya incidencia ha disminuido gracias a las medidas establecidas por el gobierno y las autoridades policiales de Nigeria, país donde se produjeron la mayoría de los casos.

En la década de los noventa, el Estrecho de Malaca tuvo un explosivo incremento en acciones delictivas relacionadas con piratería. Correspondiendo este paso internacional a uno de los de mayor tráfico en el mundo, con más de 200 buques en tránsitos diariamente, la importancia que tiene para el comercio mundial es vital, por lo que la denuncia de 50 casos por año a principio de los noventa impactó severamente a la industria, más aún en un momento en que los mercados productivos de Asia se encontraban en pleno auge. Las acciones utilizadas por los criminales, a diferencia de las tácticas empleadas en África, consistían en abordar los buques en navegación, asaltándolos y robando los valores y cargas detectadas como valiosas. Las medidas adoptadas por los países ribereños y aquellos aspectos técnicos sugeridos por OMI en su Comité de Seguridad Marítima, sobre señales de alarma a bordo de los buques, permitieron que las denuncias de incidentes disminuyeran drásticamente, con un sistema de notificación mucho más efectivo y real (Sánchez et al., 2004).

Respecto del Mar de la China Meridional, se puede indicar que conjuntamente con el deterioro en el Estrecho de Malaca, se iniciaron actividades delictivas en el Mar de China, en algunos aspectos similares al modo de operación de Malaca de ataques a buques en navegación en aguas internacionales, pero agregándose en este caso el ataque a buques pesqueros. No obstante los esfuerzos realizados por OMI y los Estados ribereños, todavía siguen registrándose incidentes. En 1998, la zona registró

36 casos, pasando a 48 en 2002. En el caso de Indonesia, en 1998 registró 38 casos y 110 en 2002.

Por otra parte en Sudamérica y el Caribe, las acciones de los delincuentes se realizaban, al igual que en África, a los buques fondeados en la bahía y algunos atracados en puerto.

Otras áreas del mundo con denuncias de actos de piratería fueron: Bangladesh, India, Mar Rojo y Somalia.

Para contrarrestar estos incidentes, la OMI adoptó varios instrumentos, entre ellos los siguientes:

- Recomendaciones a los Gobiernos para prevenir y reprimir los actos de piratería y robos a mano armada perpetrados contra buques MSC/Circ.622/Rev.1-1999, (INTERNATIONAL MARITIME ORGANIZATION, 1999).
- Directrices para propietarios y armadores de buques, capitanes y tripulaciones sobre la prevención y represión de actos de piratería y robos a mano armada perpetrados contra los buques ,MSC/Circ.623/Rev.3-2002, (INTERNATIONAL MARITIME ORGANIZATION, 2002a).
- Código de prácticas para la investigación de los delitos de piratería y robo a mano armada perpetrados contra los buques, Resolución A 922(22)-2001, (INTERNATIONAL MARITIME ORGANIZATION, 2002c)

No obstante los esfuerzos de OMI y sus Estados miembros, la amenaza de la piratería continúa vigente sobre el comercio internacional en varias regiones del mundo. Con la globalización de los mercados de producción y de consumo, el tráfico marítimo internacional va en aumento, por lo que el transporte de mercancías de importancia para los grupos delictivos también se incrementa. En este sentido, como se expresó anteriormente, la vulnerabilidad “a la viabilidad económica del transporte marítimo y su competitividad” cobra mayor énfasis, por ello la necesidad de sostener un punto de vista común entre los países y diferentes actores relacionados, que permita un mayor compromiso, una mejor evaluación de los riesgos y por ende la adopción de medidas, canalizadas a través de la OMI, de mayor efectividad en el combate de este tipo de actos ilícitos.

2.1.4.El Terrorismo

Aunque existen algunas similitudes, no conviene confundir terrorismo con piratería. El terrorismo marítimo y la piratería son dos fenómenos distintos que existen por diferentes razones, si bien muchas de sus características tienden a superponerse (Brookes, 2009). Esta superposición ha dado lugar a percepciones erróneas acerca de estos conceptos y los peligros que representan para el dominio marítimo amplio y en

gran parte sin gobierno (Nelson, 2012).

Los terroristas a menudo utilizan pequeñas embarcaciones para llevar a cabo ataques contra los buques desprevenidos. De forma similar a los piratas, los terroristas prefieren pequeñas embarcaciones debido a su velocidad y aceleración, maniobrabilidad y capacidad de evadir la detección por radar (Bonadonna, 2011). A diferencia de los piratas sin embargo, los terroristas son menos propensos a abordar el barco. Teniendo en cuenta que los terroristas tienen en general motivaciones políticas más que económicas, son más propensos a destruir la nave para enviar un mensaje político a sus adversarios (Mitchell, Col, Augustine, & Leavenworth, 2007).

Según informe del Secretario General de las Naciones Unidas, (Consejo de Seguridad ONU, 2012), la Resolución 1373 (2001), aprobada por el Consejo de Seguridad de las Naciones Unidas celebrada el 28 de septiembre de 2001, se establece una clara postura frente a amenazas a la paz y la seguridad internacional creadas por actos de terrorismo. La resolución mencionada se sustenta en la profunda preocupación frente al aumento, en varias regiones del mundo, de actos de terrorismo motivados por la intolerancia o el extremismo, e insta a los Estados a trabajar mancomunadamente “para prevenir y reprimir los actos de terrorismo, en particular acrecentando su cooperación y cumpliendo plenamente los convenios internacionales contra el terrorismo que sean pertinentes”, y “reconociendo la necesidad de que los Estados complementen la cooperación internacional adoptando otras medidas para prevenir y reprimir en sus territorios, por todos los medios legales, la financiación y preparación de esos actos de terrorismo¹”.

Dicha Resolución sostiene una condena inequívoca a los ataques terroristas ocurridos en los EUA el 11 de septiembre de 2001, y expresa su determinación de prevenir todos los actos de esa índole, “reafirmando asimismo que esos actos, al igual que todo acto de terrorismo internacional, constituyen una amenaza a la paz y la seguridad internacionales”, como así también el derecho inherente de legítima defensa individual o colectiva reconocido en la Carta de las Naciones Unidas y confirmado en la resolución 1368 (2001).

La Resolución 1373 observa con preocupación la conexión estrecha que existe entre el terrorismo internacional y la delincuencia transnacional organizada, las drogas ilícitas, el blanqueo de dinero, el tráfico ilícito de armas y la circulación ilícita de materiales nucleares, químicos, biológicos y otros materiales potencialmente letales, y a ese respecto pone de relieve la necesidad de promover la coordinación de las iniciativas en los planos nacionales, subregional, regional e internacional, para reforzar la respuesta internacional a este reto y amenaza grave a la seguridad internacional, (Sánchez et al., 2004).

Las posteriores medidas de seguridad y protección marítima y portuaria, como por

¹ Ver texto completo de la Resolución 1373 (2001) del Consejo de Seguridad de la ONU, en: <http://ods-ddsny.un.org/doc/UNDOC/GEN/N01/557/46/PDF/N0155746.pdf?OpenElement>.

ejemplo, el Código PBIP de OMI, reconocen dichas declaraciones como antecedentes válidos para sus resoluciones.

Se puede indicar que los esfuerzos diplomáticos y políticos respecto del terrorismo han sido realizados desde hace años, solo que se comenzaron a concretar con posterioridad al 11 de septiembre, principalmente su tardanza fue debida a la connotación política que el tema del terrorismo reviste y la relación del tema con diferentes tendencias o facciones políticas, religiosas y económicas.

El terrorismo marítimo constituye un medio viable de infligir un "castigo masivo coercitivo" en los enemigos de los terroristas. En este sentido, los cruceros y buques transbordadores de pasajeros (ferris) son especialmente relevantes, en gran parte debido que atienden a un gran número de personas que están confinadas en un solo espacio físico (que, al igual que los aviones, los convierte en lugares ideales para llevar a cabo asaltos destinados a maximizar las bajas civiles) (Chalk, 2008).

Entre los objetivos habituales de los terroristas están (Unnik, 2011):

- Interrupciones en la cadena de suministro, especialmente de suministro de petróleo, con el fin de degradar la economía del mundo occidental
- El contrabando de armas, personas, mercancías y otras sustancias ilícitas para financiar su lucha.
- Células de muyahidines (terrorismo Yihadista), formadas y preparadas para actuar.
- El desarrollo y el despliegue de células terroristas.

La Asamblea General de la Naciones Unidas aprobó la resolución 57/292 en diciembre de 2002, la que reafirma el combate internacional en contra del terrorismo como una de las prioridades de la organización para el periodo 2002-2005 y reafirma el rol de la Oficina de las Naciones Unidas Contra las Drogas y el Crimen (ONUDD). Por medio de este reforzamiento de la ONUDD fue posible establecer el "Programa Global Contra el Terrorismo" donde se apoya el Comité contra el Terrorismo (con su sigla en inglés CTC) como instancia de apoyo a la implementación de la Resolución 1373 del Consejo de Seguridad de ONU, y la complementariedad de la ONUDD (Asamblea General de Naciones Unidas, 2011).

2.1.5.El Bio-terrorismo

Al evaluar las facilidades y libertades existentes actualmente en el comercio internacional global, con centros de producción en diferentes continentes respecto de los centros de consumo, el transporte de mercancías de exportaciones e importaciones, representan un especial riesgo y vulnerabilidad para la comisión de actos ilícitos o maliciosos, que puedan afectar la calidad de dichos productos o en la introducción de agentes biológicos o químicos, con efectos perniciosos sobre la salud

humana en particular y, en general, en la imagen y reputación de los exportadores de origen (Sánchez et al., 2004).

Por otra parte, la posibilidad de introducir agentes biológicos o químicos en un país puede tener efectos insospechados. Se definen armas biológicas (Wikipedia) como “aquellas usadas intencionalmente para causar enfermedades o muerte mediante la difusión de microorganismos o toxinas en los alimentos, aire y el agua, mediante insectos vectores o aerosol. Sus blancos potenciales son las personas, los cultivos y el ganado”.

A diferencia de las armas nucleares, químicas y convencionales, la aparición de un ataque biológico es insidioso. Los recientes incidentes y las investigaciones sobre terrorismo, junto con el creciente número de falsas alarmas (las cuales requieren de similar empleo de recursos que una situación real), han generado un compromiso respecto a la preparación para situaciones de emergencias y el diseño de los respectivos planes de contingencia, así como de la capacidad médica y de salud pública para hacer frente a un ataque biológico.

Debido a la conectividad, movilidad, facilidad y rapidez del transporte de los diferentes agentes, un brote en cualquier lugar del mundo puede considerarse una amenaza para prácticamente todos los países, lo que implica un inmenso esfuerzo sanitario, técnico y financiero para los servicios de salud pública.

Es aterrador pensar que enfermedades infecciosas como las originadas por los virus del SIDA, hantavirus, virus Ébola, entre otros, han tenido a las autoridades de salud pública y al mundo científico con todos sus esfuerzos dedicados a la búsqueda de una pronta respuesta, aunque en algunos casos, sin resultados positivos. Dada la importancia del problema descrito, es evidente que el desarrollo de medidas efectivas que prevengan tal tipo de acciones debe ser una obligación mancomunada de los Estados.

Ibáñez Ferrándiz (2006), afirma en su libro “Bioterrorismo: la amenaza latente”, que durante el otoño de 2001, varias cartas que contenían esporas de *Bacillus anthracis* fueron enviadas a través del sistema postal de los Estados Unidos, originando 22 casos de carbunco (por inhalación y cutáneo), de entre los que fallecieron 5 personas. El primer inicio, de carbunco cutáneo, se presentó a finales de septiembre y el último, de carbunco por inhalación, a mediados de noviembre. De las cuatro cartas que se recuperaron, una estaba remitida a un locutor de noticias de televisión, otra al editor de un periódico, estas dos en Nueva York, y las otras dos a senadores de los Estados Unidos en Washington, DC.

Las cuatro cartas que se recuperaron incluían las palabras “*ALA ES GRANDE*” (“*ALLAH IS GREAT*”) y la fecha “09-11-01”, el día de los ataques con aeronaves contra el *World Trade Center* en Nueva York y el Pentágono en Virginia. El gobierno de los Estados Unidos dictó, en 2002, el Acta sobre Preparación y Respuesta para la

Seguridad de la Salud Pública y Bio-Terrorismo, que ha sido reconocida por su importancia en el tratamiento del problema, aunque hay que destacar que, debido a su condición de extraterritorialidad, la aplicación de la ley en el resto de los países ha producido muchas opiniones contrarias ante la posibilidad de realizar inspecciones en origen y crear algún tipo de barrera para-arancelaria.

2.1.6.El Ciberterrorismo

En julio de 1996, el entonces presidente de los Estados Unidos, Bill Clinton, anunció la formación de la Comisión Presidencial para la Protección de la Infraestructura Crítica (*The President's Commission on Critical Infrastructure Protection*), conocida en inglés por la sigla PCCIP. El fin de ese organismo era estudiar las infraestructuras que constituyen el soporte de la vida cotidiana de Estados Unidos, determinar sus vulnerabilidades ante una amplia gama de amenazas, y proponer una estrategia para protegerlas en el futuro. Así, se identificaron un total de ocho tipos distintos de infraestructuras: telecomunicaciones, bancos y finanzas, energía eléctrica, almacenamiento y distribución de gas y petróleo, aprovisionamiento de agua potable, transportes, servicios de emergencia y servicios gubernamentales.

Según Dorothy E. Denning directora del *Georgetown Institute for Information Assurance* de la Georgetown University, se podría definir el ciberterrorismo así:

"Para calificar como ciberterrorismo, un ataque debe resultar en violencia contra personas o contra la propiedad, o al menos causar el daño suficiente como para generar miedo. Ataques que deriven en muertes o personas heridas, explosiones, colisiones de aviones, contaminación de agua o severas pérdidas económicas pueden ser ejemplos válidos. Serios ataques contra la infraestructura crítica de un país podrían ser actos de ciberterrorismo, dependiendo de su impacto. Los ataques que interrumpen servicios no esenciales o que son básicamente una molestia costosa no entran en esta categoría".

Un buen ejemplo de ciberterrorismo puede ser el control que los terroristas pueden llegar a tener sobre el gobierno de un buque y las consecuencias que podrían derivarse de ello para las instalaciones y para las personas.

2.2. El Marco Regulatorio

Entre las medidas y normativas aprobadas y aplicadas multilateralmente en el ámbito de la seguridad se incluyeron aquellas relativas a los buques e instalaciones portuarias o recomendaciones prácticas sobre la seguridad en los puertos.

Un segundo conjunto de iniciativas para la seguridad se ha introducido en los distintos niveles nacionales con las iniciativas de los Estados Unidos de forma muy significativa. Las medidas estadounidenses comenzaron con iniciativas comunes, tales como la Ley

de Transporte Marítimo (MTSA) de 2002, que involucra tanto a las disposiciones obligatorias como a las voluntarias ISPS (DHS, 2003), y más tarde introdujo una serie de programas de seguridad en capas que se dirigen a tipos específicos de operaciones marítimas. Los principales programas de esta categoría incluyen la Iniciativa de Seguridad de Contenedores (CSI), la Regla del Manifiesto Avanzado de 24 horas (en adelante, la regla de las 24 horas), la Alianza de Aduanas y Comercio contra el Terrorismo (C-TPAT), la Operación Comercio Seguro (OSC), la iniciativa mega-puerto, y la Iniciativa de Seguridad de la Carga (SFA). Excepto la regla de las 24 horas, estos programas y otros más recientes se han codificado en la Ley de Puerto Seguro. Otros programas nacionales incluyen las propias reglas de las 24 horas de Canadá y México.

Las iniciativas también surgieron por parte la Comisión Europea (CE) con el pretexto del Reglamento CE 725/2004 sobre la mejora de los buques y protección de la instalación portuaria, el Reglamento 884/2005 por el que se establecen los procedimientos para efectuar inspecciones en materia de seguridad marítima, y la Directiva 2005/65 / CE se prorrogan las medidas de seguridad de la interfaz buque-puerto a toda la instalación portuaria, (Bichou, K., 2008).

Se resume a continuación la legislación en materia de seguridad en puertos y en infraestructuras críticas de aplicación en el territorio español.

2.2.1. Código Internacional para la Protección de los Buques y las Instalaciones Portuarias (PBIP)

La Organización Marítima Internacional (OMI), desde que fue establecida, se ha dedicado a promover mecanismos de cooperación en el campo de prácticas y regulaciones sobre la actividad naviera dentro del comercio internacional. Es por esta razón que su preocupación se enfoca a la seguridad marítima, la eficiencia de la navegación y la prevención y contención de la contaminación del mar, ocasionada por los buques.

Uno de los convenios dedicados a la seguridad marítima, es el Convenio Internacional para la Seguridad de la Vida Humana en el Mar, SOLAS (*Safety Of Life at Sea*) de 1974, sobre el que adoptó, en diciembre de 2002, una cierta cantidad de enmiendas. La más trascendental es la que se realizó al Capítulo XI por la cual se adopta el nuevo "Código Internacional para la Protección Marítima de los Buques y de las Instalaciones Portuarias, *PBIP*, (ISPS en inglés). El Código consta de dos partes, una con disposiciones obligatorias y otra con recomendaciones.

Antes de las enmiendas, el SOLAS se ocupaba solamente de la seguridad en los transportes marítimos. Las enmiendas y el Código PBIP se ocupan ahora de asuntos de transporte marítimo en relación con buques e instalaciones portuarias.

El Código PBIP (Ministerio de Asuntos Exteriores y Cooperación de España, 2004),

tiene como propósito proporcionar un marco regulatorio y consistente para evaluar riesgos, y evitar que a través de los buques, instalaciones, cargas y pasajeros, se cometan atentados terroristas utilizando como vía al transporte marítimo, permitiendo a los gobiernos aumentar en forma coordinada, a nivel internacional, las medidas de protección necesarias para enfrentar las nuevas amenazas.

Dentro de las medidas dispuestas en el Código PBIP, los buques, las instalaciones portuarias, y las compañías navieras deben designar oficiales de protección, previamente capacitados y acreditados por la autoridad marítima. Además, obliga a los puertos y compañías navieras, a realizar planes de contingencia basados en las evaluaciones de protección, con el fin de evitar potenciales actos terroristas.

La implementación del código se produjo a fecha 1 de julio de 2004, a partir de la cual comenzaron a aplicarse una serie de medidas para reforzar la seguridad marítima y portuaria, incluyendo requerimientos detallados y obligatorios relacionados con la seguridad para gobiernos, autoridades marítimas y compañías navieras junto con una serie de pautas acerca de cómo cumplir con estos requerimientos, incluidos en una segunda sección no obligatoria (Parte B).

En consecuencia, de acuerdo a la disposición, a partir del segundo semestre de 2004, en todo el mundo, solamente los puertos adecuados a la directriz podrían realizar operaciones de exportación e importación. Aquellos puertos y compañías navieras que no cumplan con el Código serían considerados inseguros y los buques que atraquen en sus puertos no podrían entrar en ningún puerto denominado seguro.

El proceso de evaluación de la seguridad de las Instalaciones Portuarias, tiene componentes esenciales. Primero, se debe identificar los componentes críticos en las instalaciones portuarias, luego, la evaluación debe identificar posibles amenazas a las partes críticas con la intención de priorizar las medidas de seguridad y, finalmente, focalizar la vulnerabilidad en las instalaciones portuarias mediante la detección de sus debilidades en seguridad física, integridad estructural, sistemas de comunicación, infraestructura en el transporte, utilidades, y otras áreas de interés.

Los Estados son quienes deben certificar el cumplimiento de las evaluaciones de seguridad en las instalaciones portuarias, para cada puerto de su territorio y para sus buques.

Contenidos de obligado cumplimiento y recomendaciones del Código

Las modificaciones al SOLAS y la Parte A del Código, contienen medidas de aplicación obligatorias, mientras que la Parte B incluye recomendaciones. Todas las medidas se refieren a buques de pasajeros, buques cargueros de más 500 GT, plataformas petroleras e Instalaciones Portuarias (definidas como los lugares donde ocurre la interfaz buque-puerto).

Entre las disposiciones obligatorias, se incluye la obligación de identificar a los buques de manera permanente, relacionada con un sistema de identificación automática (SIA)

y el establecimiento de un sistema de alerta de seguridad, que funcione ante cualquier acción hostil contra el buque. También se dispone la emisión de un documento de registro de la historia de cada buque, denominado “*Continuous Synopsis Record (CSR)*”.

También se dispone la adopción de medidas de seguridad activa y pasiva para tres niveles de protección, cuya implementación debe estar directamente relacionada con la evaluación del riesgo correspondiente. Las medidas y procedimientos de protección se aplicarán en las instalaciones portuarias de modo que, sin perder la necesaria eficacia, se reduzcan al mínimo los inconvenientes o demoras para pasajeros, buques, personal y visitantes de los buques, así como el movimiento de mercancías y servicios.

- **Nivel 1 (normal):** Es el nivel en el que funcionan normalmente los buques e instalaciones portuarias. Deberán mantenerse medidas mínimas de protección en todo momento.
- **Nivel 2 (reforzado):** Se aplicará si hay un incremento del riesgo. Deberán mantenerse medidas de protección suplementarias, derivadas de un incremento del nivel de amenaza.
- **Nivel 3 (excepcional):** Se establece durante el período de tiempo en que sea probable o inminente un suceso que afecte a la protección. Medidas de protección concretas y adicionales, durante determinado tiempo, derivadas de la sospecha o conocimiento de una amenaza grave, probable e inminente.

Los Gobiernos deben determinar el nivel de protección que se aplica en un momento determinado a los buques e instalaciones portuarias, en función de la información disponible. Existen tres niveles de protección:

Para todo esto es necesaria la designación del personal de ejecución de las medidas de seguridad (oficiales de protección de buque, de empresa y de Instalaciones Portuarias), de la preparación de los planes de contingencia que tomen en cuenta las evaluaciones de riesgos (buques e instalaciones portuarias) y de emisión del certificado de seguridad del buque, como así también la supervisión del entrenamiento del resto del personal.

Además se prevé la posibilidad de que un buque sea inspeccionado en puerto o antes de entrar al mismo, por razones de seguridad.

La Parte A del Código establece claramente las responsabilidades y obligaciones de los distintos actores involucrados en la seguridad (Estados miembros, compañías navieras, capitanes e instalaciones portuarias).

Por otro lado, la Parte B del Código, establece una serie de recomendaciones relacionadas con las disposiciones obligatorias. Se solicita a los gobiernos que designen Organizaciones de Protección Reconocidas (OPR), proveedores de servicios

de seguridad para buques en instalaciones portuarias, y puntos de contacto de seguridad marítima regional y nacional, administrar los niveles de seguridad e intercambiar información relacionada con todas las cuestiones de protección marítima.

En general, la Parte B contiene propuestas detalladas acerca de la protección, tanto para buques como para instalaciones portuarias.

2.2.2.Reglamento (CE) nº 725/2004

El 31 de marzo de 2004 el Parlamento Europeo y el Consejo de la Unión Europea adoptaron el Reglamento (CE) no 725/2004, de 31 de marzo de 2004, relativo a la mejora de la protección de los buques y las instalaciones portuarias. Las medidas de protección marítima que impone el Reglamento son sólo una parte de las actuaciones necesarias para alcanzar un grado suficiente de protección a lo largo de las cadenas de transporte que contienen algún componente marítimo. Dicho Reglamento limita su ámbito de aplicación a las medidas de protección a bordo de los buques y en la interfaz inmediata buque-puerto.

Para proteger en el máximo grado posible los sectores marítimo y portuario, conviene introducir en los puertos medidas de protección que cubran cada puerto dentro de los límites definidos por el Estado miembro interesado, y garantizando con ello que las medidas de protección aplicadas en virtud del Reglamento (CE) nº 725/2004 se beneficien de la mayor protección alcanzada en las zonas de actividad portuaria. Estas medidas deben aplicarse a todos los puertos en que existan una o varias instalaciones portuarias sujetas a las disposiciones del Reglamento (CE) nº 725/2004.

El Reglamento tiene por objetivo principal instaurar y aplicar medidas comunitarias que mejoren la protección de los buques utilizados tanto en el comercio internacional como en el tráfico nacional, así como las instalaciones portuarias asociadas a los mismos, frente a la amenaza de actos ilícitos deliberados.

Además, el Reglamento pretende sentar las bases para la interpretación y aplicación armonizadas, así como para el control comunitario, de las Medidas especiales para incrementar la protección marítima aprobadas por la Conferencia Diplomática de la OMI el 12 de diciembre de 2002, que enmiendan el Convenio Internacional para la Seguridad de la vida humana en el mar de 1974 (Convenio SOLAS) e instauran el Código internacional para la protección de los buques e instalaciones portuarias (Código PBIP).

El Reglamento realiza las siguientes consideraciones:

- Los actos ilícitos deliberados y, en especial, el terrorismo figuran entre las amenazas más graves a los ideales de democracia y libertad y los valores de la paz, que constituyen la esencia misma de la Unión Europea.
- Hay que garantizar en todo momento la protección del transporte marítimo de

la Comunidad Europea, la de los ciudadanos que lo utilizan y la del medio ambiente, frente a la amenaza de actos ilícitos deliberados, tales como actos de terrorismo, actos de piratería u otros análogos.

- En el caso del transporte de mercancías que contienen sustancias peligrosas, tales como sustancias químicas y radiactivas, el riesgo que corren los ciudadanos y el medio ambiente de la Unión a causa de actos ilícitos deliberados puede conducir a consecuencias graves.

El 12 de diciembre de 2002, la Conferencia Diplomática de la Organización Marítima Internacional (OMI) aprobó un conjunto de enmiendas al Convenio SOLAS de 1974 para la seguridad de la vida humana en el mar, así como un Código internacional para la protección de los buques y de las instalaciones portuarias (Código PBIP).

Estos instrumentos, con los que se pretende mejorar la protección de los buques utilizados en el comercio internacional y las instalaciones portuarias asociadas a los mismos, contienen disposiciones obligatorias, cuyo ámbito de aplicación en la Comunidad conviene precisar en algunos casos, así como un conjunto de recomendaciones, a algunas de las cuales debe darse carácter obligatorio en la Comunidad.

Sin perjuicio de la reglamentación de los Estados miembros en materia de seguridad nacional y de las medidas que pudieran adoptarse en virtud del Título VI del Tratado de la Unión Europea, para la realización del objetivo de protección presentado en el considerando 2 hay que adoptar medidas útiles en la política de transporte marítimo, estableciendo normas comunes para la interpretación, aplicación y control comunitarios de las disposiciones aprobadas por la Conferencia Diplomática de la OMI el 12 de diciembre de 2002. Conviene asimismo delegar en la Comisión las competencias de ejecución en lo que respecta a las disposiciones detalladas de ejecución.

Más allá de la reglamentación aplicable a los buques destinados al tráfico marítimo internacional y las instalaciones portuarias que les prestan servicio, ha de reforzarse la protección tanto de los buques que realizan viajes nacionales en el interior de la Comunidad como de sus instalaciones portuarias, especialmente en el caso de los buques de pasaje, debido al número de vidas humanas que este tipo de tráfico pone en juego.

La Parte B del Código PBIP contiene determinadas orientaciones a las que interesa dar carácter obligatorio en la Comunidad, a fin de realizar de manera homogénea el objetivo de protección formulado en el considerando 2.

Para contribuir al objetivo reconocido y necesario de fomentar el tráfico marítimo intracomunitario de corto recorrido, se debe invitar a los Estados miembros, en virtud de la Regla 11 de las medidas especiales para incrementar la protección marítima del Convenio SOLAS, a concertar acuerdos de protección para el tráfico marítimo

intracomunitario regular por rutas fijas que utilice instalaciones portuarias específicas, sin menoscabo del nivel general de protección a que se aspira.

Por lo que respecta a las instalaciones portuarias situadas en puertos que sólo ocasionalmente presten servicio al tráfico marítimo internacional, podría resultar desproporcionada una aplicación permanente de todas las reglas de protección contenidas en el presente Reglamento. Incumbe a los Estados miembros determinar, en función de las pertinentes evaluaciones de protección, los puertos que se encuentren en tales circunstancias, así como las medidas alternativas que puedan proporcionar un nivel de protección adecuado.

2.2.3. Directiva 2005/65/CE

Muchas de las Infraestructuras Críticas pertenecen o están en manos privadas. La ola de liberación en la prestación de servicios y funciones tradicionalmente proporcionadas por los gobiernos nacionales ha cambiado el panorama de la regulación.

En muchos países europeos, el suministro de energía, comunicación, atención de la salud, los servicios financieros y el transporte ha sido privatizado total o parcialmente, (Fritzon, A., Ljungkvist, K., Boin, A., Rhinard, 2007), esto mismo sucede con numerosos puertos en Europa.

La finalidad principal de la Directiva 2005/65/CE es introducir medidas comunitarias orientadas a aumentar la protección de los puertos frente a la amenaza de sucesos que afecten a la protección marítima.

Asimismo, la Directiva hará que las medidas de protección adoptadas en aplicación del Reglamento (CE) nº 725/2004 se beneficien de la mayor protección alcanzada en las zonas portuarias adyacentes.

Las medidas a las que se hace referencia consistirán en:

- a) Reglas básicas comunes en relación con las medidas de protección portuaria;
- b) Un mecanismo de aplicación de dichas reglas;
- c) Mecanismos adecuados de vigilancia del cumplimiento de las citadas reglas.

La Directiva realiza las siguientes consideraciones:

- Las personas, infraestructuras y equipos en los puertos deben protegerse contra los sucesos que afectan a la protección marítima y sus devastadores efectos. Esta protección redundaría en beneficio de los usuarios del transporte, la economía y la sociedad en su conjunto.
- La realización del objetivo de protección de la Directiva requiere aplicar medidas útiles, sin perjuicio de la normativa de los Estados miembros en el área de la seguridad nacional y de las iniciativas que puedan adoptarse en

virtud del título VI del Tratado de la Unión Europea.

- Los Estados miembros deben basarse en evaluaciones de protección detalladas para definir con precisión los límites de las zonas portuarias pertinentes para la protección, así como las diferentes medidas necesarias para garantizar la adecuada protección de los puertos.

Dichas medidas deben variar según el nivel de protección en vigor y reflejar las diferencias en el perfil de riesgo de las distintas subzonas portuarias.

Los Estados miembros deben aprobar planes de protección portuaria que incorporen las conclusiones de las evaluaciones de protección portuaria. La eficacia de las medidas de protección requiere también una división de tareas nítida entre todas las partes involucradas, así como la realización de prácticas a intervalos periódicos. Se considera que la nítida división de tareas y las prácticas en el plan de protección portuaria contribuirá en gran medida a la eficacia de las medidas de protección preventivas y correctoras.

Los buques de transbordo rodado son especialmente vulnerables a sucesos que afectan a la protección marítima, en especial si transportan pasajeros y carga. Se deben adoptar medidas adecuadas, sobre la base de evaluaciones de riesgo, para asegurarse de que los automóviles y vehículos de mercancías que embarquen para ser transportados en buques de transbordo rodado en rutas tanto nacionales como internacionales no entrañan riesgo para el buque, sus pasajeros, tripulación, ni carga. Dichas medidas deben adoptarse de un modo que dificulte lo menos posible la fluidez de las operaciones.

Los Estados miembros deben poder establecer comités de protección portuaria encargados de prestar asesoramiento práctico en los puertos a que se aplica la Directiva.

Los Estados miembros han de velar por que todos los interesados sean claramente conscientes de sus responsabilidades en relación con la protección portuaria. Los Estados miembros deben vigilar el cumplimiento de las reglas de protección y establecer una autoridad con competencia clara sobre todos sus puertos, aprobar todas las evaluaciones y planes de protección portuaria, fijar y comunicar en caso pertinente los niveles de protección y velar por que las medidas sean comunicadas, aplicadas y coordinadas correctamente.

Los Estados miembros deben aprobar las evaluaciones y planes y vigilar su aplicación en sus puertos. Con el fin de perturbar lo menos posible el funcionamiento de los puertos y reducir al mínimo la carga administrativa de los organismos de supervisión, la vigilancia de la aplicación de la Directiva por parte de la Comisión deberá llevarse a cabo junto con las inspecciones establecidas en el artículo 9, apartado 4, del Reglamento (CE) nº 725/2004.

Los Estados miembros deben garantizar la presencia de un punto de contacto para la protección portuaria entre ellos y la Comisión. Deben informar a la Comisión de los puertos a los que afecte la presente Directiva a partir de las evaluaciones de protección llevadas a cabo.

La aplicación efectiva y normalizada de las medidas que configuran esta política plantea grandes interrogantes en relación con su financiación. La financiación de algunas medidas de seguridad complementarias no debe dar lugar a distorsiones de la competencia. Para el 30 de junio de 2006, a más tardar, la Comisión debe presentar al Parlamento Europeo y al Consejo los resultados de un estudio acerca de los costes inherentes a las medidas adoptadas con arreglo a la presente Directiva, que se ocupe, en particular, del modo en que se reparte la financiación entre las autoridades públicas y los operadores.

La presente Directiva respeta los derechos fundamentales y observa los principios reconocidos, en particular, por la Carta de Derechos Fundamentales de la Unión Europea.

Procede aprobar las medidas necesarias para la ejecución de la presente Directiva con arreglo a la Decisión 1999/ 468/CE del Consejo, de 28 de junio de 1999, por la que se establecen los procedimientos para el ejercicio de las competencias de ejecución atribuidas a la Comisión.

Conviene prever un procedimiento de adaptación de la presente Directiva que permita tener en cuenta la evolución de los instrumentos internacionales y, a la luz de la experiencia, adaptar o completar las disposiciones detalladas de sus anexos sin que ello implique extensión de su ámbito de aplicación.

Dado que los objetivos de la presente Directiva, a saber, la instauración equilibrada de medidas útiles en las políticas marítima y portuaria, debido a la dimensión europea de la presente Directiva no pueden ser alcanzados de manera suficiente por los Estados miembros y pueden lograrse por ello mejor a nivel comunitario, la Comunidad puede adoptar medidas, conforme al principio de subsidiariedad consagrado en el artículo 5 del Tratado. De conformidad con el principio de proporcionalidad enunciado en el mismo artículo, la presente Directiva no excede lo necesario para alcanzar dichos objetivos.

En su Artículo 6, Evaluación de la protección portuaria, dice:

1. Los Estados miembros velarán por que se efectúe una evaluación de la protección de los puertos a los que se aplique la presente Directiva. Dichas evaluaciones reflejarán debidamente las peculiaridades de las distintas partes del puerto, así como, cuando las autoridades pertinentes de los Estados miembros lo consideren necesario, de sus zonas adyacentes si éstas tienen una incidencia en la protección del puerto, y las evaluaciones de las

instalaciones portuarias que se encuentren dentro de sus límites efectuadas de conformidad con el Reglamento (CE) nº 725/2004.

2. Toda evaluación de protección portuaria deberá efectuarse teniendo en cuenta, como mínimo, las prescripciones detalladas que figuran en el anexo I.
3. Las evaluaciones de protección portuaria podrán ser efectuadas por una organización de protección reconocida
4. Las evaluaciones de protección portuaria deberán ser aprobadas por el Estado miembro interesado.

En el Anexo I se indica que:

La evaluación de la protección portuaria es el fundamento de la elaboración del plan de protección portuaria y de su posterior ejecución. Dicha evaluación cubrirá, como mínimo, lo siguiente:

- Identificación y evaluación de los bienes e infraestructuras que es importante proteger,
- Determinación de las posibles amenazas a esos bienes e infraestructuras y de la probabilidad de que se concreten, a fin de establecer medidas de protección y una jerarquización de las mismas,
- Determinación, selección y jerarquización de las contramedidas y cambios de procedimiento y de su grado de eficacia para reducir la vulnerabilidad,
- Determinación de los puntos débiles, incluidos los relacionados con el factor humano, en las infraestructuras, políticas y procedimientos.

2.2.4. Real Decreto 1617/2007

Del texto de dicho Real Decreto (Ministerio de la Presidencia de España, 2007) se desprende que: la Organización Marítima Internacional (OMI) adoptó, en la Conferencia de los Gobiernos contratantes del Convenio Internacional para la seguridad de la vida humana en el mar de 1974, SOLAS, (Organización Marítima Internacional, 2002), celebrada del 9 al 13 de diciembre de 2002, un conjunto de resoluciones dirigidas a regular la mejora de la protección del transporte marítimo. Entre ellas cabe destacar la Resolución 1, enmiendas al Convenio SOLAS que afectan al capítulo V y XI, publicada en el Boletín Oficial del Estado el 22 de abril de 2004, y la Resolución 2, por la que se adopta un Código Internacional para la protección de los buques y de las instalaciones portuarias (Código PBIP), publicada en el BOE el 21 de agosto de 2004. Estos instrumentos pretenden mejorar la protección de los buques utilizados en el comercio internacional y la protección de las instalaciones portuarias asociadas a los mismos a través de una interfaz buque-puerto e incluyen disposiciones de obligado cumplimiento (las enmiendas al Convenio SOLAS y la Parte A del Código

PBIP), y otras de carácter no obligatorio (la Parte B del Código PBIP) cuya aplicación se recomienda para facilitar el cumplimiento de las citadas disposiciones obligatorias. Estas normas fueron aceptadas en enero de 2003 y entraron en vigor el 1 de julio de 2004 para todos los Gobiernos contratantes del Convenio SOLAS.

Por otra parte, la Unión Europea tiene encomendada la regulación de cuantas medidas sean necesarias para garantizar en todo momento la protección del transporte marítimo contra los actos ilícitos deliberados, en especial el terrorismo, que figuran entre las amenazas más graves contra los ideales de democracia y libertad y los valores de paz, que constituyen la esencia misma de la comunidad europea. Con objeto de desarrollar medidas útiles en la política del transporte marítimo y establecer normas comunes para la interpretación, aplicación y control comunitarios de las disposiciones adoptadas por la citada Conferencia diplomática celebrada en la OMI en diciembre de 2002, la Unión Europea aprobó el Reglamento (CE) nº 725/2004 del Parlamento y del Consejo, de 31 de marzo de 2004, relativo a la mejora de la protección de los buques y de las instalaciones portuarias.

Los requisitos establecidos en el Reglamento (CE) nº 725/2004 han sido aplicados a los buques autorizados a enarbolar el pabellón español obligados a cumplir esta normativa, así como a las instalaciones portuarias afectadas, en el vigente marco de concurrencia de competencias que los distintos organismos y entidades tienen asignadas en el entorno de la protección de los buques y de las instalaciones portuarias. Este reglamento confirma la obligatoriedad de la aplicación, en el ámbito marítimo europeo de los buques y de las instalaciones portuarias, de las enmiendas al Convenio SOLAS y de la Parte A del Código PBIP, que el reglamento incluye en sus anexos, y también declara de obligado cumplimiento determinadas medidas que la Parte B de dicho Código PBIP recoge como meras recomendaciones. Asimismo, el reglamento establece determinadas obligaciones para los Estados miembros en materia de mejora de la protección marítima de los buques, sus compañías y las instalaciones portuarias, tales como la identificación de las autoridades designadas y las Administraciones, la asignación de responsabilidades, la coordinación, transmisión de información, y tareas de control de la aplicación de la normativa, estableciéndose un sistema de control por parte de la Comisión Europea para verificar el grado de cumplimiento en esta materia por los Estados miembros.

La Unión Europea ha considerado que el Reglamento (CE) nº 725/2004 constituye solamente un conjunto parcial del total de las medidas necesarias para adquirir un adecuado nivel de protección para las cadenas de transporte ligadas al transporte marítimo y para las personas, infraestructuras y equipamiento contra incidentes relacionados con la protección, pues el alcance de tal reglamento se circunscribe a las medidas de protección aplicables a los buques y a la inmediata interfaz buque-puerto. Por ello, y con el objeto de conseguir la mayor protección posible para la industria marítima y portuaria, ha estimado necesario introducir medidas de protección

adicionales, aplicables al resto de las zonas portuarias, en la extensión que, en cada caso y tras la correspondiente evaluación de riesgos se considere pertinente, incluyendo el análisis de los posibles riesgos de amenazas contra la protección portuaria que pudieran tener su origen en determinadas zonas exteriores y contiguas al puerto, y todo ello sin perjuicio de la normativa específica vigente en cada Estado miembro en el área de la seguridad nacional.

Este real decreto transpone la Directiva 2005/65/CE al ordenamiento jurídico español y desarrolla las medidas que en ella se recogen, en particular las relacionadas con el establecimiento de unas reglas básicas aplicables al sistema portuario español, la definición de un mecanismo para la aplicación de dichas reglas y el diseño e implantación de los adecuados mecanismos de monitorización de su cumplimiento. Considerando que en materia de protección portuaria confluyen competencias de diferentes entidades y organismos, que han de ejercerse en coordinación con las que las Fuerzas Armadas tienen atribuidas en relación con la vigilancia y la seguridad de los espacios marítimos en virtud de la Ley Orgánica 5/2005, de 17 de noviembre, de Defensa Nacional, es necesario, igualmente, crear estructuras consultivas a nivel local para el asesoramiento en el análisis y la definición de aspectos relacionados con la protección de los buques, de las instalaciones portuarias y de los puertos, lo que permitirá la armonización de criterios y la implantación coordinada de los requisitos establecidos en el ámbito de aplicación de este real decreto. Es destacable, además, la inclusión de procedimientos y directrices encaminados a lograr la necesaria coordinación entre los agentes involucrados en la aplicación de la normativa, la mejora de la agilidad en la transmisión de información para la adecuada toma de decisiones, la armonización de criterios y métodos aplicables en el diseño del sistema de gestión de la protección del transporte marítimo, su implantación, la verificación de su eficiencia, los mecanismos de mejora continuada, y las labores de supervisión y control de su aplicación.

Por último, la experiencia derivada de la aplicación de la normativa relacionada con la mejora de la protección de los buques y de las instalaciones portuarias aconseja incluir en este real decreto diversos aspectos que facilitan la armonización de las disposiciones incluidas en el Reglamento (CE) nº 725/2004, con las de la Directiva 2005/65/CE, en especial en la determinación de los órganos competentes para la aplicación de las medidas previstas en las mismas.

2.2.5. Directiva Comunitaria 2008/114/CE

Tal y como se desprende del texto de la Directiva (Consejo de Europa, 2008), en junio de 2004 el Consejo Europeo solicitó la elaboración de una estrategia global para mejorar la protección de infraestructuras críticas. En respuesta a esa solicitud, el 20 de octubre de 2004 la Comisión adoptó la Comunicación sobre protección de las infraestructuras críticas en la lucha contra el terrorismo, en la que se formulan

propuestas para mejorar la prevención, preparación y respuesta de Europa frente a atentados terroristas que afecten a infraestructuras críticas.

A partir de entonces se suceden una serie de avances en materia de infraestructuras críticas. Así y tras la adopción del Libro Verde de las infraestructuras críticas, en diciembre de 2005, el Consejo de Justicia y Asuntos de Interior pidió a la Comisión que elaborara una propuesta para un programa europeo de protección de las infraestructuras críticas (el PEPI) y decidió que debería basarse en un planteamiento que tuviera en cuenta todo tipo de riesgo pero que diera preferencia a la lucha contra amenazas terroristas.

Posteriormente, en abril de 2007 el Consejo adoptó conclusiones sobre el PEPIC, en las que reiteró que correspondía en última instancia a los Estados miembros gestionar las disposiciones de protección de infraestructuras críticas dentro de sus fronteras nacionales, aunque acogiendo con satisfacción los esfuerzos de la Comisión para desarrollar un procedimiento europeo de identificación y designación de infraestructuras críticas europeas (las ICE) y de evaluación de la necesidad de mejorar su protección.

En toda las ICE designadas deben existir planes de seguridad del operador o medidas equivalentes que incluyan la identificación de los elementos importantes, una evaluación de riesgos y la identificación, selección y orden de preferencia de las contramedidas y procedimientos. A fin de evitar trabajos inútiles y duplicaciones de esfuerzo, cada Estado miembro debe evaluar en primer lugar si los propietarios u operadores de las ICE designadas tienen planes de seguridad del operador o medidas equivalentes. En caso de que no existan tales planes, cada Estado miembro intervendrá oportunamente para asegurarse de que se ponen en marcha las medidas adecuadas. Corresponderá a cada Estado miembro decidir el modo de actuación más adecuado en relación con la elaboración de planes de seguridad del operador.

La Directiva define "infraestructura crítica" como el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones;

Asimismo se define "infraestructura crítica europea" o "ICE", la infraestructura crítica situada en los Estados miembros cuya perturbación o destrucción afectaría gravemente al menos a dos Estados miembros. La magnitud de la incidencia se valorará en función de criterios horizontales, como los efectos de las dependencias intersectoriales en otros tipos de infraestructuras.

2.2.6.Ley 8/2011 de Infraestructuras Críticas

Según reza el preámbulo de la Ley 8/2011 de 28 de abril, (BOE núm. 102, 2011), por la que se establecen medidas para la protección de las infraestructuras críticas, dentro de las prioridades estratégicas de la seguridad nacional se encuentran las infraestructuras, que están expuestas a una serie de amenazas. Para su protección se hace imprescindible, por un lado, catalogar el conjunto de aquéllas que prestan servicios esenciales a nuestra sociedad y, por otro, diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

En la actualidad, la entrada en vigor de la Directiva 2008/114, del Consejo, de 8 de diciembre, sobre la identificación y designación de Infraestructuras Críticas Europeas y la evaluación de la necesidad de mejorar su protección (en adelante, Directiva 2008/114/CE), constituye un importante paso en la cooperación en esta materia en el seno de la Unión. En dicha Directiva se establece que la responsabilidad principal y última de proteger las infraestructuras críticas europeas corresponde a los Estados miembros y a los operadores de las mismas, y se determina el desarrollo de una serie de obligaciones y de actuaciones por dichos Estados, que deben incorporarse a las legislaciones nacionales.

Las actuaciones necesarias para optimizar la seguridad de las infraestructuras se enmarcan principalmente en el ámbito de la protección contra agresiones deliberadas y, muy especialmente, contra ataques terroristas, resultando por ello lideradas por el Ministerio del Interior.

La finalidad de la ley es la del establecimiento de medidas de protección de las infraestructuras críticas que proporcionen una base adecuada sobre la que se asiente una eficaz coordinación de las Administraciones Públicas y de las entidades y organismos gestores o propietarios de infraestructuras que presten servicios esenciales para la sociedad, con el fin de lograr una mejor seguridad para aquéllas.

Sobre esta base, se sustentarán el Catálogo Nacional de Infraestructuras Estratégicas (conforme a la comunicación del Consejo de la Unión Europea de 20 de octubre de 2004, que señala que cada sector y cada Estado miembro deberá identificar las infraestructuras que son críticas en sus respectivos territorios) y el Plan Nacional de Protección de Infraestructuras Críticas, como principales herramientas en la gestión de la seguridad de nuestras infraestructuras.

La Ley consta de 18 artículos, estructurados en 3 Títulos. El Título I se destina a las definiciones de los términos acuñados por la Directiva 2008/114/CE, así como a establecer las cuestiones relativas al ámbito de aplicación y objeto. El Título II se dedica a regular los órganos e instrumentos de planificación que se integran en el Sistema de Protección de las Infraestructuras Críticas. El Título III establece,

finalmente, las medidas de protección y los procedimientos que deben derivar de la aplicación de dicha norma. Asimismo, la Ley consta de cuatro Disposiciones Adicionales y cinco Disposiciones Finales.

En base a estas necesidades se considera de gran interés la mejora en el conocimiento de los riesgos que afectan a la seguridad de los puertos españoles.

2.2.7.Organización Internacional del Trabajo y Organización Marítima Internacional (OIT/OMI)

La Organización Internacional del Trabajo (OIT), también se ha involucrado activamente en el cuidado y mejora de la protección marítima y portuaria. Las principales acciones en tal sentido se refieren especialmente a los documentos de identidad de la gente de mar (C 185) y el “*Repertorio de Recomendaciones Prácticas sobre Protección en los Puertos*”(Organización Marítima Internacional & Organización Internacional del Trabajo, 2003).

El antecedente del C 185 data de 1958, y se ha considerado necesario proceder a su revisión con el objeto de dotar a la gente de mar de un “documento de identidad mundial uniforme que permita identificar (los) de manera segura y verificable...”².

También se reconoce la necesidad de extremar el cuidado de los procedimientos de emisión de los documentos de identificación, a los efectos de evitar el riesgo de que aquellos sean entregados a quienes no deben recibirlo, como así también se destaca la importancia de contar con una base de datos internacional que sea de acceso libre a personas autorizadas de modo tal que puedan consultarse informaciones relacionadas con los documentos emitidos (Sánchez et al., 2004).

Con respecto al “*Repertorio de Recomendaciones Prácticas sobre Protección en los Puertos*”, su elaboración fue dispuesta en forma conjunta por la OIT y OMI durante el primer semestre de 2003, estableciéndose mecanismos de consulta y participación de gobiernos, empleadores y trabajadores para el dictado de su documento final. Al momento de redacción del presente informe, el mencionado documento final está siendo discutido por ambas Organizaciones internacionales, razón por la cual no es posible presentar una descripción final del mismo (Sánchez et al., 2004).

En líneas generales, las recomendaciones están destinadas a orientar a los responsables de la protección portuaria, facilitando la identificación de tareas y responsabilidades a gobernantes, empleadores y trabajadores. Las recomendaciones no tienen por objeto reemplazar a las legislaciones nacionales, ni alterar los órdenes establecidos para las relaciones entre las partes en cada país. Sin embargo, este conjunto de recomendaciones no vinculantes contribuirán a mejorar la protección portuaria en un todo de acuerdo con los principios establecidos por el Código PBIP.

² OMI-OIT (2003); “Repertorio de Recomendaciones Prácticas Sobre Protección en los Puertos”; OIT, Ginebra.

Capítulo 3

Estado del Conocimiento

3. ESTADO DEL CONOCIMIENTO

3.1. Métodos de evaluación del riesgo

Atendiendo a la complejidad del método y a la gravedad del posible accidente, se puede definir una primera clasificación de Métodos de Evaluación del Riesgo (Romero Rubio J.C., 2004):

- a) *Métodos simplificados*. Se emplean cuando es razonable no esperar consecuencias catastróficas de la actualización del riesgo, permitiendo obtener una primera aproximación suficiente para llevar a cabo una jerarquización de los riesgos y en consecuencia determinar la priorización de las actuaciones preventivas a tomar. Cuantifican el riesgo empleando escalas numéricas relativas. No requieren un conocimiento muy profundo de los aspectos técnicos de las instalaciones y por ello son los empleados de forma general en las evaluaciones de riesgos.
- b) *Métodos complejos*. Se emplean cuando las consecuencias de la actualización de los riesgos puede llegar a ser muy grave aunque su probabilidad de ocurrencia sea menor o cuando la estimación precisa del riesgo exige la utilización de dispositivos complicados, técnicas de muestreo y conocimientos de nivel de formación superior. Suelen requerir conocer a fondo las instalaciones y equipos de trabajo y son más difíciles de aplicar.

Asimismo, y según este autor, atendiendo al aspecto cuantitativo de los resultados que se pueden obtener de la estimación del riesgo por unidad de tiempo, se podría realizar otra clasificación:

- a) *Métodos cualitativos*. La estimación que se obtiene es de tipo cualitativo.
- b) *Métodos cuantitativos*. La estimación que se obtiene es de tipo cuantitativo.

Si bien, los métodos cuantitativos se pueden emplear de forma cualitativa y los cualitativos de forma semi-cuantitativa. Por otra parte, mientras que los simplificados pueden usarse de forma cualitativa, los complejos pueden ser cuantitativos, semi-cuantitativos o cualitativos.

Se exponen a continuación de forma resumida los principales métodos existentes.

3.1.1. Métodos simplificados de evaluación del riesgo

Estos métodos contemplan la aceptación de criterios sencillos para la determinación de los tipos de accidentes posibles y sus alcances. Se clasifican en base al número de factores que proponen para la estimación de daño esperado.

3.1.1.1. Valoración simple o método ABC

La forma más sencilla de clasificar el riesgo consiste en hacerlo en base a un único parámetro, identificando previamente los peligros existentes, y se clasifican como A, B, o C, (Rubio Romero, J. C., & Rubio Gámez, M., 2005).

- A serían aquellos riesgos cuya actualización podría causar muertes, lesiones graves con incapacidades permanentes o una gran pérdida en bienes,
- B serían aquellos riesgos cuya actualización podría causar lesiones graves con baja o daños a la propiedad.
- C serían aquellos riesgos cuya actualización podría causar lesiones leves o daños a la propiedad escasos.

Este método carece de una metodología de identificación de los riesgos, y por tanto la valoración del riesgo es inmediata debido a su gran simplificación.

3.1.1.2. Método binario. INSHT, 1996

Un mismo accidente puede producir diferentes daños y de diferente magnitud (Romero Rubio J.C., 2004). La esperanza del daño de un determinado riesgo será el promedio de los daños a que daría lugar el accidente si este se repitiera un número representativo de veces, y por tanto cada uno de los niveles de daño a los que el accidente puede dar lugar tendrá asociada una frecuencia de ocurrencia asociada. Si llamamos D_i al nivel de daños del accidente “ i ”, y f_i a la frecuencia de ocurrencia del daño D_i a consecuencia del accidente “ i ” de los “ n ” accidentes representativos, la esperanza de daño como consecuencia de un accidente sería:

$$D = \sum_{i=1}^n f_i * D_i$$

Como se aprecia, se consideran por tanto dos factores para la valoración del riesgo de daño. Asimismo la valoración de cada uno de estos dos factores se realiza en base a tres valores cualitativos.

El INSHT se inspira en normas como la NORMA UNE-EN-1050 sobre los principios para la evaluación del riesgo en las máquinas, que es un método binario, y que especifica:

“El riesgo asociado a una situación o proceso técnico particular se deriva de una combinación de los siguientes elementos”:

- La gravedad del daño
- La probabilidad de que se produzca dicho daño, que es función de:
 1. La frecuencia y la duración de la exposición de las personas al peligro.
 2. La probabilidad de que ocurra un suceso peligroso
 3. Las posibilidades técnicas y humanas para evitar o limitar el daño.

Para calcular la magnitud del riesgo, el método binario del INSHT funde ambos factores, “severidad” y “probabilidad”, en uno solo que denomina “Nivel de riesgo”, utilizando la tabla 1 para a continuación, y a partir de dichos niveles de riesgo definir la base para decidir si requiere mejorar los controles existentes o implantar otros nuevos, así como la urgencia para llevar a cabo las acciones a tomar. En definitiva valora el riesgo.

Tabla 1. Niveles de riesgo en función de la probabilidad y las consecuencias

Probabilidad	Consecuencias		
	Ligeramente dañino	Dañino	Extremadamente dañino
Baja	Riesgo trivial	Riesgo tolerable	Riesgo moderado
Media	Riesgo tolerable	Riesgo moderado	Riesgo importante
Alta	Riesgo moderado	Riesgo importante	Riesgo intolerable

Fuente: INSHT (1996)

3.1.1.3. Método de William T. Fine

Este método, (Fine, 1971) consiste en un método de evaluación matemática para control de riesgos. Se diferencia fundamentalmente del método binario en que considera tres factores. Su autor descompone la probabilidad en dos factores, cuyo resultado final será equivalente a la probabilidad definida en el método binario.

Constituye el sistema clásico de valoración del riesgo que ha servido de modelo para otros sistemas posteriores. El método Fine se utiliza una vez identificados los factores de riesgo mediante el empleo de listas de comprobación. Sirve para determinar:

1. El grado de peligrosidad de los riesgos detectados.
2. Las actuaciones recomendadas para corregir el riesgo.
3. La justificación de la inversión económica necesaria para ello.

Determinación del grado de peligrosidad

El grado de peligrosidad del riesgo, o riesgo, se calcula mediante la siguiente fórmula:

$$\text{Riesgo} = \text{probabilidad} \times \text{exposición} \times \text{consecuencias}$$

Los conceptos que contempla son:

- a) Probabilidad. La posibilidad que, una vez presentada la situación de riesgo, se origine el accidente. Habrá que tener en cuenta la secuencia completa de acontecimientos que desencadenan el accidente.
- b) Exposición. Es la frecuencia con que se presenta la situación de riesgo. Siendo tal, que el primer acontecimiento indeseado iniciará la secuencia del accidente.
- c) Consecuencias. Se definen como el daño, debido al riesgo que se considera más grave posible, incluyendo desgracias personales y daños a la propiedad.

Para el desarrollo del método, se utiliza unos cuadros de cuantificación, los cuales resultan después de realizar una serie de pruebas; hechas por el autor. Estas permiten, en primer lugar, hallar un valor de riesgo, para posteriormente calcular la justificación o no de la inversión propuesta. La puntuación que se atribuye a los distintos elementos es la siguiente:

Tabla 2. Cuadros de cualificación de riesgos

FACTOR DE RIESGO	SUPUESTOS	VALOR
CONSECUENCIAS (resultado probable de un accidente potencial)	1. Catástrofe. Numerosas muertes. Daños superiores a 901,518,16 €	100
	2. Varias muertes. Daños de 450.759 € y 901,518,16 €	50
	3. Muerte y daños entre 90.151,82 € y 450.759 €	25
	4. Lesiones muy graves o daños entre 901,52 € y 90.151,82 €	15
	5. Lesiones con baja y daños de hasta 901,52 €	5
	6. Heridas leves, contusiones , pequeños daños materiales	1
EXPOSICIÓN	1. Muy alta: ocurre continuamente	10
	2. Alta: ocurre frecuentemente (al menos una vez al día)	6
	3. Ocasional: de una vez por semana a una vez por mes	3
	4. Irregularmente: de una vez al mes a una vez al año.	2
	5. Rara: se sabe que alguna vez ha ocurrido.	1
	6. Remota: no se conocen casos de accidentes similares	0,5
PROBABILIDAD de que el accidente ocurra.	El accidente se producirá: 1. Con toda probabilidad si la situación de riesgo tiene lugar	10
	2. Posiblemente (probabilidad mayor del 50%)	6
	3. Posibilidad escasa	3
	4. Coincidencia muy rara, se sabe que alguna vez ha ocurrido.	1
	5. Nunca ha ocurrido en muchos años, pero podría suceder.	0,5
	6. Es prácticamente imposible que ocurra	0,1

Fuente: Fine, W.T. (1971)

Actuación recomendada para corregir el riesgo

Según la valoración asignada al grado de peligrosidad, se recomienda adoptar una de las siguientes medidas:

Tabla 3. Grado de peligrosidad

Grado de peligrosidad	Actuación recomendada
Igual o mayor a 200 puntos	Corrección inmediata del riesgo. La actividad debe detenerse hasta que se elimine.
Entre 85 y 199	Actuación preventiva urgente.
Inferior a 85	El riesgo debe eliminarse, pero la situación no es de emergencia.

Fuente: Fine, W.T. (1971)

La puntuación obtenida permite ordenar los factores de riesgo detectados según su gravedad, es decir, establecer una relación de prioridades en la actuación preventiva a iniciar.

Justificación de la inversión

Una vez decidido el riesgo a eliminar o reducir, habrá que proceder a efectuar las inversiones necesarias para ello. Si son varias las posibilidades de actuación y su coste es diferente, Fine propone una fórmula que permita seleccionar la opción económicamente más razonable.

$$J = R / (FC \times GC)$$

Siendo:

J = Justificación de la Inversión.

R = Valor del Riesgo.

FC = Factor de coste.

GC = Grado de Corrección.

El factor de coste indica el valor aproximado de la inversión necesaria para suprimir o reducir el riesgo. Fine establece una escala de valoración entre 0,5 y 10 puntos.

El grado de corrección se puntúa según la eficacia de la medida adoptada con valores comprendidos entre 1 y 5 puntos

La fórmula propuesta para la justificación de la inversión permite obtener un valor numérico que sirve de orientación a la empresa para decidir sobre sus inversiones en seguridad.

- Si $J > 20$; Muy justificado.
- Si $10 < J < 20$ Probable Justificación
- Si $J < 10$ No justificado

3.1.1.4. Métodos de más de tres factores

En el mismo sentido que Fine, otros autores definen sus propios métodos considerando más de tres factores, pero siempre basándose en el método Fine.

Romero, J. C. R. (2005) y Steel (1990) utilizan cuatro factores, definiendo la frecuencia en base al periodo de tiempo y número de personas expuestas a un riesgo, la probabilidad, la pérdida máxima probable y el número de personas expuestas.

3.1.2. Métodos complejos

3.1.2.1. Métodos cualitativos

Estos métodos se caracterizan en general por no recurrir a cálculos numéricos. Se clasifican en métodos comparativos y métodos generalizados.

3.1.2.1.1. Métodos comparativos

Según (GUIAR, 2012), estos métodos se basan en la utilización de técnicas obtenidas de la experiencia adquirida en equipos e instalaciones similares existentes, así como en el análisis de sucesos que hayan ocurrido en establecimientos parecidos al que se analiza. Principalmente son cuatro métodos los existentes:

1. Manuales técnicos o códigos y normas de diseño
2. Listas de comprobación o "*Safety check lists*"
3. Análisis histórico de accidentes
4. Análisis preliminar de riesgos o PHA

1. Manuales técnicos. Códigos y normas de diseño

Consisten en la elaboración de manuales internos de carácter técnico que especifiquen las características de diseño, instalación, operación y utilización de los equipos existentes en un determinado establecimiento. Estos manuales se deben basar en las normas y los códigos internacionales y nacionales de diseño. Para completar el análisis, se deben realizar periódicamente auditorías de seguridad que permitan juzgar el estado de los materiales, procedimientos, operaciones, emergencias que se han establecido.

Las normas y los códigos de diseño son elaboradas por organismos internacionales de reconocido prestigio en el campo de la normalización. A nivel mundial, la organización internacional más importante es la *International Organization for Standardization, ISO*.

En Europa, cada país ha establecido un sistema de normalización de carácter oficial o semioficial. Las más importantes son las siguientes:

- España: Asociación Española de Normalización y Certificación, AENOR
Elabora las normas UNE a partir de las ISO u otras.

- Alemania: Normas DIN. Normas VDI/VDE, *Verein Deutscher Ingenieure*.
- Reino Unido: *British Standards*, BS.

En Estados Unidos de América, existen varias organizaciones gubernamentales y privadas que se dedican a la elaboración de normas:

- *American National Standards Institute*, ANSI
- *American Society for Testing and Materials*, ASTM
- *American Petroleum Institute*, API
- *National Fire Protection Association*, NFPA
- *American Society of Mechanical Engineers*, ASME

2. Listas de comprobación: Safety check lists

Se utilizan para determinar la adecuación de los equipos, procedimientos, materiales, etc. a un determinado procedimiento o reglamento establecido por la propia organización industrial basado en experiencia y en los códigos de diseño y operación. Se pueden aplicar en cualquier fase de un proyecto: diseño, construcción, puesta en marcha, operación y paradas.

Permite comprobar con cierto detalle la adecuación de las instalaciones y constituye una buena base de partida para complementarlas con otros métodos de identificación que tienen un alcance superior al cubierto por los reglamentos e instrucciones técnicas.

3. Análisis histórico de accidentes

Consiste en el estudio de los accidentes registrados en el pasado en instalaciones similares o con productos de la misma. La principal ventaja radica en que se refiere a accidentes que ya han ocurrido, por lo que el establecimiento de hipótesis de posibles accidentes se basa en casos reales. No obstante, en los bancos de datos existentes, no se cubren todos los casos posibles, sino sólo los que se han dado, además de que los datos de que dispone pueden no ser completos.

Se basa en diferentes tipos de informaciones:

- Bibliografía especializada
- Bancos de datos informatizados de accidentes
- Registro de accidentes/incidentes de la propia empresa
- Informes de otros accidentes ocurridos

4. Análisis preliminar de riesgos (APR): Preliminary Hazard Analysis (PHA)

Desarrollado inicialmente por las Fuerzas Armadas de los EUA, fue el precursor de análisis más complejos y es utilizado únicamente en la fase de desarrollo de las instalaciones y para casos en los que no existen experiencias anteriores, sea del proceso o del tipo de instalación.

Selecciona los productos peligrosos existentes y los equipos principales y revisa los puntos en los que se piensa que se puede producir algún fallo de seguridad que suponga riesgos. Los resultados del análisis incluyen recomendaciones para reducir o eliminar estos peligros, siempre de forma cualitativa.

Requiere relativamente poca inversión en su realización (2 ó 3 personas con experiencia en seguridad, códigos de diseño, especificaciones de equipos y materiales).

3.1.2.1.2. Métodos generalizados

Estos métodos generalizados de análisis de riesgos, se basan en estudios de las instalaciones y procesos mucho más estructurados desde el punto de vista lógico-deductivo que los métodos comparativos. Normalmente siguen un procedimiento lógico de deducción de fallos, errores, desviaciones en equipos, instalaciones, procesos, operaciones, etc. que trae como consecuencia la obtención de determinadas soluciones para este tipo de eventos (GUIAR, 2012).

Existen varios métodos generalizados. Los más importantes son:

1. Análisis "*What if ...?*": ¿Qué pasaría si ...?
2. Análisis funcional de operabilidad, *HAZOP*
3. Análisis de los modos de fallo y efectos, *FMEA*

1. Análisis "What if ...?": ¿Qué pasaría si ...?

Consiste en el planteamiento de las posibles desviaciones en el diseño, construcción, modificaciones y operación de una determinada instalación, utilizando la pregunta que da origen al nombre del procedimiento: "*¿Qué pasaría si ...?*". Requiere un conocimiento básico del sistema y cierta disposición mental para combinar o sintetizar las desviaciones posibles, por lo que normalmente es necesaria la presencia de personal con amplia experiencia para poder llevarlo a cabo.

Se puede aplicar a cualquier instalación o área o proceso: instrumentación de un equipo, seguridad eléctrica, protección contra incendios, almacenamientos, sustancias peligrosas, etc. Las preguntas se formulan y aplican tanto a proyectos como a plantas en operación, siendo muy común ante cambios en instalaciones ya existentes.

El equipo de trabajo lo forman 2 ó 3 personas especialistas en el área a analizar con documentación detallada de la planta, proceso, equipos, procedimientos, seguridad,

etc. El resultado es un listado de posibles escenarios o sucesos incidentales, sus consecuencias y las posibles soluciones para la reducción o eliminación del riesgo.

2. Análisis funcional de operabilidad, HAZOP

El HAZOP es una técnica de identificación de riesgos inductiva basada en la premisa de que los riesgos, los accidentes o los problemas de operabilidad, se producen como consecuencia de una desviación de las variables de proceso con respecto a los parámetros normales de operación en un sistema dado y en una etapa determinada. Por tanto, ya se aplique en la etapa de diseño, como en la etapa de operación, la sistemática consiste en evaluar, en todas las líneas y en todos los sistemas las consecuencias de posibles desviaciones en todas las unidades de proceso, tanto si es continuo como discontinuo, planteadas a través de unas "palabras guía".

El método surgió en 1963 en la compañía *Imperial Chemical Industries, ICI*, que utilizaba técnicas de análisis crítico en otras áreas. Posteriormente, se generalizó y formalizó, y actualmente es una de las herramientas más utilizadas internacionalmente en la identificación de riesgos en una instalación industrial.

La realización de un análisis HAZOP consta de las etapas que se describen a continuación:

Etapas

1. Definición del área de estudio

Consiste en delimitar las áreas a las cuales se aplica la técnica. En una determinada instalación de proceso, considerada como el área objeto de estudio, se definirán para mayor comodidad una serie de subsistemas o líneas de proceso que corresponden a entidades funcionales propias: línea de carga a un depósito, separación de disolventes, reactores, etc.

2. Definición de los nudos

En cada uno de estos subsistemas o líneas se deberán identificar una serie de nudos o puntos claramente localizados en el proceso. Por ejemplo, tubería de alimentación de una materia prima a un reactor, impulsión de una bomba, depósito de almacenamiento, etc.

Cada nudo deberá ser identificado y numerado correlativamente dentro de cada subsistema y en el sentido del proceso para mejor comprensión y comodidad. La técnica HAZOP se aplica a cada uno de estos puntos. Cada nudo vendrá caracterizado por variables de proceso: presión, temperatura, caudal, nivel, composición, viscosidad, etc.

La facilidad de utilización de esta técnica requiere reflejar en esquemas simplificados de diagramas de flujo todos los subsistemas considerados y su posición exacta.

El documento que actúa como soporte principal del método es el diagrama de flujo de proceso, o de tuberías e instrumentos.

3. Aplicación de las palabras guía

Las "palabras guía" se utilizan para indicar el concepto que representan a cada uno de los nudos definidos anteriormente que entran o salen de un elemento determinado. Se aplican tanto a acciones (reacciones, transferencias, etc.) como a parámetros específicos (presión, caudal, temperatura, etc.).

4. Definición de las desviaciones a estudiar

Para cada nudo se plantea de forma sistemática todas las desviaciones que implican la aplicación de cada palabra guía a una determinada variable o actividad. Para realizar un análisis exhaustivo, se deben aplicar todas las combinaciones posibles entre palabra guía y variable de proceso, descartándose durante la sesión las desviaciones que no tengan sentido para un nudo determinado.

Paralelamente a las desviaciones se deben indicar las causas posibles de estas desviaciones y posteriormente las consecuencias de estas desviaciones.

En la tabla anterior se presentan algunos ejemplos de aplicación de palabras guía, las desviaciones que originan y sus causas posibles.

5. Sesiones HAZOP

Las sesiones HAZOP tienen como objetivo la realización sistemática del proceso descrito anteriormente, analizando las desviaciones en todas las líneas o nudos seleccionados a partir de las palabras guía aplicadas a determinadas variables o procesos. Se determinan las posibles causas, las posibles consecuencias, las respuestas que se proponen, así como las acciones a tomar.

Toda esta información se presenta en forma de tabla que sistematiza la entrada de datos y el análisis posterior. A continuación se presenta el formato de recogida del HAZOP aplicado a un proceso continuo.

Tabla 4. Formato de recogida del HAZOP

Planta:								
Sistema:								
Nudo	Palabra guía	Desviación de la variable	Posibles causas	Consecuencias	Respuesta	Señalización	Acciones a tomar	Comentarios

Fuente: Protección Civil. Guía Técnica: Métodos cualitativos para el análisis de riesgos

El significado del contenido de cada una de las columnas es el siguiente:

Tabla 5. Contenido de las columnas

Columna	Contenido
Posibles causas	Describe numerándolas las distintas causas que pueden conducir a la desviación
Consecuencias	Para cada una de las causas planteadas, se indican con la consiguiente correspondencia en la numeración las consecuencias asociadas
Respuesta del sistema	Se indicará en este caso:
	1. Los mecanismos de detección de la desviación planteada según causas o consecuencias: por ejemplo, alarmas
	2. Los automatismos capaces de responder a la desviación planteada según las causas: por ejemplo, lazo de control
Acciones a tomar	Propuesta preliminar de modificaciones a la instalación en vista de la gravedad de la consecuencia identificada o a una desprotección flagrante de la instalación
Comentarios	Observaciones que complementan o apoyan algunos de los elementos reflejados en las columnas anteriores

Fuente: Protección Civil. Guía Técnica: Métodos cualitativos para el análisis de riesgos

6. Análisis de los Modos de Fallo y Efectos, AMFE: *Failure Modes and Effects Analysis, FMEA*

El método consiste en la elaboración de tablas o listas con los posibles fallos de componentes individuales, los modos de fallo, la detección y los efectos de cada fallo.

Un fallo se puede identificar como una función anormal de un componente, una función fuera del rango del componente, función prematura, etc.

Los efectos son el resultado de la consideración de cada uno de los fallos identificados individualmente sobre el conjunto de los sistemas de la planta o instalación.

El método FMEA establece finalmente qué fallos individuales pueden afectar directamente o contribuir de una forma destacada al desarrollo de accidentes de una cierta importancia en la instalación.

Es un método válido en las etapas de diseño, construcción y operación y se usa habitualmente como fase previa a la elaboración de árboles de fallos, ya que permite un buen conocimiento del sistema. Con ciertas limitaciones se puede usar como método alternativo al HAZOP.

El equipo necesario suele ser de dos personas perfectamente conocedoras de las funciones de cada equipo o sistema así como de la influencia de estas funciones en el resto de la línea de proceso. Es necesario para la correcta ejecución del método disponer de listas de equipos y sistemas, conocimiento de las funciones de cada equipo, junto al conocimiento de las funciones de los sistemas en su conjunto dentro de la planta.

Es posible incluir en la última columna de la tabla de trabajo lo que se denomina índice de gravedad, que representa mediante una escala del 1 al 4 un valor que describe la gravedad de los posibles efectos detectados. El valor 1 representaría un suceso sin efectos adversos; el 2 efectos que no requieren parada del sistema; el 3 riesgos de cierta importancia que requieran parada normal y el 4 peligro inmediato para el personal e instalaciones, por lo que se requiere parada de emergencia. En este caso, el análisis se denomina Análisis del Modo de Fallos, Efectos y Criticidad, FMECA (AMFEC).

En la tabla 6 se presenta un ejemplo de formulario de trabajo para el análisis FMECA aplicado a un sistema de descarga de cisternas para tanques.

Tabla 6. Formulario de trabajo para análisis FMECA

Fecha:			Página:		De:
Planta:			Analista:		
Sistema:			Referencia:		
Identificación del elemento	Designación	Modo de fallo	Detección	Efectos	Índice de gravedad
1	Manguera flexible	Agujereada	Visual	Derrame ¿incendio?	4
		Taponada-aplastada	Visual	Falta o reducción de caudal	2
		Tipo equivocado	Visual (marcas)	Corrosión, rotura o contaminación	3

Fuente: Protección Civil. Guía Técnica: Métodos cualitativos para el análisis de riesgos

3.1.2.1.3. Frecuencias de ocurrencia

La evaluación cualitativa de las frecuencias de ocurrencia, se puede realizar mediante dos enfoques fundamentalmente distintos:

- Mediante una **valoración semicuantitativa**, que sin entrar en el análisis exhaustivo de las causas, puede asignar un nivel o rango de probabilidad a los accidentes.
- Mediante la **construcción y evaluación cualitativa de los árboles de fallos y eventos**. A través de esta técnica se puede realizar un estudio exhaustivo de

las causas que conducen a un accidente, así como una valoración cualitativa de las que tendrán mayor peso en la frecuencia resultante final.

Índices de frecuencias

En los primeros métodos se proponen diferentes niveles de probabilidad del suceso, determinándose posteriormente un factor de seguridad (FS) sobre la base de diversos valores, p.e:

- (PR) Participación en el riesgo del sistema, calculado en función de otros parámetros que caractericen el sistema y que tienen asignada una determinada ponderación.
- (RE) Importancia del riesgo en operación, calculado en función de otros parámetros que caracterizan la operación del sistema y que tienen asignada una determinada ponderación.
- (NG) Nivel de gravedad, valor que mide la magnitud de las consecuencias y que adopta un valor comprendido en un rango.

Estos métodos encuentran su aplicación cuando no sea preciso un análisis exhaustivo de las causas de los accidentes y basta con una idea del orden de magnitud de la frecuencia con que cabe esperar dichos accidentes.

Existen otros métodos que recurren a una asignación directa de la probabilidad de ocurrencia.

Son métodos que para que alcancen un mínimo de precisión en la clasificación realizada, exigen en cualquier caso un análisis previo de las causas y fallos que conducen al accidente.

Su aplicación conduce a una clasificación de las probabilidades del siguiente tipo:

- Baja.- Probabilidad de ocurrencia considerada REMOTA durante el tiempo de vida expresado de la instalación asumiendo que se realiza una operación y mantenimiento usuales.
- Media.- Probabilidad de ocurrencia considerada POSIBLE durante el tiempo de vida esperado de la instalación.
- Alta.- Probabilidad de ocurrencia considerada suficientemente alta para asumir que el evento OCURRIRÁ por lo menos una vez durante el tiempo de vida esperado de la planta.

La aplicación de estos métodos es sumamente subjetiva y precisa una gran experiencia en su realización.

3.1.2.1.4. Consecuencias

La evaluación semicualitativa de los alcances de consecuencias de accidentes se basa normalmente sobre métodos simplificados de cálculo que contemplan la aceptación de criterios sencillos para la determinación de los tipos de accidentes posibles y sus alcances.

Índices de consecuencias

Se plantean dos métodos diferentes para evaluar las consecuencias. En el primero se utiliza una **escala creciente de la gravedad**, graduada en diferentes niveles de consecuencia:

- Nivel 0: Consecuencias nulas. Caracteriza los sucesos que ocurren normalmente durante el funcionamiento.
- Nivel 1: Consecuencias leves. No hay pérdida sensible en la capacidad de la instalación, ni interrupción de la operación, ni heridas a personas, ni daños notables a los bienes o a las instalaciones.
- Nivel 2: Consecuencias significativas. Hay pérdida significativa de la capacidad de la instalación, pudiendo representar la detención de la operación normal. No hay heridas a las personas ni daños notables al sistema o a los bienes. Este nivel implica riesgos muy limitados en alcance e importancia.
- Nivel 3: Consecuencias críticas. Pueden haber heridas a las personas y/o daños notables al sistema o a los bienes. Este nivel comporta daños limitados a la unidad que incluye el sistema accidentado.
- Nivel 4: Consecuencias catastróficas con efectos limitados a la instalación industrial. Hay destrucción del sistema o de los sistemas vecinos, y/o varios heridos, y/o varios muertos.
- Nivel 5: Consecuencias críticas o catastróficas en las que los efectos sobrepasan los límites de la instalación industrial. Además de los descritos anteriormente, hay daños a las personas, a los bienes o a los sistemas exteriores a la instalación industrial.

La asignación del nivel de gravedad está fundamentada en el empleo de un esquema lógico dividido en seis diagramas. El seguimiento del esquema proporciona, según las características del sistema al cual se aplique, las ecuaciones a utilizar para calcular las distintas consecuencias y los criterios para asignar nivel de gravedad según el efecto considerado. El valor de nivel de gravedad resultante es el máximo obtenido. Las ecuaciones o de correlaciones altas que recurre el método son simplificadas en sentido conservador o tendentes a sobreestimar las magnitudes.

Esta fase de asignación del nivel de gravedad se articula en torno a cuatro puntos clave:

1. Criterios de asignación del nivel de gravedad.
2. Definición de accidentes. La ocurrencia de fenómenos no deseados (causas), conlleva efectos (consecuencias) que pueden ocurrir solos o en combinación con terceros.
3. Selección de hipótesis que puedan conducir de forma conservadora a la cuantificación de las consecuencias; a reducir el número de variables en las ecuaciones o correlaciones utilizadas; a establecer un procedimiento de cálculo fácilmente ejecutable con o sin medios informáticos, etc.
4. Normalización de los datos de entrada relativos al emplazamiento, equipos, al producto, etc.

Este método encuentra su aplicación cuando no es necesaria una cuantificación detallada del alcance de la consecuencia del accidente. No permite, por lo tanto, dimensionar las zonas de intervención y alerta, aunque puede permitir fijar la categoría de los accidentes.

Existen otros métodos que recurren a una asignación directa de la gravedad de las consecuencias por comparación con casos tipo ya resueltos, son métodos muy poco precisos y en el mejor de los casos sirven para fijar un orden de magnitud de los daños esperados.

Su aplicación conduce, por ejemplo, a una clasificación de las consecuencias de una fuga tóxica en las siguientes categorías:

- **Baja:** Las concentraciones esperadas de sustancia química en los alrededores de la instalación son muy bajas. Se puede esperar afectaciones sólo para exposiciones durante largos períodos de tiempo o cuando afecta a personas con condiciones de salud precarias.
- **Media:** Las concentraciones esperadas de sustancia química en los alrededores de la instalación son suficientes para causar heridas o muertes a menos que se tomen medidas correctivas efectivas de forma rápida. Se pueden esperar víctimas mortales sólo para exposiciones durante largos períodos de tiempo o cuando afecta a personas con condiciones de salud precarias.
- **Alta:** Las concentraciones esperadas de sustancia química en los alrededores de la instalación son suficientes para causar muertes o heridos graves para exposiciones breves. Se puede esperar un gran número de personas afectadas.

Se puede emplear en un estudio preliminar como método de selección del tipo de consecuencia a evaluar con mayor detalle.

3.1.2.2. Métodos semicuantitativos

Los métodos semicuantitativos son aquellos que introducen una valoración cuantitativa respecto a las frecuencias de ocurrencia de un determinado suceso y se denominan métodos para la determinación de frecuencias, o bien se caracterizan por recurrir a una clasificación de las áreas de una instalación en base a una serie de índices que cuantifican daños: índices de riesgo.

Los índices de riesgo son métodos de evaluación de peligros semicuantitativos directos y relativamente simples que dan como resultado una clasificación relativa del riesgo asociado a un establecimiento industrial o a partes del mismo. No se utilizan para estimar riesgos individuales, sino que proporcionan valores numéricos que permiten identificar áreas o instalaciones de un establecimiento industrial en las que existe un riesgo potencial y valora su nivel de riesgo. Sobre estas áreas o instalaciones, puede realizarse posteriormente un análisis más detallado del riesgo mediante otros métodos generalizados (Dirección General de Protección Civil, 2010a).

Los métodos desarrollados de mayor difusión a nivel internacional son dos:

1. Índice de Dow, de incendio y explosión
2. Índice de Mond, de fuego, explosión y toxicidad

1. Índice de Dow de incendio y explosión

Se trata de un método (Dow, 1997) desarrollado inicialmente por la compañía Dow Chemical en los años 60 con la denominación *de Dow's Fire & Explosion Index* que se ha ido perfeccionando con los años en ediciones sucesivas incorporando nuevos procesos de análisis.

El método se desarrolla siguiendo una serie de etapas y que se presentan de forma gráfica en la Figura 2. Las etapas son:

- a. Dividir la planta en estudio en unidades de proceso para las que se determina su índice de incendio y explosión, IIE.
- b. Determinar un factor material FM para cada unidad de proceso.
- c. Evaluar los factores de riesgo, considerando las condiciones generales de proceso (reacciones, transporte, accesos, etc.), denominadas F1, y los riesgos específicos del proceso/producto peligroso, denominados F2.
- d. Calcular un factor de riesgo, F3, y un factor de daño, FD, para cada unidad de proceso.
- e. Determinar los índices de incendio y explosión, IIE, y el área de exposición, AE, para cada unidad de proceso seleccionada.
- f. Calcular el valor de sustitución, VS, del equipo en el área de exposición.

- g. Calcular el daño máximo probable a la propiedad, MPPD (*Maximum probable property damage*), tanto básico como real, por consideración de los factores de bonificación, FB y FBE.
- h. Determinar los máximos días de interrupción, MPDO (*Maximum probable days outage*), y los costes por paralización de la actividad, BI (*Business interruption*), en estos días.

Factor material

Da una idea de la medida de la intensidad de liberación de energía de una sustancia o preparado. Toma valores entre 1 y 40 y existen valores para más de 300 sustancias usadas habitualmente en la industria. También establece la posibilidad de calcularlo a partir de unas determinadas propiedades físico-químicas de la sustancia.

Factores de riesgo

Tienen en cuenta las especiales condiciones del proceso que pueden modificar el riesgo de las instalaciones estudiadas. Hay que tener en cuenta tres tipos de factores de riesgo:

- Factores generales del proceso, F1: reacciones exotérmicas, endotérmicas, transferencias de producto, condiciones de ventilación, etc.
- Factores especiales, F2: toxicidad de las sustancias, considerada como complicación adicional, operaciones a presiones inferiores a la atmosférica, bajas temperaturas, corrosiones, etc.
- Factor de riesgo, F3: calculado a partir de los anteriores $F3 = F1 \cdot F2$.

Figura 2. Método Dow. Procedimiento de cálculo

Fuente: Dow's Fire & Explosion Index (1997)

Índice de incendio y explosión, IIE

Se calcula mediante la siguiente expresión:

$$IIE = FM \cdot F3$$

El método determina según este índice el área de exposición, AE, que representaría o daría una idea de la parte afectada por un incendio o explosión generada en la unidad de proceso estudiada.

Paralelamente, se determinarían las sucesivas variables: valor de sustitución (VS), el factor de daño (FD) y el máximo daño probable a la propiedad (MPDD).

Factores de bonificación

Son aquellos factores que protegen a la instalación mediante medidas de protección, sistemas de emergencia, etc. lo que hace disminuir el máximo daño probable a la propiedad. Los principales factores de bonificación pueden ser:

1. Controles de proceso: sistemas de refrigeración, control de explosiones, paros de emergencia, energía de emergencia, programas de mantenimiento, etc.
2. Aislamiento material: válvulas de control remoto, frenajes, enclavamientos, depósitos para vertidos de emergencia, cubetos, etc.
3. Protección contra el fuego: detectores, protección de estructuras, rociadores, cortinas, tanques de doble pared, sistemas especiales de extinción, etc.

Se calcula el factor de bonificación a partir de estos tres factores anteriores y se obtiene el daño máximo probable real a la propiedad:

$$MPDD (real) = MPDD \times FBE$$

A partir de este resultado, se calcula tanto el número de días de interrupción de la actividad, como el coste asociado a la interrupción industrial.

El método Dow se emplea principalmente como procedimiento de clasificación previa en grandes instalaciones o complejos (refinerías, complejos petroquímicos) para identificar las áreas con mayor riesgo potencial a las que se deben aplicar otro tipo de técnicas de identificación y cuantificación de riesgos.

2. Índice de Mond, de fuego, explosión y toxicidad.

Método desarrollado inicialmente en la Imperial Chemical Industries PLC (ICI) a partir del índice de Dow. La principal diferencia con el anterior es que el índice de Mond introduce la toxicidad de las sustancias presentes, y este parámetro se introduce como factor independiente, considerando los efectos de las sustancias tóxicas por contacto cutáneo, inhalación o ingestión en (Dirección General de Protección Civil, 2010a).

La aplicación del método permite cuantificar numéricamente:

- Un nivel de riesgo, que se establece a través de un valor numérico denominado índice de incendio y explosión y que normalmente se sitúa en el rango 1-200 (rango que comprende diferentes calificativos de peligro, que van de "ligero" a "severo").
- Un área de exposición, identificada con un círculo de radio proporcional al índice de incendio y explosión y que normalmente se sitúa en el rango 0-50 m.

- El máximo daño probable, evaluado como coste económico del accidente debido a la pérdida de instalaciones. Se evalúa como una fracción del coste de las instalaciones afectadas por el área de exposición.
- Los máximos días probables de indisponibilidad, desde el momento del accidente hasta el momento en que puede reanudarse la producción.
- El daño derivado de la pérdida de producción, como producto de los días de indisponibilidad de la planta por el valor perdido de la producción. Se sugiere utilizar un factor multiplicador de 0,7 para tener en cuenta ciertos rendimientos de los costes fijos.

La aplicación del método supone seguir los siguientes pasos:

1. Selección de la unidad de proceso
2. Determinación del factor de material MF
3. Cálculo del factor general de riesgo $F1 = 1 + \Sigma \text{penalización}$
4. Cálculo del factor especial de riesgo $F2 = 1 + \Sigma \text{penalización}$
5. Cálculo del factor de riesgo de la unidad $F3 = F1 \times F2$
6. Cálculo del índice de incendio y explosión $FEI = F3 \times MF$
7. Determinación del radio de exposición (en gráfico, Fig. 8 de la guía [INSH83]), que indica el alcance de los daños materiales según la valoración que se indica en el paso núm. 8
8. Cálculo del valor de sustitución de los equipos dañados. El método establece que el coste asociado a la destrucción derivada del accidente sería igual al producto: $0,82 \times (\text{coste original}) \times (\text{factor de escalado})$. El factor 0,82 se explica teniendo en cuenta que ciertas obras pueden ser aprovechadas (cimentaciones, accesos, etc.) en caso de rehacer las instalaciones. El factor de escalado es un coeficiente de actualización del precio original de la instalación
9. Determinación del factor de daño
10. Cálculo de máximo daño probable a propiedad (MPPD)
11. Cálculo del factor de bonificación, como producto de los factores de bonificación por control de proceso (C1), por aislamiento de material (C2) y por protección contra incendio (C3). Cada uno de estos factores se calcula a través del producto de las bonificaciones aplicables por cada concepto ($C_i = \Pi \text{ bonificación}$). Este valor multiplicará al MPPD para obtener un valor MPPD efectivo que tenga en cuenta la reducción del daño que puede darse por la adecuada actuación de los sistemas de protección instalados
12. Determinación de los máximos días probables de indisponibilidad

13. Cálculo del daño económico por la pérdida de producción (proporcional al valor de pérdidas por este concepto durante los días de indisponibilidad).

Las Figura 3 y Figura 4 siguientes resumen el método expuesto, con referencia a las tablas y figuras necesarias para aplicar el método.

Figura 3. Esquema de cálculo del índice DOW. Factores de penalización

Fuente: Dow's Fire & Explosion Index (1997)

Figura 4. Esquema de cálculo del índice DOW. Factores de bonificación

Fuente: Dow's Fire & Explosion Index (1997)

3.1.2.3. Métodos cuantitativos

3.1.2.3.1. Introducción

En un análisis cuantitativo de riesgos existe la necesidad de cuantificar la frecuencia o probabilidad de una serie de sucesos, en el sentido más amplio del término (Dirección General de Protección Civil, 2010b).

Básicamente puede considerarse la necesidad de cuantificación de los siguientes sucesos:

- **Iniciadores:** En esta categoría se incluyen sucesos externos, fallos de operación, humanos o pérdidas de inventario. Estos sucesos tienen una determinada frecuencia de ocurrencia en el tiempo, generalmente expresada en ocasiones por año.
- **Los sucesos que condicionan la evolución de un suceso iniciador:** En esta categoría se incluyen indisponibilidades de sistemas de seguridad, fenómenos físicos (ignición, explosión, etc.). Estos sucesos se caracterizan por su probabilidad de ocurrencia.

Se considera *Suceso Básico* a un evento simple cuya frecuencia/probabilidad se puede determinar de forma directa.

Se distinguen de los *Sucesos Complejos* para los cuales la obtención de la frecuencia/probabilidad no es inmediata.

3.1.2.3.2. Árbol de Fallos, AAF: Fault tree analysis, FTA

El Análisis por Árboles de Fallos (AAF), (Vesely, Goldberg, Roberts, & Haasl, 1981) es una técnica deductiva que se centra en un suceso accidental particular (accidente) y proporciona un método para analizar las causas que han producido dicho accidente. Nació en la década de los años 60 para la verificación de la fiabilidad de diseño del cohete Minuteman y ha sido especialmente utilizado en el campo nuclear y químico. El hecho de su gran utilización se basa en que puede proporcionar resultados tanto cualitativos mediante la búsqueda de caminos críticos, como cuantitativos, en términos de probabilidad de fallos de componentes.

Se trata de un método deductivo de análisis que parte de la previa selección de un "*suceso no deseado o evento que se pretende evitar*", sea éste un accidente de gran magnitud (explosión, fuga, derrame, etc.) o sea un suceso de menor importancia (fallo de un sistema de cierre, etc.) para averiguar en ambos casos los orígenes de los mismos.

Para el tratamiento del problema se utiliza un modelo gráfico que muestra las distintas combinaciones de fallos de componentes y/o errores humanos cuya ocurrencia simultánea es suficiente para desembocar en un suceso accidental.

Figura 5. Ejemplo de árbol de fallos

Fuente: Fault Tree Handbook, (1981)

La técnica consiste en un proceso basado en las leyes del Álgebra de Boole, que permite determinar la expresión de sucesos complejos estudiados en función de los fallos básicos de los elementos que intervienen en él.

Se descompone sistemáticamente un suceso complejo denominado suceso TOP en sucesos intermedios hasta llegar a sucesos básicos.

Suceso TOP: Ocupa la parte superior de la estructura lógica que representa el árbol de fallos. Es el suceso complejo que se representa mediante un rectángulo. Tiene que estar claramente definido (condiciones,...).

Sucesos intermedios: Son los sucesos intermedios que son encontrados en el proceso de descomposición y que a su vez pueden ser de nuevo descompuestos. Se representan en el árbol de fallos en rectángulos.

Sucesos básicos: Son los sucesos terminales de la descomposición. Pueden representar cualquier tipo de suceso: sucesos de "fallos" error humano o sucesos de "éxito": ocurrencia de un evento determinado. Se representan en círculos en la estructura del árbol.

En el proceso de descomposición del árbol se recurre a una serie de puertas lógicas que representan los operadores del álgebra de sucesos. Los dos tipos más elementales corresponden a las puertas AND y OR cuyos símbolos se indican a continuación. La puerta OR se utiliza para indicar un "O" lógico: significa que la salida lógica S ocurrirá siempre y cuando ocurran por lo menos una de las dos entradas lógicas e_1 o e_2 .

La puerta AND se utiliza para indicar un "Y" lógico. Para que ocurra la salida lógica S es necesario que ocurran conjuntamente las dos entradas lógicas e_1 y e_2 .

Se suelen numerar las puertas del árbol para facilitar su identificación. En la Tabla 7 extracto del *Fault Tree Handbook (1981)* se indican otros tipos de puertas lógicas (menos utilizados) y su simbología.

Tabla 7. Símbolos utilizados para la representación del árbol de fallos

SÍMBOLOS	SIGNIFICADO DEL SÍMBOLO
SUCESO BÁSICO. No requiere de posterior desarrollo al considerarse un suceso de fallo básico.
SUCESO NO DESARROLLADO. No puede ser considerado como básico, pero sus causas no se desarrollan, sea por falta de información o por su poco interés.
SUCESO INTERMEDIO. Resultante de la combinación de sucesos más elementales por medio de puertas lógicas. Asimismo se representa en un rectángulo el "suceso no deseado" del que parte todo el árbol.
PUERTA "Y" El suceso de salida (S) ocurrirá si, y sólo si ocurren todos los sucesos de entrada (E1 B1).
PUERTA "O" El suceso de salida (S) ocurrirá si ocurren uno o más de los sucesos de entrada (E1 B1).
SÍMBOLO DE TRANSFERENCIA. Indica que el árbol sigue en otro lugar.
PUERTA "Y" PRIORITARIA. El suceso de salida ocurrirá si, y sólo si todas las entradas ocurren en una secuencia determinada, que normalmente se especifica en una elipse dibujada a la derecha de la puerta.
PUERTA "O" EXCLUSIVA. El suceso de salida ocurrirá si lo hace una de las entradas, pero no dos o más de ellas.
PUERTA DE INHIBICIÓN. La salida ocurrirá si, y sólo si lo hace su entrada y además se satisface una condición dada (X).

Fuente: Fault Tree Handbook, (1981)

Sucesos no desarrollados. Existen sucesos en el proceso de descomposición del árbol de fallos cuyo proceso de descomposición no se prosigue, bien por falta de información, bien porque no se considera necesario. Se representan mediante un rombo y se tratan como sucesos básicos.

Con esta simbología, el árbol de fallos se va desarrollando, partiendo de un suceso no deseado o accidental que ocupa la cima del árbol. A partir de este suceso, se van estableciendo de forma sistemática todas las causas inmediatas que contribuyen a su ocurrencia definiendo así los sucesos intermedios unidos mediante las puertas lógicas.

Se definen dos fases bien diferenciadas: la primera consiste en la elaboración del árbol y la segunda en su cuantificación.

a) Elaboración del árbol de fallos

En esta fase se integran todos los conocimientos sobre el funcionamiento y operación de la instalación con respecto del suceso estudiado.

El primer paso consiste en identificar el suceso no deseado (TOP) que ocupará la cúspide de la estructura gráfica representativa del árbol. De la definición clara y precisa del TOP depende todo el desarrollo del árbol.

Con este TOP se establecen de forma sistemática todas las causas inmediatas que contribuyen a su ocurrencia, definiendo así los sucesos intermedios unidos a través de las puertas lógicas. El proceso de descomposición de un suceso intermedio se repite sucesivas veces hasta llegar a los sucesos básicos o componentes del árbol.

b) Cuantificación del árbol de fallos

Para ello se reduce la lógica del árbol hasta obtener las combinaciones mínimas de sucesos primarios cuya ocurrencia simultánea garantiza la ocurrencia del propio TOP. Cada una de estas combinaciones, también llamadas conjunto mínimo de fallo (*Minimal cut set*), corresponde a la intersección lógica (en Álgebra de Boole) de vanos sucesos elementales. Como por hipótesis de los árboles de fallos se supone que los sucesos básicos son mutuamente independientes (es decir que la ocurrencia de uno de ellos no tiene influencia sobre la ocurrencia de otro), la probabilidad de un conjunto mínimo de fallo viene dada por el producto de las probabilidades de los sucesos elementales que lo componen.

Asimismo el suceso no deseado viene representado por la unión lógica de todos los N conjuntos mínimos de fallos y se evalúa su probabilidad -P(TOP)- aplicando el "Teorema de las probabilidades totales o de Poincaré";

$$P(TOP) = \sum_{i=1}^N C_i - \sum_{i=1}^{N-1} \sum_{j=i+1}^N C_i * C_j + \sum_{i=1}^{N-2} \sum_{j=i+1}^{N-1} \sum_{k=j+2}^N C_i * C_j * C_k + \\ \dots + (-1)^{N-1} * C_i * C_j * \dots * C_N$$

donde C_i designa la probabilidad de un conjunto mínimo de fallos:

$$C_i = \prod_{s=1}^P a_s,$$

Fuente: *Fault Tree Handbook*, (1981)

siendo a_s , la probabilidad de s-ésimo suceso básico del conjunto mínimo de P sucesos (o de orden P).

Se suele aproximar la expresión (1) truncándola en el primer término. Esta simplificación, que se conoce como la del “suceso raro”, facilita los cálculos y el error que se comete se puede despreciar.

En los análisis mediante árboles de fallos se suele recurrir a otros estudios para acotar mejor los resultados. Entre ellos se destacan los análisis de incertidumbre y las clasificaciones de los sucesos base según distintas medidas de importancia.

Se comentan brevemente a continuación cada uno de estos puntos.

c) Análisis de incertidumbre

Las tasas de fallos de los componentes que aparecen en un árbol de fallos deben ser extraídas de los bancos de datos de fiabilidad.

Estos bancos estudian el comportamiento de un cierto número de equipos a lo largo del tiempo. Posteriormente los datos recogidos son tratados estadísticamente para obtener un valor representativo. Sin embargo, la mayoría de bancos de datos proporcionan no sólo un valor medio, sino que lo acompañan de un intervalo de variación dentro del cual podría oscilar el valor.

Esta dispersión obedece al hecho de que, en muchos casos, han entrado, en la “población” estadística considerada, componentes que:

- Trabajan en condiciones exteriores distintas (atmosféricas, entorno, etc.) o con productos diferentes,
- Son de características constructivas no directamente comparables,
- O están sometidos a políticas de mantenimiento no semejantes.

El valor medio extraído es, por tanto, un dato genérico que puede no adecuarse al caso en estudio.

Se considera habitualmente que la dispersión que existe sobre datos de este tipo puede ser descrita o ajustada a través de una ley de distribución logarítmica normal caracterizada por dos parámetros: un valor mediano (m) (que tiene acumulado un 50% de probabilidad) y un factor de error. Este factor de error (f) de limita un intervalo de variación para la probabilidad de fallo del componente definido como:

$$[\min, \max]$$

donde: $\min = m/f$

$$\max = m f$$

La tasa de fallos estará situada en el intervalo reseñado en un 90% de los casos.

La escasez de datos a veces obliga a intentar medir la dispersión que puede existir sobre el resultado de una evaluación de un árbol de fallos en función de la dispersión

que puedan tener los datos de partida. Este estudio es el denominado *análisis de incertidumbre*.

El análisis de incertidumbre consiste en medir la dispersión existente sobre el suceso TOP en función de la que puedan tener los fallos básicos.

En el caso en que se conoce la ley de distribución de los “n” componentes básicos del árbol, se suele recurrir al Método de Montecarlo que consiste en:

- Para cada componente se simula aleatoriamente una tasa de fallo. Para ello se genera un número aleatorio entre 0 y 1 que corresponde a la probabilidad de una determinada tasa; conocida la ley de distribución, se determina entonces la tasa de fallos correspondiente.
- Con los “n” valores de tasas de fallos generados aleatoriamente dentro de las distribuciones respectivas y correspondientes a los “n” componentes del árbol de fallos, se realiza una evaluación del árbol de fallos.
- Se repite N veces la operación con un nuevo conjunto de n-valores en cada caso.

Al final se obtienen N valores posibles del suceso TOP que a su vez pueden ser tratados estadísticamente para calcular:

- Valor medio
- Intervalo de variación

d) Análisis de importancia

Con las medidas de importancia se pueden clasificar los conjuntos mínimos de fallos o los sucesos básicos según los criterios que permiten determinar los que son críticos para la instalación. Las principales medidas de importancia son las tres que se describen a continuación. Hay que reseñar que según las fuentes, las denominaciones e incluso las expresiones varían, aunque al ser valores relativos, no se alteran las conclusiones que se pueden extraer de este tipo de estudios.

Medida de importancia *RAW (Risk Achievement Worth)*: Se define como el cociente entre la suma de las probabilidades de los conjuntos mínimos donde aparece el componente, asumiendo para éste una probabilidad de fallo de 1 (fallo seguro), y la probabilidad total del suceso TOP. Este factor mide la degradación que sufre el sistema en caso de ocurrir el fallo del componente. Tiene en cuenta la importancia “estructural” de un componente. Por ejemplo para un componente que constituye un conjunto mínimo de fallo de orden uno este factor es igual a la inversa de la probabilidad del suceso TOP. La expresión matemática del factor RAW respecto al componente C es:

$$\sum_{i=1 \text{ y } C \in C_i \text{ y } p(C)=1}^N P(C_i) / \sum_{i=1}^N P(C_i)$$

dónde:

- C es el componente respecto del cual se calcula la medida de importancia.
 ci es uno de los N conjuntos mínimos de fallos del sistema.
 p(Ci) es la probabilidad de Ci.
 C ∈ Ci representa que el componente C es uno de los componentes del conjunto mínimo de fallos Ci.
 p(C)=1 indica que el componente C adopta una tasa de fallos igual a 1 (fallo seguro).

Medida de importancia *RRW (Risk Reduction Worth)*: Se define como el cociente entre la probabilidad total del suceso TOP y la suma de las probabilidades de todos los conjuntos mínimos, asumiendo para el componente una tasa de fallo nula. Este factor proporciona el coeficiente por el cual quedaría dividida la frecuencia total del suceso TOP analizado en el caso de que el componente fuera perfecto. Este factor permite determinar qué componentes se tienen que modificar para reducir apreciablemente el riesgo. La expresión matemática del factor RRW respecto del componente C es:

$$= \sum_{i=1}^N P(C_i) / \sum_{i=1 \text{ y } p(C)=0}^N P(C_i)$$

dónde:

- C es el componente respecto del cual se calcula la medida de importancia.
 ci es uno de los N conjuntos mínimos de fallos del sistema.
 p(Ci) es la probabilidad de Ci.
 p(C)=0 indica que el componente C adopta una tasa de fallos igual a 0 (no falla el componente).

Medida de importancia de Fussell-Vesely: Se define el factor de importancia de Fussell-Vesely respecto de un componente C como el cociente entre la suma de las probabilidades de todos los conjuntos mínimos que contienen a este componente y la probabilidad total (o suma de las probabilidades de todos los conjuntos mínimos). Su expresión es:

$$\sum_{i=1}^N \sum_{C \in C_i} p(C_i) / \sum_{i=1}^N p(C_i)$$

dónde:

- C es el componente respecto del cual se calcula la medida de importancia.
ci es uno de los N conjuntos mínimos de fallos del sistema.
p(Ci) es la probabilidad de Ci.
C_ε Ci representa que el componente C es uno de los componentes del conjunto mínimo de fallos Ci.

Este factor tiene en cuenta el número de conjuntos mínimos de fallos en que aparece un componente (frecuencia de aparición en el árbol); su probabilidad y la de los componentes a los cuales va asociado.

Las medidas de importancia RAW y RRW son las más utilizadas porque su significado es más directo: se expresan en términos de porcentaje de mejora o empeoramiento de la probabilidad del TOP.

Por último, cabe tener en cuenta que también existen medidas de importancia respecto de los conjuntos mínimos de fallos.

Esta metodología se suele aplicar a sucesos relativamente complejos para los cuales intervienen muchos elementos y que se pueden descomponer en sucesos más sencillos.

Requiere analistas con amplia experiencia y conocimiento del sistema a analizar, frecuentes consultas a técnicos, operadores y personal experimentado en el funcionamiento del sistema y la documentación necesaria consiste en diagramas de flujos, e instrumentación hasta los procedimientos de operación/mantenimiento seguidos, ya que el árbol de fallos incorpora multitud de aspectos.

Ventajas

1. La técnica estudia las causas de sucesos indeseados y permite identificar los puntos débiles de un sistema (conjuntos mínimos de fallos). Este aspecto es vital en la prevención de accidentes.
2. A través del análisis de importancia se conoce el peso relativo de los distintos elementos del sistema. Con ello se puede establecer una lista de prioridades a fijar para mejorar la instalación.
3. La técnica es un método para conocer a fondo un sistema.

Inconvenientes

1. No permite tratar directamente fallos dependientes, al menos de forma directa, aunque siempre sea posible añadir el fallo dependiente como un componente más del árbol.
2. Sólo permite el tratamiento de situaciones temporales homogéneas.

3.1.2.3.3. Árboles de Sucesos, AAS: *Event tree analysis, ETA*

La técnica de análisis por árboles de sucesos, (Dirección General de Protección Civil, 2010a) consiste en evaluar las consecuencias de posibles accidentes resultantes del fallo específico de un sistema, equipo, suceso o error humano, considerándose como sucesos iniciadores y/o sucesos o sistemas intermedios de mitigación, desde el punto de vista de la atenuación de las consecuencias.

Las conclusiones de los árboles de sucesos son consecuencias de accidentes, es decir, conjunto de sucesos cronológicos de fallos o errores que definen un determinado accidente.

a) Construcción del árbol

La construcción del árbol comienza por la identificación de los N factores condicionantes de la evolución del suceso iniciador. A continuación se colocan éstos como cabezales de la estructura gráfica. Partiendo del iniciador se plantean sistemáticamente dos bifurcaciones: en la parte superior se refleja el éxito o la ocurrencia del suceso condicionante y en la parte inferior se representa el fallo o no ocurrencia del mismo.

Se obtienen así 2^N combinaciones o secuencias teóricas. Sin embargo, las dependencias entre los sucesos hacen que la ocurrencia o éxito de uno de ellos pueda eliminar la posibilidad de otros reduciéndose así el número total de secuencias.

La disposición horizontal de los cabezales se suele hacer por orden cronológico de evolución del accidente si bien este criterio es difícil de aplicar en algunos casos.

El suceso iniciador puede ser cualquier desviación importante, provocada por un fallo de un equipo, error de operación o error humano. Dependiendo de las salvaguardias tecnológicas del sistema, de las circunstancias y de la reacción de los operadores, las consecuencias pueden ser muy diferentes. Por esta razón, un AAS, está recomendado para sistemas que tienen establecidos procedimientos de seguridad y emergencia para responder a sucesos iniciadores específicos.

Se presenta un árbol de sucesos correspondiente a un suceso iniciador dado a modo de ejemplo.

Figura 5. Ejemplo de árbol de sucesos

Fuente: Protección Civil. Guía Técnica: Métodos cualitativos para el análisis de riesgos (2010)

b) Evaluación del árbol

El árbol de sucesos así definido tiene las siguientes características:

- El suceso iniciador viene determinado por una frecuencia (f), expresada normalmente en ocasiones por año.
- Los N factores condicionantes son sucesos definidos por su probabilidad de ocurrencia: p_i , $i=1,N$.
- Los sucesos complementarios de estos tienen asociada una probabilidad de $1-p_i$, $i=1,N$.

Como se considera que los factores condicionantes son sucesos independientes, cada una de las secuencias, S , tiene asociada una frecuencia, f_s de:

$$f_s = f \cdot \prod_{i,j} p_i \cdot (1 - p_j) \quad i=1, N; j=1, n_j$$

siendo:

N_i : el número de sucesos de éxito de la secuencia s .

N_j : el número de sucesos de fallo de la secuencia s .

De esta forma también se cumple que la suma de las frecuencias de todas las secuencias accidentales es igual a la frecuencia del iniciador:

$$\sum f_s = f$$

La obtención de los valores p_i se basa generalmente en datos bibliográficos, estimaciones de expertos o en la aplicación de la técnica del árbol de fallos descrita en el apartado anterior.

Ventajas

1. Permite un estudio sistemático y exhaustivo de la evolución de un suceso.
2. Su aplicación es muy sencilla.

Inconvenientes

1. El valor obtenido está sujeto a incertidumbre por la dificultad que existe normalmente en evaluar las probabilidades de los factores asociados.
2. Si el árbol es grande su tratamiento puede hacerse laborioso.

3.1.2.3.4. Análisis causa-consecuencias

Este método de análisis, (Dirección General de Protección Civil, 2010a) consiste en una combinación de árboles de fallos y árboles de sucesos. Posee la gran ventaja de la facilidad para ser usado como un buen recurso de comunicación, ya que los diagramas causa-consecuencia son extremadamente gráficos para mostrar las consecuencias de los accidentes postulados y causas elementales que los provocan.

El análisis causa-consecuencia es un método cualitativo, pero que puede ser desarrollado, asimismo, en su vertiente cuantitativa estableciendo las probabilidades de cada accidente y determinando sus consecuencias.

Posee la gran ventaja que permite moverse "hacia delante" con la técnica de los árboles de sucesos y hacia atrás" a través de los árboles de fallos. Todo ello apoyado en un diagrama que permite al analista una gran comodidad de movimientos frente al problema contemplado.

La resolución del diagrama causa-consecuencia es un listado de caminos críticos o secuencias de fallos (*minimal cut sets*) en línea de los determinados en los árboles de fallos que muestran las secuencias accidentales que provocarán la consecuencia accidental indeseada.

El proceso de desarrollo de este método de análisis es el siguiente:

- Selección de un suceso para ser evaluado:

Que puede ser, tanto un TOP indicado en los árboles de fallos, como un suceso iniciador, de los árboles de sucesos.

En los correspondientes apartados se han comentado con profundidad ambos elementos básicos del análisis, por lo que no se repite en este punto su descripción.

- Identificación de las funciones de seguridad y desarrollo de las secuencias accidentales:

Se desarrollan en paralelo, tanto la sucesión cronológica de sucesos, como los posibles fallos de los sistemas o funciones de seguridad existentes (sistemas de protección o prevención, actuaciones de los operadores, procedimientos, etc.).

Una primera diferencia entre el análisis causa-consecuencia y los árboles de sucesos es la simbología utilizada en los Diagramas.

Figura 6. Simbología básica utilizada en diagramas

Fuente: Protección Civil. Guía Técnica: Métodos cualitativos para el análisis de riesgos

El diagrama causa-consecuencia utiliza normalmente la simbología que se muestra en la Figura 7. En esta simbología destaca el símbolo de “toma de decisión adjunta”.

Figura 7. Símbolo de toma de decisión adjunta

Fuente: Protección Civil. Guía Técnica: Métodos cualitativos para el análisis de riesgos

Permite analizar el funcionamiento de un sistema de seguridad (cortinas de agua, por ejemplo) que debería actuar en un punto de la secuencia accidental.

La operación correcta o incorrecta del sistema analizado conducirá a dos situaciones absolutamente diferentes. En el caso de operación de unas cortinas de agua accionadas frente a una fuga de gas tóxico para un confinamiento, el resultado de su correcta operación (SI) es el confinamiento de la fuga y, por lo tanto, la interrupción o disminución del suceso accidental.

Si el sistema falló (NO), la nube de gas tóxico no se diluye y, por lo tanto, se extenderá fuera de los límites del confinamiento previsto.

- Desarrollo del suceso y de los fallos de funciones de seguridad para determinar las causas elementales:

Este paso consiste en la aplicación del análisis por árboles de fallos para cada uno de los sucesos iniciales o los fallos de funciones de seguridad identificados en el diagrama causa-consecuencia.

Es decir, cada fallo de las funciones de seguridad es utilizado, en definitiva, como un suceso iniciador o TOP en la técnica de los árboles de fallos descrita en el apartado 3.2.3.3.2.

No se reitera en este punto la técnica de desarrollo de los árboles de fallos y se remite al apartado correspondiente para conocer su desarrollo en detalle.

- Determinación de los conjuntos mínimos de fallo (*Minimal Cut Sets*) de las secuencias accidentales:

Emplea la misma técnica de determinación de los *Minimal Cut Sets* que se expone en los árboles de fallos.

Para cada secuencia accidental identificada en el diagrama, se determinan estos conjuntos mínimos de fallos que serán los caminos críticos que serán necesarios que ocurran para que se produzca el suceso final indeseado.

- Evaluación de resultados:

Los resultados de aplicación de los diagramas causa-consecuencia son evaluados en las siguientes etapas: en primer lugar se establece un orden

decreciente entre las consecuencias evaluadas, en función de su gravedad y de su importancia para la seguridad del entorno y de las propias personas e instalaciones; posteriormente, en un segundo paso, para cada secuencia accidental notable, se establece una clasificación de caminos críticos de fallo (*Minimal Cut Sets*) para determinar los fallos elementales o causas más importantes que puedan provocar los accidentes postulados.

La aplicación más adecuada para este método es en la etapa de diseño y proyecto de cualquier instalación, lo que facilitará enormemente la implantación de las recomendaciones derivadas del estudio.

Esta mayor viabilidad no implica, sin embargo, su no aplicación en instalaciones existentes para evaluar en profundidad los sistemas de seguridad existentes.

Como conjunción de los métodos de árboles de fallos y árboles de sucesos, está claro que para el desarrollo de este tipo de análisis es necesaria una persona con conocimiento profundo de aplicación de las técnicas que ambos métodos requieren.

El resto de miembros del equipo deben conocer con probada experiencia las posibles interacciones entre los sistemas, equipos o elementos incluidos en el desarrollo del análisis.

3.1.3. Otros métodos

Básicamente se incluyen aquí las auditorías de seguridad que suelen responder a otros objetivos (relativas a la organización de seguridad, el cumplimiento de una legislación, etc.), pero que pueden constituir una base para la identificación de riesgos.

La finalidad principal es verificar que las instalaciones, en operación y mantenimiento siguen las normas establecidas.

Estas revisiones de seguridad deben entenderse siempre como un complemento de las inspecciones rutinarias y deben partir siempre de un espíritu de colaboración para conseguir la operación de la planta en las mejores condiciones posibles de seguridad.

La labor incluye el desarrollo de entrevistas con personas de todo nivel: operadores de planta, mantenimiento, ingeniería, seguridad, gerencia, dirección general. Ello permite contemplar las situaciones desde diferentes y a veces contrastantes puntos de vista.

Generalmente, como instrumentos de apoyo de la labor realizada, pueden utilizarse métodos ya descritos tales como listas de chequeo, partes del método *What If* y otras.

El resultado de estas inspecciones son recomendaciones para mejorar las deficiencias observadas.

3.2. Evaluación de riesgos en infraestructuras

Con el fin de conocer cuáles son los métodos o sistemas de evaluación del riesgo empleados actualmente en el ámbito de las infraestructuras, se describen a continuación diferentes metodologías existentes para la evaluación de riesgos en infraestructuras de diferente tipo, marco en el que se disponen las instalaciones portuarias.

Para el desarrollo de este apartado se consideraron aquellas metodologías de mayor interés por su alcance para este estudio.

3.2.1. Conceptos básicos de la evaluación de riesgos

El informe *Natural Disasters and Vulnerability Analysis*, (Lewis, J. 1981), incluyó las siguientes definiciones relativas a la evaluación del riesgo:

- a) Amenaza, peligro o peligrosidad (Hazard - H). Es la probabilidad de ocurrencia de un suceso potencialmente desastroso durante cierto período de tiempo en un sitio dado.
- b) Vulnerabilidad (Vulnerability -V). Es el grado de pérdida de un elemento o grupo de elementos bajo riesgo resultado de la probable ocurrencia de un suceso desastroso.
- c) Riesgo específico (Specific Risk - Rs). Es el grado de pérdidas esperadas debido a la ocurrencia de un suceso particular y como una función de la amenaza y la vulnerabilidad.
- d) Elementos en riesgo (Elements at Risk - E). Son la población, los edificios y obras civiles, las actividades económicas, los servicios públicos, las utilidades y la infraestructura expuesta en un área determinada.
- e) Riesgo total (Total Risk - Rt). Se define como el número de pérdidas humanas, heridos, daños a las propiedades y efectos sobre la actividad económica debido a la ocurrencia de un desastre, es decir el producto del riesgo específico Rs, y los elementos en riesgo E.

3.2.1.1. Riesgo

La Real Academia de la Lengua Española define el riesgo de dos formas diferentes:

1. Contingencia o proximidad de un daño.
2. Cada una de las contingencias que pueden ser objeto de un contrato de seguro.

Desde un punto de vista formal y en función del campo de conocimiento en el que se evalúa, el riesgo tiene varias implicaciones y significados: riesgo estadístico, el riesgo como la probabilidad de fallo o riesgo financiero. En el campo de la ingeniería se

pueden encontrar diversas definiciones. (Akintoye & MacLeod, 1997) y la (UNDRO, 1979) definen el riesgo específico como es el grado de pérdidas esperadas debido a la ocurrencia de un suceso particular y como una función de la amenaza y la vulnerabilidad. En particular, formula el riesgo como el producto de los términos anteriores y los elementos en riesgo, que son la población, los edificios y obras públicas, las actividades económicas, los servicios públicos y la infraestructura que está expuesta a una cierta amenaza en cierto lugar. Una definición más positiva está dada por Asociations (2002); Del Caño, A., & de la Cruz, M. P. (2002); (Project Management Institute (PMI), 2000); (Özcan, 2008) que indican que el riesgo es el efecto positivo o negativo que la incertidumbre genera sobre los objetivos perseguidos. (Hillson, 2002) también considera el riesgo como una oportunidad, cuando los efectos son positivos; y una amenaza, cuando los efectos son negativos.

El riesgo es definido también como el "efecto de la incertidumbre en los objetivos "y un efecto es una desviación positiva o negativa de lo que se espera (ISO, 2010).

López, A. J., (2008) lo define 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:

$$R=f(f, c).$$

3.2.1.2. Amenaza

Si bien no existe una definición oficial para la amenaza, como sucedía con el riesgo, existen diferentes definiciones, así la amenaza se puede definir como un fenómeno, sustancia, actividad humana o condición peligrosa que puede ocasionar la muerte, lesiones u otros impactos a la salud, al igual que daños a la propiedad, la pérdida de medios de sustento y de servicios, trastornos sociales y económicos, o daños ambientales (UNISDR, 2009). La amenaza se determina en función de la intensidad y la frecuencia.

La amenaza se puede definir asimismo como la probabilidad de ocurrencia de un suceso potencialmente desastroso durante cierto período de tiempo en un sitio dado (UNDRO, 1979).

En general, hoy se acepta que el concepto de amenaza se refiere a un peligro latente o factor de riesgo externo de un sistema o de un sujeto expuesto, que se puede expresar en forma matemática como la probabilidad de exceder un nivel de ocurrencia de un suceso con una cierta intensidad, en un sitio específico y durante un tiempo de exposición determinado (Cardona, 2001).

3.2.1.3. Vulnerabilidad

La vulnerabilidad se puede definir como las características y las circunstancias de una comunidad, sistema o bien que los hacen susceptibles a los efectos dañinos de una

amenaza (UNISDR, 2009).

Özcan, (2008) hizo una revisión exhaustiva de la definición de vulnerabilidad, descrita por algunos autores como las características de un sistema que generan la posibilidad de que un daño que se produzca (Sarewitz, Pielke, & Keykhah, 2003); (Ezell, 2007) o la capacidad de la sistema para hacer frente a un evento de riesgo (Zhang, 2007) y para resistir y recuperarse de los efectos (Blaikie et al., 1994). En esta revisión, la vulnerabilidad también se puede encontrar como un sinónimo particular de peligro (Agarwal & Blockley, D. I., 2007); como el grado de incertidumbre y el riesgo (Buchanan, 1991); como la probabilidad de ocurrencia y el impacto de fenómenos meteorológicos y climáticos relacionados (Nicholls, Hoozemans, & Marchand, 1999); en relación con la población, los grupos sociales que experimentan recursos limitados y el consiguiente riesgo relativamente alto de morbilidad y mortalidad prematura (Levine, 2004). Asimismo (Kumpulainen, 2006) define la vulnerabilidad como el grado de fragilidad de una persona, un grupo, una comunidad o una zona, hacia el riesgo definido. Es un conjunto de condiciones y procesos resultantes de factores físicos, sociales, económicos y ambientales que aumentan la susceptibilidad de una comunidad al impacto de amenazas. Por lo tanto, se puede considerar como una combinación de daño potencial y la capacidad de afrontamiento, pero también se aprecia el carácter versátil de vulnerabilidad a través de tres dimensiones de vulnerabilidad: económicas, sociales y ecológicas. La definición de vulnerabilidad dada por la (UNDRO, 1979) se define como el grado de pérdida de un elemento o grupo de elementos bajo riesgo resultado de la probable ocurrencia de un suceso desastroso, expresada en una escala desde 0 o sin daño a 1 o pérdida total (UNDRO, 1979).

3.2.1.4. Consecuencias

Las consecuencias se pueden definir como el daño, debido al riesgo que se considera, más grave razonadamente posible, incluyendo desgracias personales y daños materiales (Fine, 1971).

La consecuencia es el resultado de un evento (ISO, 2009; Standards Australia/Standards New Zealand, 2005). En el US Department of Defense, 2006 se define como "El resultado de un suceso futuro expresado cualitativa o cuantitativamente, siendo una pérdida, lesión, una desventaja o una ganancia." El PMBOK (Project Management Institute (PMI), 2000) amplía la definición de consecuencia de ser "el efecto de los objetivos del proyecto, si se produce el evento de riesgo".

Una consecuencia es el resultado de un evento y tiene un efecto sobre los objetivos. Un solo evento puede generar una serie de consecuencias que pueden tener efectos tanto positivos como negativos sobre los objetivos. Las consecuencias iniciales también pueden escalar a través de efectos en cadena (ISO, 2010).

3.2.1.5. *Infraestructuras críticas*

- Según las define el *USA Patriot Act 2001* en su Sección 1016, las infraestructuras críticas están compuestas por aquellos sistemas y sus activos, ya sean físicos o virtuales, tan vitales para los Estados Unidos que la inhabilitación o la destrucción de estos sistemas y sus activos tienen un alto impacto en la seguridad económica nacional, en la salud pública, en la seguridad nacional, o cualquier combinación de estas cuestiones (USA Government, 2001).
- Según la Directiva 2008/114/CE de la UE: Las infraestructuras críticas son todos los elementos, sistemas o parte de éstos situados en los Estados miembros, esenciales para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones (Consejo de Europa, 2008).
- De acuerdo con la Ley 08/2011 sobre protección de infraestructuras críticas: Están constituidas por aquellas instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios públicos esenciales, cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su interrupción o destrucción tendría un grave impacto sobre los servicios públicos esenciales, los cuales a su vez son requeridos para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las Instituciones del Estado y de las Administraciones Públicas (Consejo de Europa, 2008).

Las infraestructuras están sometidas a riesgos corto plazo (relacionados con la interrupción inesperada de su operación) y riesgos de largo plazo (relacionados con la suficiente disponibilidad de energía para satisfacer la demanda y la adecuación de la infraestructura para abastecer los mercados que, a su vez, dependen de los niveles de inversión y contratación, el desarrollo tecnológico y la disponibilidad de fuentes de energía primaria).

3.2.1.6. *Infraestructura portuaria*

Según el Reglamento (CE) n° 725/2004 del Parlamento Europeo y del Consejo, de 31 de marzo de 2004, relativo a la mejora de la protección de los buques y las instalaciones portuarias, en su artículo 2, se define Instalación portuaria como “el lugar donde se realiza la interfaz buque-puerto. Incluye, según sea necesario, zonas como los fondeaderos, atracaderos de espera y accesos desde el mar” (Parlamento Europeo, 2004).

Asimismo, esta se constituye por obras de infraestructura y superestructura e

instalaciones mecánicas y eléctricas, fijas o flotantes, construidas en el puerto para dar servicio al buque y a las mercancías.

3.2.1.7. *Evaluación del riesgo*

La evaluación de la seguridad de una instalación es fundamentalmente un análisis de riesgos de todos los aspectos relacionados con las operaciones y elementos asociados a ella, 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.

El análisis del riesgo tiene su origen en el sector industrial y surge por la necesidad de evaluar los riesgos de un proceso productivo, eliminando con éste en la medida de lo posible, aquellas situaciones que generen un riesgo, en general, para la salud de los empleados.

Este análisis se ha extendido de forma generalizada a muchos otros sectores de la ingeniería, manteniendo el esquema de vinculación de riesgos con frecuencias y daños causados, aunque con parámetros diferentes y específicos para cada caso de estudio, aplicándose a otro tipo de riesgos, y no exclusivamente asociados a los accidentes laborales, sino también a la seguridad en las operaciones o a la seguridad en términos de amenazas de ataques y/o pérdidas de vidas humanas en infraestructuras.

La evaluación de riesgos tiene tres componentes básicos: la evaluación del entorno de amenazas (probabilidad de un ataque); la vulnerabilidad del sistema (probabilidad de que un ataque sea exitoso); la criticidad y la magnitud de las posibles consecuencias (impacto de un ataque con éxito). Una evaluación de riesgos correctamente realizada debe ser iterativa y actualizada periódicamente para determinar cómo los riesgos cambian según la aplicación de medidas de seguridad y medios de vigilancia. Este proceso inherentemente complejo requiere conocimientos especializados tanto de transporte como de seguridad.

Dada la magnitud de estas tareas, se deben establecer prioridades para orientar las decisiones y los beneficios de equilibrio frente a los costos, incluyendo la identificación de las externalidades a nivel de sistema y la posibilidad de consecuencias no deseadas. Un enfoque basado en el riesgo priorizado es un elemento fundamental para determinar soluciones prácticas y asequibles. Una vez que los riesgos son identificados, evaluados y priorizados, los planes de acción se podrán desarrollar para mitigar los riesgos, (Center, V., 2003).

La evaluación de riesgos es un proceso que, a su vez, se compone de tres procesos: identificación de riesgos, análisis de riesgos y evaluación de riesgos (ISO, 2010).

La identificación de riesgos es un proceso que se utiliza para buscar, reconocer y describir los riesgos que podrían afectar a la consecución de los objetivos.

El análisis de riesgos es un proceso que se utiliza para comprender la naturaleza, las fuentes y causas de los riesgos que se han identificado y para estimar el nivel de riesgo. También se utiliza para estudiar los impactos y consecuencias y para examinar los controles que existen en la actualidad.

La evaluación del riesgo es un proceso que se utiliza para comparar los resultados de análisis de riesgos con criterios de riesgo con el fin de determinar si es o no un determinado nivel de riesgo es aceptable o tolerable.

3.2.1.8. Protección marítima

Según el Reglamento (CE) n° 725/2004 del Parlamento Europeo y del Consejo, de 31 de marzo de 2004 (Parlamento Europeo, 2004), relativo a la mejora de la protección de los buques y las instalaciones portuarias, en su artículo 2, se define la protección marítima como la combinación de métodos preventivos destinados a proteger el transporte marítimo y los puertos contra la amenaza de actos ilícitos deliberados.

3.2.2. Gestión del riesgo

La gestión del riesgo es parte fundamental de las determinaciones contenidas en los códigos y reglamentos relativos a la protección, por lo que parece adecuado hacer una breve definición del concepto de gestión de riesgos, término que se aplica a un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, seguir y comunicar los riesgos asociados a cualquier actividad, función o proceso, de tal forma que permita a las organizaciones minimizar las pérdidas y maximizar la seguridad y/o los beneficios, (Sanchidrián, 2008).

La Gestión de Riesgos trata tanto de identificar los acontecimientos peligrosos, como de impedir o reducir las pérdidas. A continuación se muestra un esquema del proceso de gestión de riesgos aplicado a la protección.

En este contexto el análisis de riesgos que requiere la aplicación del Código PBIP, el Reglamento CE, la Directiva CE y su trasposición al sistema español es un procedimiento que permite evaluar la incidencia de cada uno de los sucesos en el buque, la instalación portuaria, o elemento de ella que se analiza, o el puerto (incluidas sus zonas adyacentes), determinando, a partir de la probabilidad de presentación del suceso o verosimilitud, de la vulnerabilidad del elemento y de las consecuencias que se derivarían de la materialización del suceso analizado, el riesgo de cada uno de los casos estudiados y, en función de él, determinar si es o no aceptable, determinando en este segundo caso las posibles medidas para tratar y reducir este riesgo de manera que, una vez implementadas, el riesgo residual del caso estudiado pudiera ser aceptable.

El análisis del riesgo parte de la evaluación de los buques, las instalaciones, o el puerto, a partir de los sistemas y procedimientos existentes, ya que su finalidad es

definir unas instalaciones, sistemas o procedimientos modificados que permitan reducir el riesgo de manera que no se sobrepasen los valores aceptables, (Sanchidrián, 2008).

Hay tres elementos principales que deben ser examinados para identificar los riesgos que son relevantes para la organización (Victoria Department of Transport (Australia), 2012):

- Establecer los activos críticos de la instalación. Esto permitirá centrarse en los activos o las dependencias que son esenciales para la organización para funcionar y alcanzar sus objetivos.
- Identificar las fuentes del riesgo (tradicionalmente conocido como amenazas), para comprender mejor la gama de factores potenciales que pueden afectar sus activos críticos.
- Determinar las posibles áreas de impacto en la instalación, si se activan las fuentes de riesgo en contra de los activos críticos.

3.2.3. Metodologías de evaluación de riesgos en infraestructuras críticas

En el Libro verde las Infraestructuras Críticas de la UE, (European Commission, 2005), se propone la creación de un marco común de la UE para la protección de las infraestructuras críticas en Europa, que podría ser puesto en marcha con el fin de asegurarse de que cada Estado miembro está proporcionando niveles adecuados de seguridad y la igualdad de protección en cuanto a su infraestructura crítica.

En la medida en que los diferentes sectores que contienen las infraestructuras críticas son muy diversos, es difícil prescribir exactamente qué criterios deben utilizarse para identificar y proteger a todas ellas en un mismo marco; esto deberá llevarse a cabo sector por sector, (European Commission, 2005).

En el contexto de la investigación asociadas a las amenazas en infraestructuras críticas, se desarrolló el proyecto SEDUCE (CDTI, 2011), Sistemas para la Detección de Explosivos en Infraestructuras y Centros Públicos, financiado por el CDTI, elaborado mediante un consorcio de empresas públicas y privadas y varias universidades, y que tuvo como objetivo el desarrollo de tecnologías para la detección de artefactos explosivos improvisados en centros e infraestructuras públicas. Dentro del mismo se analizaron y modelizaron los entornos de aplicación que demandan un análisis de seguridad ante explosivos, se estudiaron las características físicas y legales, así como los puntos clave, de cada tipo de infraestructura de transporte y finalmente se identificaron las posibles amenazas, individuales o integradas, para cada tipo de entorno estudiado.

La Universidad Politécnica de Madrid, participó asimismo en dicho proyecto en las fases de investigación básica, realizando un análisis integrado de amenazas para cada infraestructura.

En lo relativo a infraestructura portuaria, y en las cuestiones objeto de estudio aquí, el estudio concluyó que en los escenarios de un puerto las consecuencias de las amenazas varían enormemente dependiendo del tipo que sean. Los efectos de un coche bomba están limitados a las zonas de acceso de vehículos privados. Sin embargo, un ataque suicida sería extremadamente dañino en un entorno de pasajeros como Estaciones Marítima o club náuticos. Quizá sean los sabotajes las amenazas de mayor factibilidad, aunque su repercusión varíe considerablemente en función del activo afectado.

Especialmente peligrosas resultan las estaciones de servicio de combustible o las instalaciones de las empresas concesionadas de hidrocarburos en los puertos. Las consecuencias indirectas serían inimaginables dada la cercanía del casco urbano de la ciudad al puerto.

En todas las amenazas a instalaciones, repostaje o transporte de hidrocarburos, las consecuencias de un atentado incluirían el desastre medioambiental.

Durante el proceso de investigación se localizaron numerosas metodologías para la estimación de riesgos en infraestructuras críticas, si bien solo se presentan aquí un número seleccionado de estas en base a sus registros de citación y su reconocimiento en la comunidad científica.

Con el fin de obtener una revisión estructurada se realizó la selección de estas metodologías según los siguientes criterios:

- Ámbito de aplicación de la metodología: sector al que se dirige, a quien está dirigida (responsables políticos, investigadores, operadores etc.).
- Objetivos de la metodología
- Interdependencia de amenazas
- Tipos de riesgos para los diferentes sectores

En base a los mismos se seleccionaron aquellas que permiten evaluar cualquier tipo de infraestructura y que consideran riesgos de cualquier tipo o de forma específica actos terroristas, inmigración ilegal desde el puerto, intrusión, sabotaje, etc. Así, se seleccionaron y analizaron 14 metodologías diferentes para la evaluación de riesgos en infraestructuras críticas y portuarias de forma específica. Las metodologías analizadas preliminarmente fueron:

1. AERONÁUTICA CIVIL .Colombia, (Dirección de Seguridad y Supervisión Aeroportuaria, 2010).

2. BMI Protection of Critical Infrastructures. Alemania, (Federal Ministry of the Interior, Germany), 2008).
3. CARVER. Ejército de los EUA., (Taylor, 2002).
4. CIP/DSS. Critical Infrastructure Protection Decision Support System, (Bush, B., Dauelsberg, L., LeClaire, R., Powell, D., DeLand, S., Samsa, M., 2005).
5. COUNTERACT. Generic Guidelines for Conducting Risk Assessment in Public Transport Networks, (COUNTERACT, 2009).
6. DECRIS. SINTEF. Noruega. (Utnea, I. B., Hokstad, P., Kjøllec, G., Vatna, J., Tøndeld, I. A., Bertelsene, D., Fridheimf, H, Røstumg, 2008).
7. DIRECTRICES PARA TERMINALES DE TRANSPORTE COMBINADO. Union of Combined Road-rail transport companies,(UIRR, 2007).
8. EURACOM. Comisión Europea. (EURACOM, 2007).
9. FAA. Federal Aviation Administration. EE. UU., (Hunt & Kellerman, 1998).
10. RAM. Risk Assessment Methodology (Baker et al., 2002).
11. RBDM. Navigation and Vessel Inspection. EUA., (U. S. Coast Guard, 2003).
12. SECUREPORT. España, (Sanchidrián, 2008).
13. TERMINALES DE CONTENEDORES INTERIORES. Austria, (Gronalt, Häuslmayer, Jammernegg, Schindlbacher, & Weishäupl, 2005).
14. TRAM. OTI/OMI, (Organización Marítima Internacional & Organización Internacional del Trabajo, 2003).

Con el fin de conocer su alcance y contenido detallados, se realiza una descripción pormenorizada de las mismas en el *Anexo 1. Metodologías consideradas*.

3.3. Análisis de riesgos en puertos

Una vez enunciadas las metodologías tradicionalmente empleadas en la evaluación del riesgo en infraestructuras críticas y en particular en las portuarias, se procede a continuación a la revisión del Estado del Conocimiento del estudio de la evaluación de riesgos en instalaciones portuarias.

Dentro de dichos estudios se localizan diferentes tipologías de riesgo; medioambientales, debidos a desastres naturales, económicos, para la mercancía, etc.

El estudio de los riesgos asociados a los puertos, en general es reciente, y la bibliografía existente se centra en diferentes aspectos de interés para las instalaciones portuarias, en función del daño que se quiera evitar y las vulnerabilidades que se derivan de las instalaciones o infraestructuras a proteger.

3.3.1. Riesgos medioambientales y ante desastres naturales

Los cambios medioambientales a nivel mundial han dado lugar a frecuentes situaciones de clima extremo como los tsunamis, huracanes, etc. Los desastres naturales resultan por tanto cada vez más frecuentes y en general son de gran magnitud.

En este sentido (Hsieh, 2014) examina el riesgo de fallos en puertos desde la perspectiva de la vulnerabilidad. De forma específica se estudian siete factores vulnerables derivados de la literatura existente y de las lecciones aprendidas de los casos de desastres anteriores, empleando para ello los Sistemas de Información Geográfica. Los resultados revelan que la capacidad del puerto y su eficiencia tienen un efecto significativo sobre la vulnerabilidad de este, en aquellos puertos en los que la eficiencia de las grúas de pórtico, la mano de obra, el volumen de negocios en la denominada Zona de Libre Comercio (FTZ) del puerto evaluado, y los accesos terrestres desempeñan un papel fundamental en fallos del puerto. Por otra parte, los riesgos asociados con la operación del puerto son evaluados mediante la superposición de un mapa de peligro de las zonas propensas a inundaciones y flujos de restos arrastrados por el tsunami. Los mapas de riesgo pueden ayudar a los responsables en la toma de decisiones a la comprensión de la vulnerabilidad y la adopción adecuada de las estrategias para minimizar los riesgos de desastres.

Se crea un prototipo de modelo para ayudar a los decisores en la comprensión global de riesgo del puerto desde la perspectiva de la vulnerabilidad. Además de la vulnerabilidad física, se consideran en la evaluación de la vulnerabilidad del puerto los impactos sociales y económicos.

En base a los resultados de la revisión bibliográfica, talleres y entrevistas a expertos, el estudio construye siete factores vulnerables en el fallo del puerto. Se realiza una prueba empírica en el Puerto de Taipéi, en el norte de Taiwán. De acuerdo con los resultados, la capacidad y la eficiencia de la capacidad de la grúa de pórtico, la productividad del trabajo, y el volumen de negocios de FTZ afectan sustancialmente a la vulnerabilidad del puerto.

El análisis de riesgos se lleva a cabo para ayudar a los responsables en la toma de decisiones a comprender los sistemas vulnerables, permitiendo adoptar así las estrategias adecuadas de prevención y preparación ante desastres y reduciendo así dichos riesgos. Los flujos de escombros y posibles inundaciones causadas por tsunamis son considerados como peligros para la evaluación del riesgo de desastres en el Puerto de Taipéi. El caso estudiado verifica la factibilidad y viabilidad de los enfoques propuestos. Los sectores públicos deben formular estrategias para los servicios operativos relativamente vulnerables (es decir, vulnerabilidades alta y muy alta) en base a consideraciones a largo plazo. Para eliminar el riesgo de desastres, los sectores públicos deben desarrollar la planificación regional integrada para reducir la

exposición de las infraestructuras e instalaciones vulnerables a los riesgos, y deben implementarse sistemas de alerta temprana fiables para la prevención de desastres para mejorar las capacidades de autoprotección. Los factores de vulnerabilidad y su importancia para un sistema varían debido a las características espacio-temporales y de riesgo. Por lo tanto, es difícil para validar los resultados con estudios previos sobre lugares específicos, duraciones, y amenazas.

Por otra parte, las vulnerabilidades de las operaciones portuarias aumentan gradualmente como resultado del crecimiento económico y los cambios en la estructura social. Las autoridades deben invertir en la redundancia de las redes de transporte y la construcción de sistemas de logística portuaria suficientemente resistentes para garantizar que las operaciones portuarias pueden resistir el impacto de las amenazas. Los enfoques propuestos pueden ayudar a los planificadores no sólo en la comprensión integral del marco los instrumentos de la vulnerabilidad y del riesgo de desastres, sino también en la determinación de si las infraestructuras específicas relacionadas con los puertos desempeñan un papel fundamental, lo que facilita la priorización de la asignación de recursos.

La propuesta de una estrategia para determinar las prioridades en la asignación de recursos teniendo en cuenta la interdependencia, el cálculo de capacidad de servicio del puerto, la simulación del rendimiento de políticas interrumpidas para la mejora de las vulnerabilidades sería útil para la gestión de desastres en las operaciones portuarias.

Por su parte (Velásquez et al., 2014) realizaron un estudio sobre la evaluación de los riesgos de desastres mediante la creación de curvas de exceso de pérdidas híbridas. Teniendo en cuenta que el riesgo de peligros naturales es un suceso accidental y, por tanto, un riesgo soberano de los gobiernos nacionales, es importante evaluar adecuadamente las pérdidas potenciales para diseñar una estrategia de reducción del riesgo, la retención y la transferencia adecuada. Los autores proponen así una metodología de evaluación del riesgo de desastres basada en dos enfoques: por una parte, la estimación empírica de las pérdidas, el uso de la información disponible en las bases de datos locales de desastres, lo que permite estimar las pérdidas por fenómenos de pequeña escala y, por otra parte evaluaciones probabilísticas para estimar las pérdidas para eventos mayores o incluso catastróficas, para los cuales la información por lo general no está disponible debido a la falta de datos históricos. Se determina así la denominada "curva' híbrida" de exceso de pérdidas, que combina los resultados de estos dos enfoques y representa el riesgo de desastres de una manera adecuada y completa. Esta curva se fusiona dos componentes: el que corresponde a las pérdidas pequeñas y moderadas, calculadas mediante un análisis inductivo y retrospectivo, y la correspondiente a las pérdidas extremas, calculada mediante un análisis deductivo y prospectivo.

Los autores proponen una nueva metodología de análisis de riesgos basándose en una curva híbrida de exceso de pérdidas, que representa el riesgo de una manera adecuada y completa. Esta curva de exceso de pérdidas tiene dos componentes. El primero corresponde a la frecuencia, los eventos menores, por lo general producen pequeñas y moderadas pero repetitivas y extensas pérdidas, y se calcula mediante el uso de un análisis inductivo y retrospectivo. La segunda se tiene en cuenta la posible aparición de fenómenos extremos que producen pérdidas intensivas y enormes y se calcula mediante el uso de un análisis deductivo y prospectivo para lo que se empleó la plataforma CAPRA (Enfoque Integral para la Evaluación Probabilística del Riesgo). El riesgo amplio tiene que ser mitigado con estrategias de intervención eficaces, como la planificación de la protección, ordenación del territorio o bien obras de protección, mientras que para el riesgo intensivo, se requieren regulaciones y estrategias de protección financiera y la transferencia del riesgo.

Tabla 8. Curva híbrida de exceso de pérdidas

Fuente: Velásquez et al., 2014

El estudio realizado a nivel nacional muestra que es indispensable medir el riesgo retrospectivamente, con un enfoque empírico y, al mismo tiempo, de manera prospectiva, con un enfoque probabilístico. La falta de procedimientos para evaluar las pérdidas debidas a eventos menores y repetitivos ha impedido hasta ahora que los gobiernos sean conscientes de las enormes pérdidas debido a este tipo de eventos. El enfoque propuesto y los estudios de casos realizados permiten, no sólo ilustrar, sino también promover el interés de los decisores por una gestión eficaz del riesgo, basado en la evaluación de riesgos completa y de múltiples peligros facilitada por la curva híbrida de exceso de pérdidas. La curva híbrida propuesta permite la captura de

aspectos que la LEC (curva de exceso de pérdidas) prospectiva no es capaz de tener en cuenta, para evitar la subestimación de las consecuencias de pequeña escala y eventos recurrentes. Y, obviamente, es importante tener la posibilidad de estimar las pérdidas esperadas que un país puede enfrentar probablemente cada año y la planificación del mecanismo económico necesario para recuperarse más rápidamente.

La metodología propuesta hace un uso distinto de los datos históricos de los desastres en comparación con otros enfoques existentes. En lugar de utilizar los datos empíricos de eventos y pérdidas para calibrar o validar modelos catastróficos, se propone un enfoque que permite evaluar el costo de los desastres anteriores, su efecto sobre la sociedad, y mide la responsabilidad fiscal país, proporcionando métricas de riesgo tales como la AAL (pérdida media anual) y la LEC (curva de exceso de pérdidas). Los modelos existentes por lo general no tienen en cuenta las estimaciones de las consecuencias de los pequeños acontecimientos cuya impacto acumulado en el tiempo es de especial relevancia, principalmente para los gobiernos y gestores de riesgo. La AAL y la LEC no se pueden obtener de los pequeños desastres debido a la complejidad de los modelos y la información detallada necesaria a escala local, tales como la topografía o las características mecánicas del suelo que han de influir en gran medida en los resultados. Además, la exposición también requiere datos detallados disponibles sólo en las grandes ciudades, pero no en las zonas rurales. Combinando el enfoque retrospectivo con uno prospectivo (que representa los futuros acontecimientos catastróficos que aún están por ocurrir), puede lograrse un cuadro general del riesgo de desastres permitiendo a los gobiernos diseñar mejores políticas de reducción de riesgos.

3.3.2. Riesgos económicos

Los riesgos económicos resultan de vital importancia en la gestión de los puertos, debido a la trascendencia de estos en la cadena logística del transporte de mercancías e industrias asociadas, y a la relevancia del sector marítimo en las economías nacionales.

Es por ello que los riesgos económicos derivados de diferentes situaciones; problemas en la cadena logística, problemas climatológicos, etc., se han estudiado con mucho interés en los últimos tiempos, especialmente aquellos asociados a situaciones graves de seguridad para el funcionamiento del puerto y por ende a la economía de determinados sectores industriales.

En este campo de estudio del riesgo (Yi Zhang, Siu, & Lam, 2016) realizaron una investigación con el objeto de estimar las pérdidas económicas de los sectores industriales debido a las interrupciones del servicio en los puertos.

Las operaciones portuarias son muy importantes para las industrias que dependen en gran medida de las importaciones y exportaciones. Una evaluación fiable de los

riesgos portuarios es esencial para controlar el funcionamiento normal de transporte marítimo y por lo tanto las economías industriales. La ruptura del servicio que proveen los puertos implica la interrupción en la fluidez de las cadenas de suministro a las industrias. La estimación de la pérdida económica para una industria cuando un puerto interrumpe sus operaciones es una tarea difícil ya que la relación entre las agrupaciones portuarias e industriales es compleja.

El trabajo analiza el impacto de la interrupción del servicio del puerto, la cual afecta a las diferentes industrias, mediante el examen de las pérdidas económicas directas e indirectas producidas.

Los autores realizan una contribución original mediante la propuesta de un marco sistemático para calcular las pérdidas económicas industriales cuando se produce una interrupción del servicio del puerto. Se empleó un modelo de redes Petri para formular el flujo de la cadena de suministro. Posteriormente se realizó un estudio del caso en el puerto de Shenzhen (China). Empleando el negocio de las impresoras HP como ejemplo, este trabajo demuestra el uso del enfoque propuesto en el cálculo de las pérdidas económicas industriales como resultado de la interrupción del puerto de Shenzhen. Se proporciona una discusión completa por la pérdida industrial. El análisis realizado ayuda a los políticos y profesionales de la industria para tener una comprensión clara de las pérdidas económicas cuando se produzca la interrupción del puerto. Por otra parte, el trabajo también investiga diversos escenarios de control de inventario para averiguar el esquema más apropiado que permita reducir las pérdidas económicas totales. La cuantificación de la pérdida potencial podría ayudar a los responsables de la industria a evaluar el comportamiento de la cadena de suministro antes los riesgos considerados de interrupción del puerto.

Si bien este trabajo se esfuerza por desarrollar un marco para evaluar las pérdidas económicas de las industrias como resultado de la interrupción del servicio del puerto, las hipótesis realizadas en la evaluación son asimismo las limitaciones del estudio. En primer lugar, la identificación de los límites de un clúster industrial determinado se basa en la red de flujo de carga. La cadena de suministro considerada en el análisis está constituida específicamente por los principales participantes; el proveedor de materia prima, el transportista, el puerto, el fabricante y el destinatario, así como las compañías de seguros que asumen las pérdidas económicas aseguradas. Sin embargo, debe tenerse en cuenta que la cadena de suministro de un clúster de industrias incluye más participantes, como el promotor de la carga y la aduana. El estudio presente no tiene en cuenta las pérdidas económicas de estos participantes. En segundo lugar, en las estimaciones de pérdidas económicas, el valor de la producción diaria se utiliza como una medida de las pérdidas económicas reales. Sin embargo, las unidades producidas se pueden vender parcialmente y, por lo tanto, las ventas perdidas no tendrían una relación directa con la producción. Por lo tanto hay que asumir que todos los productos pueden ser consumidos cuando se produce la

interrupción del servicio del puerto. Sólo con ese consumo, la pérdida de oportunidades de producción implica la pérdida de ventas. En tercer lugar, el ajuste de los cuatro escenarios de riesgo planteados podría ser muy diferente en función de los diferentes casos. Por ejemplo, el proceso de entrega de la carga se ha simplificado, pues sólo se centra en el transporte por vía marítima. En el flujo de carga real la entrega de la carga debería incluir también el transporte terrestre. Los escenarios implementados dependen en gran medida de los servicios logísticos adoptados por las empresas. En cuarto lugar, al igual que en el mundo real, los sucesos de interrupción del servicio son considerados de forma súbita y resultan por tanto difíciles de predecir. El estudio asume que los responsables de la industria no tendrían tiempo suficiente para encontrar otra cadena de suministro para sustituir a la actualmente empleada (es decir, un puerto alternativo, transportista, proveedor, ruta, etc.). Por lo tanto, el coste de oportunidad de la carga el transporte no está incluido.

Por último, el enfoque actual no tiene en cuenta el coste de inventario extra debido a una permanencia mayor de la debida de la carga en el almacén. Se supone que el volumen de carga retrasada no es muy grande y el fabricante o empresa de logística tiene reservado espacio suficiente para esta. Por lo tanto, el coste de inventario de cargas retrasadas es mínimo.

De cara a futuros estudios se podrían investigar diferentes tipos de estrategias de mitigación de riesgo. Este estudio se centra en el papel de un puerto Gateway que sirve a las importaciones y exportaciones de varias industrias.

Anteriormente, estos mismos autores, (Y. Zhang, Siu, & Lam, L., 2015), evaluaron las pérdidas económicas producidas por la interrupción del servicio en un puerto debido al riesgo de vientos extremos. La estimación de los riesgos debidos a factores climáticos en puertos es una tarea difícil, no sólo debido a la complejidad del clima, sino también las variaciones diarias que se producen en el volumen de comercio en el puerto.

Los autores estiman las pérdidas económicas debidas a las interrupciones del puerto debidas a los efectos derivados de viento extremo y llevan a cabo un estudio de dos puertos seleccionados, Ningbo y Shanghai, ambos en China. La pérdida considera tanto la variación en el rendimiento de carga diaria así como el clima. El rendimiento se analiza en un análisis de regresión que representa tanto la tendencia a largo plazo como los componentes cíclicos anuales. La probabilidad de interrupción del servicio del puerto se estima a partir de un análisis del clima basado en el registro histórico en ambos puertos.

El estudio lleva a cabo el análisis de riesgos para los puertos de Shanghai y Ningbo considerando casos de viento extremo. Los modelos de regresión empleados incluidos tanto la tendencia a largo plazo como las condiciones cíclicas anuales se aplican para caracterizar el momento en que varía el rendimiento de las propiedades cada variable de la terminal. En base al registro de la velocidad del viento, se lleva a cabo un análisis

climático en ambos puertos para estimar el número potencial de días de interrupción del puerto relacionados con el viento entre cada mes. La pérdida económica debida a vientos extremos se calcula de acuerdo a cuatro categorías: pérdida de reputación, las pérdidas de las compañías navieras, las pérdidas de los transportistas y las pérdidas de los puertos. El resultado muestra que la pérdida para los puertos es la componente principal en el coste global. Una comparación general también se lleva a cabo con el puerto de Shenzhen. El clima estacional es el factor dominante en las evaluaciones del riesgo. La cuantificación de la pérdida potencial podría ayudar a los administradores de puertos a evaluar el rendimiento de los puertos ante los desastres por viento considerados.

Es importante señalar que esta investigación limita su ámbito de estudio a los contenedores en ambos puertos. La estimación sólo proporciona una medida cuantitativa de las terminales de contenedores específicos en los puertos de Shanghai y Ningbo. La carga real debe consistir en una amplia gama de tipos. Además, en la evaluación del impacto de la interrupción del servicio, se supone que los barcos se verán afectados por los retrasos relacionados con la interrupción, sin embargo en algunas terminales específicas se podría proporcionar la coordinación necesaria y realizar la re-planificación de las rutas de los buques después de la interrupción del servicio. La reasignación podría permitir al buque elegir un puerto alternativo dentro de la red de puertos existentes, lo cual permitiría reducir el coste inducido por la demora, los cuales no se han tenido en cuenta en el presente estudio. Aparte de estas, el trabajo se centra en la realización de una evaluación de las pérdidas directas debidas a la interrupción del puerto. Las pérdidas indirectas no se consideraron en el estudio.

3.3.3. Riesgos asociados a la mercancía

En el contexto del análisis del riesgo en instalaciones portuarias, el papel del análisis del riesgo para las mercancías es clave, dado que estas deben llegar en perfecto estado al puerto de destino y no perder su valor en términos comerciales.

(Kumar & Verruso, 2008) realizaron una investigación cuyo objetivo era evaluar el riesgo para la seguridad de los contenedores que entraban en los EUA. Según estos autores, es posible evitar riesgos en el sistema mediante el estudio de las áreas en las que la carga de los contenedores es manipulada y transportada, empleando para ello el marco de decisión propuesto para el manejo de carga fiable y segura y el sistema de envío.

Esto proporcionaría una información valiosa que se puede utilizar de manera efectiva para evitar y detectar un fallo en el sistema y una ocurrencia potencialmente catastrófica. La seguridad y la fiabilidad de la manipulación de contenedores de carga y el envío se reduce así a un error humano, principalmente, el sabotaje, el mal funcionamiento del equipo, y la falta de seguridad, que puede ser evitada a través de

los indicadores propuestos en cada uno de estos modos en los árboles de fallo. Aunque éstos son difíciles de mantener, sería necesario inspeccionarlos y mantenerlos a fin de evitar cualquier daño catastrófico importante para la industria de la logística global.

Los autores presentan un prototipo de un sencillo sistema de evaluación de riesgos que protege contra los posibles riesgos de seguridad en los envíos de contenedores de carga. El modelo propuesto se puede extrapolar para analizar los diferentes nodos y las capas de la red de transporte existente. Esta evaluación pretende ser una guía para determinar dónde deben asignarse los recursos dentro de la red, de la manera más efectiva para evitar un suceso catastrófico. La red de abastecimiento también requiere la integración de alta tecnología para incorporar el monitoreo y control sofisticado en todo el sistema. Las nuevas tecnologías también deben ser estudiadas desde la perspectiva de la eficacia de su incorporación al sistema. Debe realizarse un análisis comparativo entre las tecnologías actuales y futuras en el diseño de sistemas de monitorización y control mejorados para el transporte mundial de contenedores de carga.

(Vilko & Hallikas, 2012) realizaron un estudio de evaluación de riesgos en cadenas de suministro multimodales. Dicho estudio amplía la perspectiva de la gestión de riesgos en las cadenas de suministro marítimos multimodales teniendo en cuenta tanto las necesidades de la cadena de suministro como las de la seguridad del suministro a los clientes finales. El principal objetivo era doble: en primer lugar, identificar y evaluar los riesgos que afectan a los flujos de carga en el caso de la cadena de suministro en terminales marítimas multimodales, desde la perspectiva de la gestión de riesgos, y en segundo lugar, analizar el impacto de los riesgos en términos de retrasos.

Tras realizar una revisión de la literatura actual sobre las cadenas de suministro y gestión de riesgos marítimos en estas, se llevó a cabo la parte empírica de la investigación en dos etapas secuenciales que se solapaban. En la primera etapa del estudio de caso fueron entrevistados los representantes de las organizaciones que comprenden parte de la cadena de suministro que se desarrollan en el Golfo de Finlandia y que terminan en su parte continental. Estas entrevistas fueron semi-estructuradas y exploratorias. Estas entrevistas fueron semi-estructuradas y preliminares. La segunda etapa consistió en el mapeo y evaluación los riesgos identificados en función de sus resultados en la cadena de suministro. En tercer lugar se construyó un modelo de simulación sobre la base de los efectos de retraso debido a los riesgos identificados con el fin de investigar cualquier variación en la distribución de los resultados posibles de la cadena de suministro, su probabilidad, y sus valores subjetivos.

Dados los antecedentes de los entrevistados, ni la claridad conceptual de los riesgos, ni las fuentes de riesgo, ni los conductores fueron tomados en consideración; los entrevistados en vez respondieron con falsedades de causa y efecto.

Los riesgos impuestos a las diferentes partes de una cadena de suministro multimodal dependen de numerosos factores. La gestión eficaz del riesgo requiere una clara comprensión global del mismo. El aumento de la visibilidad y la cooperación en la cadena de suministro mejorarían la identificación de riesgos y por lo tanto serían más fáciles de manejar. Algunos de los operadores logísticos que fueron entrevistados habían dado ya pasos en esta dirección, pero la falta de confianza parecía demandar una mayor cooperación e intercambio de información entre las partes. Los riesgos identificados como más graves; conflictos laborales (huelgas) y situaciones con fuego y hielo en invierno, afectaron a toda la cadena y a muchas componentes de ella, siendo por lo tanto la cooperación muy beneficiosa en este contexto. La fuente más significativa de riesgo parecía relacionarse con el suministro, así como para el entorno operativo, y el efecto principal en la mayoría de los casos fue un retraso de tiempo: en otras palabras, el impacto más grande está en carga que es sensible al tiempo. Para las empresas que aplican el tratamiento del riesgo adecuado, la capacidad de mitigar o responder a estos riesgos podría llegar a ser un beneficio clave en la intensa competencia logística actual.

El resultado esperado del análisis de vulnerabilidad va de arriba a abajo y es el análisis de factores de riesgo en la cadena de suministro y su impacto, y una investigación más profunda sobre la relación entre el cumplimiento de las medidas de exposición al riesgo y la cadena de suministro, como es el tiempo. El trabajo estudia conjuntamente los generadores del riesgo y la incertidumbre en las cadenas de suministro, si bien normalmente se analizan por separado. La exposición en términos de probabilidad y de impacto proporciona una estructura sólida sobre la que explorar los riesgos en diferentes partes de la cadena. La simulación arroja luz sobre los condicionantes del riesgo y su impacto en el rendimiento de la cadena de suministro. El impacto del retraso se usa para modelar la exposición al riesgo en la cadena de suministro, caso de este estudio. Sin embargo, puede ser extremadamente difícil de obtener datos para aplicaciones de simulación, en las que las opiniones de expertos serían de gran valor.

Los enfoques para el análisis de riesgos adoptados en el estudio se basan en el conocimiento experto de unas pocas personas y en la evaluación subjetiva. Por tanto, el método del caso impone limitaciones. El estudio también tiene limitaciones en cuanto a la generalización, dado el tamaño de la muestra y la naturaleza subjetiva de los datos.

Los investigadores Mabrouki, Bellabdaoui, & Mousrij, (2013) estudiaron el problema de la gestión del riesgo operativo dentro de la actividad RO-RO en terminales portuarias. El enfoque se basa en tres pasos. En primer lugar, la identificación de factores de riesgo. La tormenta de ideas permitió encontrar trece riesgos importantes. Posteriormente un análisis de riesgos condujo a la determinación de la naturaleza y el

nivel de riesgo de la instalación, teniendo como objetivo describir cuantitativamente el riesgo.

Por último, selecciona los riesgos más probables, que son evaluados según el método del proceso analítico jerárquico (AHP) utilizado en el análisis de decisión multicriterio. El desarrollo de criterios y su ponderación, a continuación, les permitió escoger cuál de estas soluciones resultan de mayor interés. De esta forma se invita al tomador de decisiones o al planificador a adoptar planes de acción para corregir las alternativas más probables de riesgo para las terminales RO-RO.

En lo relativo a los riesgos asociados a la cadena de suministro de contenedores, (Van de Voort, Willis, Ortiz, & Martonosi, 2007) realizaron un estudio en 2007 cuyas conclusiones se resumen a continuación.

Durante las últimas décadas, el transporte de contenedores ha experimentado un auge con un crecimiento promedio anual de 9,3% el aumento de su cuota modal del 6,3% en 1980 a más del 25% en 2007. Los principales puertos de contenedores del mundo manejan actualmente más de 20 millones de unidades de 20 pies equivalentes (TEU) al año y han mostrado un crecimiento espectacular en los últimos años, con un desarrollo especialmente significativo del mismo en Asia. El flujo global de contenedores representa el elemento vital de las economías modernas, sin el cual no seríamos capaces de disfrutar de la forma de vida que tenemos. Esto es, desafortunadamente, uno de los criterios que conocen los terroristas para actuar a la hora de seleccionar sus objetivos, haciendo de la cadena de suministro mundial de contenedores un objetivo potencialmente atractivo.

Sin embargo, ¿qué amenazas son las más importantes en el entorno marítimo y cómo se deben gestionar los recursos para reducir los riesgos de estas? El análisis de riesgos (entendido este como una función de tres componentes: la amenaza, la vulnerabilidad, y consecuencia) proporciona un marco para priorizar las amenazas al sector marítimo. Para este propósito es necesario:

1. Evaluar las amenazas para determinar contra qué nos estamos protegiendo,
2. Evaluar vulnerabilidades.
3. Considerar las consecuencias de los ataques y las posibles interrupciones de cadenas de suministro.

En el contexto del transporte de contenedores, se consideran dos tipos de escenarios relevantes:

1. Los contenedores marítimos se utilizan para mercancías ilícitas de tráfico más allá de las fronteras de un país, especialmente cuando implican potencial detonación nuclear.

2. El sistema de transporte de mercancías en sí está gestionado con el fin de crear una interrupción ampliada de las operaciones en los puertos principales.

Dado que sólo del 5 al 6% de todos los contenedores manipulados en los puertos occidentales son inspeccionados físicamente, las posibilidades de interceptar un contenedor que transporta mercancías ilícitas son pequeñas. Una vez que un contenedor de transporte de contrabando ha eludido los controles de aduanas, que viajan rápido, haciendo zonas de influencia accesible dentro de horas a días. Estos tipos de escenarios se mueven hacia arriba en el ranking de evaluación del riesgo, sobre todo si las armas nucleares entran en juego. Sin embargo, a pesar de su deseo de utilizar este tipo de armas, los terroristas hasta el momento han demostrado poca capacidad para ejecutar ataques no convencionales a gran escala.

Si los terroristas atacaran la cadena de suministro, con el objetivo de interrumpir su funcionamiento, estas interrupciones podrían tener un gran impacto económico.

Los responsables políticos han tomado nota de estas amenazas y promulgado varias medidas para protegerse de ellos, tales como la implementación del Código internacional para la Protección de los Buques y de las Instalaciones Portuarias (PBIP), Iniciativa de Seguridad de Contenedores y Asociación Aduanas-Comercio contra el Terrorismo. La pregunta sigue siendo, sin embargo: ¿han conseguido estas medidas que estemos más seguros de los que estábamos antes?

Esta evaluación muestra que los enfoques actuales para la inspección de contenedores de carga que se mueven a través del sistema de transporte de contenedores son poco prácticos e imperfectos, debido al gran número de contenedores y los errores inherentes (tanto falsos positivos como falsos negativos) de las inspecciones con tecnología. Además, se demuestra que la introducción de nuevas tecnologías y soluciones innovadoras de procesos pueden superar estos problemas si se traducen en un menor número de falsos positivos. La metodología de evaluación de riesgos propuesta se ha aplicado para evaluar los riesgos de seguridad de la cadena de suministro de contenedores, así como la eficacia de las medidas que tienen como objetivo para asegurarla. Además, la metodología permite la clasificación de los riesgos y las contramedidas para identificar los más importantes y eficaces.

3.3.4. Riesgos asociados a la operación

Existe otro tipo de riesgos asociados a la operación que pueden influir en la seguridad de la manipulación de la carga, pudiendo producirse retrasos importantes en la carga y descarga de la mercancía, además de generarse un riesgo para la propia seguridad de las mercancías y las personas.

(Molina, 2014) desarrollo su tesis doctoral, "Caracterización de la agitación local y la respuesta oscilatoria de un buque mediante el uso de técnicas de visión artificial.

Aplicación al análisis de los umbrales operativos en líneas de atraque y amarre” en este ámbito de investigación.

El desarrollo de actividades de carga y descarga son parte de la esencia de la naturaleza funcional de un puerto, de las cuales derivan en gran medida los ingresos del mismo y la eficiencia de la cadena logística en su conjunto.

Las oscilaciones en el interior de una dársena y en una línea de atraque disminuyen la calidad de la estancia de las embarcaciones en puerto, reducen el rendimiento de la estiba de los buques y solicitan y fatigan las estructuras y los cuerpos flotantes amarrados.

Si los parámetros que definen la agitación local se aproximan a regiones de fallo o parada, el subsistema pierde rendimiento, fiabilidad y finalmente se paralizan las operaciones, produciéndose de este modo tiempos de inactividad.

Estas paradas operativas conllevan pérdidas económicas para la terminal y, consecuentemente, para el puerto.

Hoy día se dispone de vastas redes de monitorización destinadas a la caracterización del medio físico en el entorno de los puertos. Paralelamente, las operaciones de manipulación de cargas en las terminales se están dirigiendo hacia modelos de automatización o semi-automatización, que permiten no sólo la sistematización de procesos, sino también un profundo conocimiento del flujo de tareas. En este contexto hay un déficit de información sobre cómo afectan los diferentes forzadores del medio físico al rendimiento, la seguridad funcionalidad del proceso de manipulación de carga y descarga. Esto se debe en gran medida a la falta de registros dilatados en el tiempo que permitan correlacionar todos los aspectos mencionados de un modo particularizado para cada línea de atraque y amarre de un puerto.

En esta investigación se desarrolla una metodología de vídeo monitorización no intrusiva y de bajo coste basada en la aplicación de técnicas “pixel tool” y la obtención de los parámetros extrínsecos de una observación monofocal. Con ello se pretende poner en valor las infraestructuras de vídeo vigilancia de los puertos y de los laboratorios de experimentación a escala reducida, con el objeto de facilitar el estudio los umbrales operativos de las áreas de atraque y amarre.

Por su parte, (Gómez, 2015) desarrolló una interesante investigación en su tesis doctoral, elaborando una propuesta metodológica para la obtención de previsiones de parámetros operacionales y la evaluación riesgos operacionales en terminales de contenedores. Las terminales de contenedores son sistemas complejos en los que un elevado número de actores económicos interactúan para ofrecer servicios de alta calidad bajo una estricta planificación y objetivos económicos. Las conocidas como "terminales de nueva generación" están diseñadas para prestar servicio a los mega-buques, que requieren tasas de productividad que alcanzan los 300 movimientos/hora. Estas terminales han de satisfacer altos estándares dado que la competitividad entre

terminales es elevada. Asegurar la fiabilidad de las planificaciones del atraque es clave para atraer clientes, así como reducir al mínimo el tiempo que el buque permanece en el puerto. La planificación de las operaciones es más compleja que antaño, y las tolerancias para posibles errores, menores. En este contexto, las interrupciones operativas deben reducirse al mínimo. Las principales causas de dichas perturbaciones operacionales, y por lo tanto de incertidumbre, se identifican y caracterizan en esta investigación. Estudios adicionales, tanto teóricos como en sitios específicos, son necesarios para definir y caracterizar los modos de fallo y la suspensión del funcionamiento de las instalaciones de la terminal de contenedores.

Existe una escasa investigación para la determinación de la estructura de costos de las actividades de la terminal de contenedores, incluso en un campo tan importante como es la manipulación de la carga. Por esta razón, se propone aquí un enfoque alternativo, donde los impactos son evaluados de acuerdo a su capacidad de modificar los parámetros descriptivos de rendimiento de terminales, como la capacidad.

La disponibilidad de los registros operacionales y climáticos hace posible el desarrollo de modelos probabilísticos para caracterizar la incertidumbre en las operaciones de terminales de contenedores, y, en consecuencia, los análisis de riesgo se pueden llevar a cabo en base a esta información, y el modelado neuronal también se puede realizar para obtener predicciones operativas.

Las Redes Neuronales Artificiales son particularmente susceptibles a la modelización del comportamiento de los sistemas complejos y por lo general han demostrado un rendimiento predictivo superior en comparación con los métodos tradicionales, tales como técnicas de regresión.

Se ha validado el método propuesto para obtener predicciones de parámetros de funcionamiento en terminales de contenedores. La conclusión se confirma mediante un caso en estudio, en el que las previsiones de rendimiento de la nave se han obtenido en base a la información sobre el tamaño de la manga del buque.

Se verifica la hipótesis inicial sobre la influencia del clima en las operaciones, ya que la red neuronal mostró que los errores de formación más bajos se obtienen cuando se considera la velocidad media del viento.

Las variaciones a corto plazo en las operaciones producidas por el clima no han podido observarse en el caso debido a las diferencias en la frecuencia de muestreo entre la información operativa y climática.

La falta de información sobre las muestras resulta en errores de alto valor, aunque su frecuencia sea baja.

El sistema, concebido para integrarse en las condiciones de servicio, puede ser utilizado por los tomadores de decisiones para obtener planes de operaciones más precisas debido a la aleatoriedad inducida en las operaciones por factores climáticos

se combina con los valores adoptados por factores operacionales, proporcionando así información sobre el valor añadido para los planificadores. Esta herramienta ayudaría a mejorar la percepción de los planificadores de cómo las diferentes variables participan en las operaciones y adquirir experiencia afrontar nuevas condiciones de funcionamiento.

3.3.5. Riesgos asociados a variables políticas de seguridad

Se deben contemplar otros tipos de riesgos, asociados en este caso a las políticas de seguridad definidas por los estados. En este sentido (Yeo, Pak, & Yang, 2013) realizaron un análisis de los efectos dinámicos en los puertos que adoptan políticas de seguridad del puerto.

Según los autores, las variables políticas, como la definición de los niveles de seguridad en los puertos, afectan la eficiencia portuaria de una forma no-lineal, mientras que otros factores que afectan también a la eficiencia en los puertos, como el número de ataques, la superficie de patio del puerto y el número de puestos de trabajo portuarios tienen una relación estructural lineal. Sin embargo, hay una falta de estudios empíricos claros en este tema para proporcionar un indicador cuantitativo para que los responsables políticos puedan tomar una decisión racional.

Para investigar un caso real, se seleccionaron los puertos marítimos de Corea del Sur. El patrón de comercio de Corea depende en gran medida de las importaciones y exportaciones, lo que tiene un alto nivel de dependencia de los puertos. Por esta razón se seleccionan los puertos de Corea para mostrar los cambios de volumen de contenedores acorde con situaciones de seguridad dinámicas. Asimismo se ha observado que las tensiones militares en la península coreana han debilitado la productividad portuaria en términos de manejo de cargas de contenedores, ya que Corea ha adoptado un nivel de seguridad elevado en comparación con los países vecinos. Desde el punto de vista de la maximización del crecimiento económico, podría ser útil para evaluar los impactos de seguridad del puerto en volumen de carga de contenedores con el fin de dar a las partes interesadas implicaciones de puertos marítimos y para hacer frente a una complejidad global del puerto, específicamente en términos de problemas de seguridad. La Dinámica de Sistemas (SD) se ha utilizado para analizar la relación entre los niveles de seguridad de puertos y volumen de contenedores en este estudio. El uso de la SD demuestra los beneficios de simulaciones. El efecto dominó de la escalada de la protección portuaria se observan a lo largo de la productividad de todo un puerto.

En un sistema de este tipo, cualquier impacto negativo inadecuado puede aparentemente hacer entrar al puerto en una espiral de disminución de su competitividad.

Uno de los hallazgos de esta investigación es la configuración de los efectos cuantitativos de tiempo, coste, fiabilidad, y el nivel de seguridad en el atractivo del puerto y el volumen de contenedores. Mientras se exploran los impactos, el estudio aporta nuevas contribuciones a la literatura incluyendo el desarrollo de un Diagrama de Lazo Casual visual (CLD) entre los factores de evaluación, la representación de varios sub-modelos y la creación de escenarios de análisis valiosos. Los diagramas del lazo causales muestran las relaciones causa-efecto entre las variables de un sistema. El CLD se crea a través del intercambio de ideas y de entrevistas en profundidad con las partes interesadas en relación con las operaciones portuarias. Para mejorar la capacidad de realizar un análisis rápido del ¿qué pasaría si...? y para determinar las compensaciones en los niveles de seguridad de los puertos, los escenarios se diseñan incluyendo un modelo base, un modelo de escenario optimista, y un modelo de escenario pesimista. El CLD, los sub-modelos y el análisis de escenarios ofrecen una plataforma para nuevos estudios. A partir de la adaptación de la metodología en el contexto de los puertos marítimos de Corea, los autores demostraron que la carga de los costes de alta seguridad para un puerto puede iniciar una espiral de disminución de la competitividad, que a su vez se traduce en una pérdida significativa de cuota de mercado. Un exceso de un nivel de seguridad adecuado podría comenzar a revertir el atractivo del puerto. Los resultados cuantitativos de los volúmenes de contenedores obtenidos a partir de diferentes escenarios indican los beneficios económicos significativos de que podrían disfrutar los puertos marítimos de Corea mediante el mantenimiento de un nivel de seguridad más bajo (Nivel de seguridad 1 en el PBIP). Los resultados pueden generar una especial atención y un mayor interés en la investigación futura a los puertos de Corea, así como los puertos de otras regiones. Específicamente, la exploración de las soluciones a cuestiones tales como (1) la evaluación de la capacidad portuaria necesaria con arreglo a las fluctuación en los volúmenes de carga contenerizada en el futuro; (2) el suministro de análisis empíricos mediante el uso de datos financieros del puerto (3) análisis comparativo a largo plazo de la competitividad de los puertos de destino, puede facilitar el estudio económico de la protección portuaria de una manera cuantitativa. Asimismo se considera que un estudio “ad hoc” de la metodología basada en SD puede estimular el análisis cuantitativo de seguridad económica a partir de un rango más amplio de contexto portuario, promoviendo así la aplicación efectiva de las medidas de seguridad genéricas.

Figura 8. CFD de seguridad del puerto.

Fuente: Yeo, Pak, & Yang, 2013

3.3.6. Nuevas metodologías de evaluación de riesgos

Recientemente (Z. Yang et al., 2014) llevaron a cabo un estudio con el fin de realizar una aproximación cuantitativa del riesgo en la evaluación de la seguridad en instalaciones portuarias.

A lo largo de las últimas décadas, ha habido una preocupación generalizada ante la idea de que grupos terroristas puedan obtener fácilmente la capacidad para influir en el sector marítimo, incluyendo los puertos. A pesar de la existencia de investigaciones previas sobre la seguridad del puerto y el análisis del riesgo, poco ha se hecho en el desarrollo de una metodología generalmente aceptada para llevar a cabo la evaluación de la seguridad del puerto de una manera cuantitativa. Para hacer frente a dicha necesidad, este documento propone una metodología cuantitativa novedosa usando un enfoque de razonamiento probatorio difuso.

De hecho, el estudio es único y novedoso en cuanto al uso de entrevistas y cuestionarios para identificar los indicadores de rendimiento de seguridad claves en la práctica de seguridad del puerto y organizarlos eficazmente con una jerarquía. La investigación revisa el estado actual de la seguridad de puerto para identificar la

necesidad de desarrollar un método de evaluación cuantitativa del riesgo. Tras el desarrollo de un método de evaluación de la protección innovador, se llevan cabo un estudio del caso y un análisis de sensibilidad para validar los resultados. El desarrollo de una metodología cuantitativa es capaz de valorar la credibilidad de la identificación de amenazas, análisis de riesgos, el control de la seguridad y las mejoras, pudiendo disfrutar de beneficios sustanciales, ocupándose de todos los aspectos de la protección de la instalación portuaria de una manera integrada y cuantitativa, permitiendo a las amenazas que aún no se han producido, ser consideradas adecuadamente.

El método se puede adaptar para hacer frente a los requisitos específicos de los usuarios industriales en un contexto amplio (por ejemplo ataque terrorista en un canal) con el fin de reforzar su validez y flexibilidad.

Además el estudio ofrece un valor sustancial a los estudiosos, los responsables de la planificación y los encargados de formular políticas en el diseño, planificación y evaluación de medidas de seguridad eficaces y estrategias de seguridad, reduciendo así el riesgo para la seguridad de los sistemas de transporte y la cadena de suministro en todo el mundo.

Capítulo | **4**

Metodología

4.METODOLOGÍA

4.1. Introducción

Una vez revisado el Estado del Conocimiento relativo a la evaluación del riesgo en instalaciones portuarias, se llevó a cabo la investigación para el desarrollo del objeto principal de esta Tesis, el enunciado de una nueva metodología para la evaluación del riesgo en instalaciones portuarias mediante la obtención de nuevos parámetros.

Como ya se ha explicado anteriormente, se trata de mejorar el conocimiento del riesgo real que amenaza una instalación portuaria basándose en datos, es decir en información obtenida tanto del explotador de las instalaciones portuarias, como de la Guardia Civil, máximo responsable de la seguridad portuaria en los puertos comerciales españoles.

El análisis del riesgo que se pretende realizar se centra en las principales amenazas de destrucción de la infraestructura y ataques a personas, dejando de lado aquellas otras que incurran en otros aspectos del funcionamiento del puerto.

Tal y como ya se citó anteriormente, en la actualidad existen numerosas metodologías de evaluación del riesgo en diferentes tipos de infraestructuras, si bien aquellas destinadas de forma específica a la evaluación en instalaciones portuarias son escasas, como ya se ha mostrado en el *Capítulo 3 Estado del Conocimiento*, y en ningún caso se han realizado considerando las opiniones de los responsables de la seguridad o empleando datos estadísticos que signifiquen de una forma clara las principales amenazas o las instalaciones más vulnerables.

La investigación se efectuó mediante la aplicación del Método Científico, si bien el tema objeto de la misma; la evaluación de riesgos en puertos, es un tema actual y de escasa antigüedad investigadora, lo cual supuso la necesidad de incorporar otro método de desarrollo que diera soporte al científico. La carencia habitual de estadísticas relevantes de sucesos contra la seguridad condujo a la consideración del empleo del Método Delphi o Método Experto, dado que sí existen en el sector de la seguridad numerosos profesionales con amplia experiencia y una clara visión de que aspectos son mejorables y en qué sentido y por tanto son quienes pueden aportar más a esta investigación.

Conjugando ambos métodos y mediante el estudio de datos estadísticos de seguridad en los principales puertos comerciales españoles, se obtuvo información de gran interés, como son las principales amenazas reales que deben abordar los puertos y por ende la evaluación de los riesgos que de estas se deriven.

La metodología obtenida se define mediante cuestiones clave, como son la validez de los datos de seguridad, al tratarse de datos reales del Ministerio del Interior de España y el conocimiento de la realidad de las terminales en términos de seguridad, de amenazas y de su frecuencia. De ella se podrá obtener una idea global del valor de riesgo de cada instalación portuaria evaluada.

4.2. Etapas de la metodología de la investigación

La metodología de la investigación se divide en varias etapas con el fin de obtener la propuesta metodológica de evaluación del riesgo. En el desarrollo de la investigación se emplean diferentes métodos y herramientas que más adelante se describen en detalle.

La metodología se estructura en las siguientes cuatro etapas que más adelante se desarrollan:

Etapa 1. Definición de criterios y selección de metodologías a considerar

- Definición de los criterios de selección de las metodologías. Para la realización de un análisis que pueda cumplir con los objetivos de la Tesis se requiere la definición de una serie de criterios que permitan elegir adecuadamente qué metodologías resultan de interés de las previamente descritas.
- Selección de metodologías de interés para la investigación. Una vez definidos los criterios de selección, se eligen las metodologías de mayor relevancia para la investigación.

Etapa 2. Análisis y evaluación comparativa de las metodologías seleccionadas

- Análisis de metodologías seleccionadas. Se analizan las diferentes metodologías, evaluando aspectos de interés para la investigación, como son su forma de aplicación, la forma de valoración de las amenazas, vulnerabilidades y consecuencias, etc.
- Evaluación comparativa de los parámetros de las metodologías. Se seleccionan los parámetros que definen cada una de ellas y se comparan cualitativamente, buscando similitudes y diferencias entre estos.

Etapa 3. Identificación de nuevos parámetros a considerar

- Mediante el uso de herramientas como la elaboración de encuestas o el análisis de estadísticas de seguridad, se determinarán aquellos posibles aspectos de relevancia para la evaluación de la seguridad no considerados adecuadamente o novedosos.
- Una vez identificados los aspectos novedosos se trata de cuantificar su influencia en la evaluación del riesgo mediante su definición con nuevos

parámetros.

- Definidos los parámetros nuevos, y siguiendo un método basado en la evaluación del riesgo descrito por W.T. Fine (1971) se validan los resultados a través de un panel de expertos.

Etapas 4. Elaboración de la Propuesta Metodológica

- Finalmente se enuncia la propuesta metodológica para la evaluación del riesgo.

En el esquema que aparece a continuación se representa la metodología desarrollada.

Figura 9. Etapas de la metodología de la investigación.

Fuente: Elaboración propia

4.3. Métodos y herramientas de investigación

En el presente apartado se explican los métodos y las herramientas empleadas en el desarrollo de esta Tesis Doctoral, sus características y su correcta aplicación en función de los resultados a obtener.

La cuestión principal que se plantea en la investigación, como base para el enunciado de una propuesta metodológica de evaluación del riesgo, es si existen nuevos parámetros a considerar en la evaluación del riesgo en instalaciones portuarias. Para ello se consideran, tal y como se indicó anteriormente, una serie de objetivos previos que tras su consecución darán paso al cumplimiento del objetivo principal, el enunciado de la propuesta.

Los resultados a obtener se corresponden con el objetivo principal y los previos planteados en la PARTE 1 de la investigación. En la Figura 10 se detallan los objetivos planteados, indicando las preguntas que han dado lugar a estos.

Figura 10. Preguntas y objetivos que determinan las actividades y herramientas aplicadas.

Fuente: Elaboración propia

El desarrollo de este apartado se estructura en función de los resultados a obtener, en los seis apartados a desarrollar, que se corresponden con las cuatro etapas que conformarán el desarrollo de la propuesta metodológica.

Antes de comenzar a describir cada uno de las etapas que constituyen el desarrollo de la investigación, es conveniente describir el proceso sistemático seguido, indicando sus actividades, en relación al significado otorgado a cada etapa, así como también las herramientas que se utilizan y los resultados a obtener en cada una de las etapas.

En la Figura 11 se muestran los métodos y herramientas del desarrollo de la investigación que se detallan posteriormente.

ETAPAS DE LA INVESTIGACIÓN	MÉTODOS / HERRAMIENTAS
Definición de criterios y selección de metodologías de interés	Recopilar y revisar bibliografía
	Método deductivo
Análisis y evaluación comparativa de metodologías	Método comparativo
Identificación preliminar de nuevos parámetros a considerar	Encuestas al Sistema Portuario Español y Análisis de estadísticas de seguridad
	Método inductivo
Definición de nuevos parámetros y enunciado de una propuesta metodológica	Método Delphi
	Aplicación a una instalación portuaria

Figura 11. Métodos y herramientas. Fuente: Elaboración propia

4.3.1. Recopilación y revisión bibliográfica

Una vez definido el objeto de la investigación se trata de realizar el análisis preliminar y la búsqueda de la bibliografía relacionada con el objeto de la investigación. Posteriormente, y una vez recopilada dicha bibliografía relacionada se revisa en detalle con el objeto de seleccionar aquella bibliografía de mejor se ajusta a los objetivos de la investigación y que por tanto aporta mayor información de partida a esta.

4.3.2.Método deductivo

El método deductivo o la deducción, es uno de los métodos más usados a instancias de lograr obtener, conclusiones sobre diversas cuestiones. El rasgo distintivo de este método científico es que las conclusiones siempre se hayan impresas en las premisas, es decir, es posible inferir a la conclusión de las proposiciones que conforman un argumento, de ellas y solamente de ellas deviene.

Este método no es algo que la modernidad trajo consigo ni mucho menos sino que se trata de un método que ya era referenciado en la antigüedad clásica por filósofos de la talla de Aristóteles.

Por otra parte, la deducción, siempre parte de una cuestión o ley general para llegar a lo particular, o sea, va de lo general a lo particular y esto es lo que lo enfrenta al método inductivo que se mueve en el lado opuesto: de lo particular a lo general.

Un rasgo diferencial de este método es la utilización que hace de diferentes herramientas y elementos para demostrar o esclarecer cuestiones. Esquemas, cuadros gráficos, sinopsis, entre otros, que recogen las diversas proposiciones así como también las relaciones que se establecen entre ellas y que son las asistentes ideales en este sentido

En este caso su aplicación servirá para deducir, en base a los criterios definidos previamente, que metodologías cumplen con los criterios a considerar en la selección de alternativas, y por tanto servirá como ayuda para una selección adecuada de las metodologías a considerar para el objeto de la investigación.

4.3.3.Método comparativo

Este método científico es un procedimiento sistemático y ordenado para examinar relaciones, semejanzas y diferencias entre dos o más objetos o fenómenos con la intención de extraer determinadas conclusiones.

Su aplicación se considera en la evaluación de las metodologías seleccionadas para la investigación. Se trata de realizar una evaluación que refleje las cualidades de interés de cada metodología para la investigación, como puede ser la estructura de evaluación del riesgo, la forma de evaluación de las amenazas, su forma de aplicación, sencillez, etc. Para ello se evalúan las diferentes ventajas y desventajas que, a juicio del autor, y en base a los objetivos de la tesis, poseen cada una de estas. Posteriormente se realizará una evaluación comparativa de los parámetros de las metodologías consideradas siguiendo el mismo método.

4.3.4. Encuesta al Sistema Portuario Español

4.3.4.1. Objetivo de la encuesta

La encuesta tiene por objetivo facilitar una visión de la seguridad aplicada desde la perspectiva del Sistema Portuario Español, orientando así las preguntas a aspectos clave como son las amenazas y las vulnerabilidades más destacables en las instalaciones.

En su redacción se tomaron en consideración las cuestiones de relevancia que se dedujeron de las diferentes metodologías consideradas para la investigación y que sirvieron para el planteamiento de algunas cuestiones de la encuesta.

La encuesta se preparó dirigiéndola a los responsables de seguridad de las instalaciones.

4.3.4.2. Estructura de la encuesta

Se estructuró planteando inicialmente una serie corta de preguntas dirigidas a averiguar el grado de conocimiento de la metodología aplicable en España para la evaluación de riesgos y de su contenido por parte de los responsables de seguridad de los puertos.

Posteriormente se realizaron una serie de preguntas encaminadas a conocer las amenazas y vulnerabilidades más frecuentes en las instalaciones a juicio de estos, así como la discriminación entre amenazas a la mercancía o a las personas.

Se plantearon además varias cuestiones con el objetivo de conocer las instalaciones que requieren un mayor grado de protección en la instalación, así como la valoración de la accesibilidad y la disposición de las instalaciones en el conjunto del puerto.

Por último se plantearon cuestiones relativas al grado de confort del encuestado respecto del nivel de seguridad actual de la instalación y si éste considera que es mejorable.

Se pretende de esta forma con las preguntas tener la perspectiva directa de la seguridad en los puertos españoles, años después de la puesta en marcha e implantación del Código PBIP y de los Planes de Seguridad y Protección correspondientes, así como averiguar cómo consideran los responsables de la seguridad que se podría mejorar la evaluación actual del riesgo.

La encuesta y las respuestas recibidas se incluyen en el *Anexo 2. Encuesta al Sistema Portuario Español*.

4.3.5. Análisis de las estadísticas de seguridad

Una herramienta importante para esta investigación es la obtención y análisis de datos estadísticos de seguridad del Sistema Portuario Español, que servirán como referencia de datos históricos de amenazas para la seguridad de las infraestructuras portuarias.

Para ello se contactó con la Dirección General de la Guardia Civil, en adelante DGGC, y en particular con la Jefatura del Servicio de Costas y Fronteras, responsable de la seguridad en los puertos comerciales de España.

4.3.6. Método inductivo

El método inductivo es el método científico que partiendo de unas hipótesis o unos antecedentes en particular, alcanza unas conclusiones generales. Se trata del método científico más usual, en el que pueden distinguirse cuatro pasos esenciales: la observación de los hechos para su registro; la clasificación y el estudio de estos hechos; la derivación inductiva que parte de los hechos y permite llegar a una generalización; y la contrastación.

El método inductivo es aquel método científico que alcanza conclusiones generales partiendo de hipótesis o antecedentes en particular. Fuentes expresan que este método originalmente puede ser asociado a estudios de Francis Bacon a inicios del siglo XVII.

El método inductivo suele basarse en la observación y la experimentación de hechos y acciones concretas para así poder llegar a una resolución o conclusión general sobre estos; es decir en este proceso se comienza por los datos y finaliza llegando a una teoría, por lo tanto se puede decir que asciende de lo particular a lo general. En el método inductivo se exponen leyes generales acerca del comportamiento o la conducta de los objetos partiendo específicamente de la observación de casos particulares que se producen durante el experimento

La metodología utilizada para la realización de este proceso puede resumirse en cuatro pasos, los cuales comprenden:

- La observación de los hechos o acciones y registro de ellos, la indagación científica da inicio siempre partiendo de un fenómeno en particular, que no posee una explicación propia dentro de los posibles conocimientos científicos existentes en dado momento;
- La elaboración de una hipótesis o el análisis de lo observado anteriormente, aquí se forma una posible explicación y posible definición de lo observado;

- En la tercera parte del proceso se presenta la deducción de predicciones o la clasificación de los fundamentos anteriormente obtenidos, estas predicciones se formulan a partir de la hipótesis;
- Finalmente el cuarto paso se pone en marcha el experimento, y encontramos la representación de los enunciados universales derivados del proceso de investigación que se realizó.

En esta etapa de la investigación, y una vez realizada la encuesta al sector portuario y el análisis de las estadísticas de seguridad, se aplica el método inductivo para poder identificar nuevos parámetros a considerar en la evaluación del riesgo.

4.3.7. Método Delphi

En el desarrollo de la investigación, se ha considerado que una forma adecuada de realizar la validación de resultados previos es la aplicación del denominado Método Delphi.

El objetivo del Método Delphi es la consecución de un consenso basado en la discusión entre expertos mediante un proceso interactivo. Su funcionamiento se basa en la elaboración de un cuestionario que ha de ser contestado por cada experto. Una vez analizados los resultados globales de este, se vuelve a realizar otro cuestionario para ser contestado de nuevo por los mismos expertos, tras darles a conocer los resultados obtenidos en la anterior consulta. El proceso puede repetirse varias veces hasta alcanzar cierto nivel de consenso.

El método Delphi pretende extraer y maximizar las ventajas que presentan los métodos basados en grupos de expertos y minimizar sus inconvenientes. Para ello, se aprovecha la sinergia del debate en el grupo y se eliminan las interacciones sociales indeseables que existen dentro de todo grupo. De esta forma se espera obtener un consenso lo más fiable posible del grupo de expertos.

Esta metodología de predicción utiliza juicios de expertos en tecnología o procesos sociales considerando las respuestas a un cuestionario para examinar las probables orientaciones del desarrollo de tecnologías específicas u otro tipo de soluciones que requieran criterio de expertos para su consecución. El resumen de los juicios de los expertos (en las formas de evaluaciones cuantitativas y comentarios escritos) se provee a modo de retroalimentación a los mismos expertos como partes de una ronda siguiente de cuestionario (next-round).

A continuación, los expertos reevalúan sus opiniones a la luz de esta información, y generalmente se produce un consenso de grupo. La técnica Delphi se basa en conceptos firmes para sacar conclusiones con argumentos soportados.

Se trata de obtener el mayor consenso posible en la respuesta teniendo en cuenta la calidad del juicio del grupo, cuya opinión es considerada igual o mejor que las opiniones individuales.

Este método presenta tres características fundamentales:

- Anonimato; durante un Delphi ningún experto conoce la identidad de los otros que componen el grupo de debate.
- Iteración y realimentación controlada; la iteración se consigue al presentar varias veces el mismo cuestionario
- Respuesta del grupo en forma estadística; la información que se presenta a los expertos no es sólo el punto de vista de la mayoría, sino que se presentan todas las opiniones, ya que el análisis del cuestionario permite conocer la respuesta estadística.

En la realización de un análisis Delphi aparece una terminología específica, que denomina a los distintos elementos presentes en el método, o a cada una de sus fases:

- Panel: es el conjunto de expertos que toma parte en el Delphi
- Moderador: es la persona responsable de recoger las respuestas del panel y preparar los cuestionarios
- Cuestionario: el cuestionario es el documento que se envía a los expertos. No es sólo un documento que contiene una lista de preguntas, sino que es el documento con el que se consigue que los expertos interactúen, ya que en él se presentarán los resultados de anteriores circulaciones
- Circulación: Es cada uno de los sucesivos cuestionarios que se presenta al grupo de expertos.

Antes de iniciar un Delphi se realizan una serie de tareas previas, como son:

- Delimitar el contexto y el horizonte temporal en el que se desea realizar la previsión sobre el tema en estudio.
- Seleccionar el panel de expertos y conseguir su compromiso de colaboración.
- Las personas elegidas no sólo deben ser grandes conocedores del tema sobre el que se realiza el estudio, sino que deben presentar una pluralidad en sus planteamientos. Esta pluralidad debe evitar la aparición de sesgos en la información disponible en el panel.
- Explicar a los expertos en qué consiste el método. Con esto se pretende conseguir la obtención de previsiones fiables, pues los expertos van a conocer en todo momento cuál es el objetivo de cada uno de los procesos que requiere la metodología.

Para la selección de los expertos previamente se constató la experiencia en el área de cada uno de ellos, así como el interés de estos en el tema en investigación, explicándoles además la importancia de la investigación para esta área y las implicaciones futuras que podría tener en la mejora de la evaluación del riesgo en puertos. De esta forma sus aportaciones, serían más relevantes y se aseguraría su participación en las sucesivas rondas.

Se preparó una lista de expertos que cumplieran con las cualidades necesarias para aportar un criterio experimentado a las cuestiones planteadas por la investigación, siendo principalmente consultores en seguridad, responsables de seguridad en puertos, directores de puertos, etc.

Se contactó con ellos a través del correo electrónico, las respuestas fueron rápidas y casi todos ellos aceptaron participar. Se envió a cada uno de ellos un primer mensaje de invitación a participar en el análisis, así como los objetivos de la investigación, y se les planteaban los objetivos de la investigación, además de algunos datos sobre el investigador. Este sistema agiliza enormemente el proceso, no sólo en cuanto a la velocidad de comunicación, sino también porque facilita el acceso a personas que están muy ocupadas, que ostentan cargos importantes o viajan mucho, como es el caso de la mayoría de los expertos consultados en este estudio.

4.3.8. Aplicación a una instalación portuaria

Una vez obtenidos los parámetros y enunciada la propuesta metodológica, se propone su aplicación al caso específico de una instalación portuaria (en varias de sus terminales portuarias), con el fin de validar los resultados. Para ello se evalúan las amenazas consideradas en un puerto escogido previamente, aplicándose la propuesta metodológica resultante, analizándose posteriormente los resultados y obteniendo unas conclusiones.

4.4. Desarrollo de las etapas de la metodología

A continuación se desarrollan las etapas de la metodología, describiéndose sus objetivos y alcance.

4.4.1. Etapa 1. Definición de criterios y selección de metodologías a considerar

En el *Capítulo 3 Estado del Conocimiento*, apartado 3.2. *Evaluación de riesgos en infraestructuras*, se recogen las principales metodologías de aplicación a la evaluación de riesgos en infraestructuras y que el autor ha considerado de interés reflejar en el estado de la cuestión de la investigación. Se trata de catorce metodologías de entre

las que tres son de aplicación específica a instalaciones portuarias. Una vez descritas dichas metodologías de interés para la investigación, se deben definir los criterios con los que poder evaluar comparativamente las metodologías de mayor interés de entre las catorce descritas.

En base a sus características y a los objetivos de la investigación se definen unos criterios con el fin de escoger aquellas de mayor interés para la investigación por su configuración, alcance, etc., comparándolas en detalle.

4.4.2.Etapa 2. Análisis y evaluación comparativa de las metodologías seleccionadas

Con el fin de obtener una mayor información y más práctica acerca de las características, detalle del ámbito de aplicación, formato de presentación del resultado de la evaluación del riesgo, alcance de la evaluación, etc., se analizan las metodologías de forma cualitativa con el fin de obtener así sus ventajas e inconvenientes, en base a los criterios expuestos anteriormente. Esta evaluación pretender servir como referencia para definir una propuesta metodológica posteriormente, basándose así en las cualidades de las metodologías analizadas.

La comparativa se realiza en dos sentidos. En primer lugar se analizan cuestiones como:

- Método de evaluación del riesgo empleado.
- Forma de valoración del riesgo, ¿cualitativa o cuantitativa?
- Sencillez y facilidad de aplicación.
- ¿Considera la probabilidad del suceso?
- Tipología de amenazas consideradas, ¿se especifican?, ¿tipos?
- Identificación precisa de las vulnerabilidades con diferentes índices *ad hoc* para cada vulnerabilidad
- ¿Desglose del análisis de las vulnerabilidades por índices o análisis global de estas?
- Esquema de determinación de las consecuencias, ¿se valoran específicamente o de forma global?

Posteriormente y una vez realizada la comparación cualitativa de las características de las metodologías, se comparan los parámetros que definen estas, con el fin de

conocer las similitudes, diferencias y especialmente el alcance que proporcionan a la evaluación de la seguridad cada una de las metodologías.

La segunda parte de la comparativa entre metodologías consiste en la aplicación del Método Deductivo para evaluar el alcance de los parámetros que cada de ellas emplea en la definición de su valoración de las amenazas, las vulnerabilidades y las consecuencias, los aspectos particulares considerados en estos, así como su forma de valoración parcial o la valoración global del riesgo.

El resultado se plasma en una tabla comparativa que resume los índices estudiados y que se muestra en el *Apartado 5 Resultados*.

Los parámetros a comparar son los descritos para cada una de las metodologías seleccionadas en el *Anexo 1 Metodologías consideradas*.

4.4.3. Etapa 3. Identificación de nuevos parámetros

Los nuevos parámetros a considerar se determinan en base a las conclusiones obtenidas del análisis pormenorizado realizado en las Etapas 1 y 2 de la Metodología y a las conclusiones derivadas de la opinión del Sector Portuario Español ante el funcionamiento de la seguridad en las instalaciones portuarias, a través de la opinión de expertos en seguridad, respecto a aquellas cuestiones que a su juicio son susceptibles de mejora en el esquema actual de evaluación del riesgo asociado a la seguridad portuaria.

Asimismo se realiza el análisis de las estadísticas de seguridad a través de la cual se pretende obtener una aproximación mayor a la realidad de la seguridad mediante el estudio de datos reales de amenazas.

4.4.3.1. Encuesta al Sistema Portuario Español

La encuesta realizada se estructuró en 18 preguntas y fue enviada a los 28 Autoridades Portuarias españolas, recibándose contestación de 15 puertos.

La encuesta se formuló y se dirigió personalmente a los responsables de seguridad de los Puertos, una vez identificados personalmente estos, con el fin de que las respuestas fueran ofrecidas por expertos con un conocimiento elevado de las cuestiones que se plantean en la encuesta y que por tanto la no respuesta a alguna de las cuestiones sea debida a que no se tienen datos sobre la misma y no a desconocimiento sobre la misma.

La encuesta realizada se puede consultar en el *Anexo 2 Encuesta al Sistema Portuario Español*, donde se incluye el modelo de encuesta enviada a los diferentes puertos que componen el Sistema Portuario.

4.4.3.2. Análisis de Estadísticas de Seguridad

Una vez realizada la encuesta se procede al análisis de los “Boletines de Seguridad” que como ya se indicó, son las estadísticas de sucesos contra la seguridad en los puertos españoles que emite mensual e internamente la Guardia Civil, a través de su Jefatura de Costas y Fronteras, como responsable directo de la seguridad en los puertos de interés general españoles

Los boletines recogen para cada puerto numerosas incidencias de todo tipo; accidentes, incidentes contra el medio ambiente y contaminación marina, delincuencia común, inmigración ilegal, conflictividad socio-laboral, terrorismo, tráfico ilícito, riesgos sanitarios, vulnerabilidad de los sistemas de seguridad, etc. Conviene aclarar que la inmigración ilegal es un problema de Estado, y que por tanto no se produce de manera exclusiva en los puertos, si bien estos son altamente sensibles a aquella, y que por tanto no se trata este problema solo en ellos.

Si bien los actos delictivos registrados son numerosos en su tipología y variedad, no todos son de interés para esta investigación, seleccionándose solo los tipos adecuados al objeto de la tesis.

En el análisis se comprueba que, simultáneamente y de forma complementaria a las amenazas descritas, existen otras de gran interés por su frecuencia y repercusiones económicas sobre la mercancía y/o la instalación portuaria. Se trata de las siguientes:

- Inmigración ilegal
- Intrusiones en el puerto (robo, hurtos...)
- Ataques terroristas
- Conflictos socio-laborales
- Sabotaje

Si bien se consideran el robo, el hurto y el sabotaje como delitos derivados de la intrusión en el puerto en este caso al ser los datos recogidos en las estadísticas, no son estos los únicos delitos posibles derivados de la intrusión, pudiéndose dar otros, como es la colocación de explosivos, disparos, etc.

Los problemas de conflictividad laboral por su parte suelen llevar aparejados deterioros físicos de la infraestructura y afecciones a la operación portuaria.

Los resultados de este análisis se muestran en el *Apartado 7 Resultados*.

4.4.3.3. Identificación de nuevos parámetros

Como resultado final de las Etapas 2 y 3 de la metodología, se identifican de forma preliminar aquellos aspectos que a juicio del investigador resultarán de interés recoger posteriormente en forma de nuevos parámetros de la propuesta metodológica de

evaluación del riesgo en instalaciones portuarias que se formulará más adelante. Estos aspectos se recogen en el apartado 5. *Resultados*.

Una vez identificados los nuevos aspectos a considerar a continuación se trata de validar estos mediante el enunciado de un parámetro que describa cada uno de ellos y que permita valorarlo posteriormente en la propuesta metodológica.

4.4.4. Etapa 4. Elaboración de la Propuesta Metodológica

La propuesta metodológica se basará, como ya se citó con anterioridad en métodos de estimación del riesgo de tipo simplificado, y en particular se seguirá el método de Fine, W. T. (1971) para su formulación y estructura, el cual considera que el riesgo es el resultado de considerar los efectos de las amenazas consideradas, las vulnerabilidades que se dan en la infraestructura ante dichas amenazas y las consecuencias resultantes para aquellas. Además se consideran otros aspectos derivados del estudio de otras metodologías empleadas en la estimación del riesgo.

Asimismo en esta etapa se definen y justifican aquellos otros aspectos o criterios empleados en la definición de la propuesta metodológica, los cuales darán forma a la misma.

Una vez definidos los parámetros y demás propuestas, se someten al criterio experto para su validación y posterior empleo en la formulación de la propuesta metodológica.

Capítulo 5

Resultados

5.RESULTADOS

A continuación se muestran los resultados de la investigación ordenados en base a las etapas que componen la metodología de la investigación, descritas en el apartado 4.2. *Etapas de la metodología de la investigación.*

5.1. Etapa 1. Definición de criterios y selección de metodologías a considerar

5.1.1.Criterios propuestos

Como resultado de la *Etapa 1. Definición de criterios y selección de metodologías a considerar*, y en base a los objetivos de la investigación, se definen los criterios de selección siguientes:

1. El objetivo de la metodología se centra en la evaluación de la seguridad ante actos terroristas, sabotajes, intrusismo etc., dejando de lado otro tipo de riesgos de menor interés para la investigación (informáticos, climáticos, operacionales, etc.).
2. Su aplicación es específica para instalaciones portuarias o infraestructuras con múltiples instalaciones y/o distribución de elementos, como es el caso de las instalaciones aeroportuarias.
3. La estimación del riesgo se realiza mediante la aplicación de métodos simplificados.

5.1.2.Metodologías seleccionadas

En base a dichos criterios se seleccionan una serie de metodologías de interés para su análisis comparativo y su consideración como base de partida de la investigación.

A continuación se resumen y justifica su selección para el estudio en detalle:

1. AERONÁUTICA CIVIL (OACI, COLOMBIA). Se trata de la Metodología de la OACI en Seguridad de la Aviación, aplicada en los aeropuertos de Colombia y otros tres países de la región. Es una metodología con una probada validez en esos países y que cumple todos los criterios propuestos para su selección; considera las amenazas

seleccionadas (criterio 1), se aplica a instalaciones aeroportuarias (criterio 2), y evalúa el riesgo a través de un método simplificado (criterio 3). Asimismo Colombia es un país con graves problemas de seguridad debidos a la existencia de grupos terroristas desde hace décadas y que por tanto resulta interesante considerar.

2. CARVER (Ejército de los EEUU). La metodología CARVER es una metodología de amplio uso y que ya ha sido empleada específicamente en evaluaciones de riesgos en entornos portuarios (del continente americano), cuya bondad ha quedado probada sobradamente, habiendo servido además como base para el desarrollo de otras metodologías como SECUREPORT, todo lo cual le da una validez y una credibilidad para su consideración. Además cumple todos los criterios propuestos para su selección; considera las amenazas seleccionadas (criterio 1), se puede aplicar a instalaciones portuarias (criterio 2), y evalúa el riesgo a través de un método simplificado (criterio 3).

3. RBDM. *Navigation and Vessel Inspection*. (Servicio de Guardacostas de EUA.). La metodología seguida por los puertos de los EEUU (2003) es una metodología que tiene un amplio ámbito de aplicación, puesto que su uso trasciende de las fronteras del propio EEUU, habiéndose implantado en la práctica mayoría de los países iberoamericanos, debido a las relaciones comerciales por vía marítima con los EUA y a las exigencias de seguridad en algunos casos con el movimiento de mercancías en origen en terceros países y con destino a los puertos de dicho país. Asimismo cumple también con los criterios propuestos para ser escogida; considera las amenazas seleccionadas (criterio 1), es de aplicación exclusiva a instalaciones portuarias (criterio 2), y evalúa el riesgo a través de un método simplificado (criterio 3).

4. SECUREPORT (Puertos del Estado, España). La metodología española, denominada así por su desarrollo específico para el ámbito portuario español fue desarrollada por Puertos del Estado siendo aprobada y puesta en práctica en 2004 en los 46 puertos de interés general de España. Su consideración y selección para la evaluación específica se justifica por varios motivos, el principal es que considera las amenazas seleccionadas (criterio 1), se trata además de la metodología aplicable en los puertos españoles (criterio 2) y por tanto su interés es evidente, y evalúa el riesgo a través de un método simplificado (criterio 3). Por otra parte la metodología se desarrolla siguiendo el formato de cálculo de CARVER, y por tanto en este sentido, su interés en la evaluación también es claro.

5. THREAT AND RISK ANALYSIS MATRIX (TRAM). Organización Internacional del Trabajo (OIT) y Organización Marítima Internacional (OMI). Esta metodología es la originalmente propuesta por la OIT/OMI y por tanto es la referencia base para el estudio y valoración de riesgos en instalaciones portuarias en el mundo, por ello se justifica su consideración en el estudio. Sin duda cumple también con los criterios

propuestos para ser escogida; considera las amenazas seleccionadas (criterio 1), es de aplicación exclusiva a instalaciones portuarias (criterio 2), y evalúa el riesgo a través de un método simplificado (criterio 3).

5.2. Etapa 2. Análisis y evaluación comparativa de las metodologías seleccionadas

El análisis realizado es de carácter cualitativo, mostrándose las ventajas e inconvenientes de cada una de ellas para su empleo en la estimación del riesgo.

A continuación se muestran los resultados del análisis de las diferentes metodologías consideradas.

5.2.1. AERONÁUTICA CIVIL (Colombia)

Ventajas

- La valoración del riesgo es del tipo cuantitativo simplificado y sigue el método de Fine (1971).
- Es sencilla y resulta fácil de aplicar.
- Considera la probabilidad del suceso en la estimación del riesgo, hecho que dota de mayor credibilidad al resultado, en base a información previa, estadísticas, informes de seguridad, etc.
- Considera específicamente riesgos de ataque terrorista, sabotaje, intrusión, etc.
- Por cada amenaza se identifica el peligro, teniendo en cuenta las capacidades de la instalación (vulnerabilidades): infraestructura del Aeropuerto (cerramiento, puertas de acceso, sistema de control de acceso, iluminación, comunicaciones, capacitación y de la seguridad aeroportuaria, etc.).

Desventajas

- La valoración del riesgo de ataque, si bien se describe en sus bases, es inespecífica en su cuantificación, puesto que no se detallan los elementos que pueden ser objeto de ataque, o aquellos aspectos que son susceptibles de valorar ante una amenaza para la seguridad. Esto conduce a una evaluación subjetiva del riesgo.
- No concreta las consecuencias de pérdidas humanas, ni las valora de alguna manera.

5.2.2.CARVER (EUA)

Ventajas

- La valoración del riesgo es del tipo cuantitativo simplificado.
- Es sencilla y resulta fácil de aplicar.
- Identifica muy bien las vulnerabilidades de la instalación, con lo que las medidas a tomar al respecto se pueden ajustar con detalle.
- Valora la importancia (criticidad) del objetivo en términos económicos, sociales, operativos, de reposición de servicio, etc.
- Diseñada específicamente para amenazas terroristas.
- Valora el efecto de las medidas adoptadas sobre la población. Lógico tratándose de una metodología con origen militar que busca los puntos débiles de los objetivos de ataque.

Desventajas

- La cuantificación del riesgo si bien emplea un método simplificado, no se ciñe exactamente al método Fine (1971).
- No realiza una evaluación de las probabilidades de suceso o frecuencia de presentación del riesgo a evaluar.
- No especifica el tipo de ataques o amenazas concretas a valorar, si bien se entiende que son fundamentalmente ataques con armas, por tratarse de una metodología de origen militar.
- No permite estimar las consecuencias del ataque terrorista en la valoración del riesgo.

5.2.3.RBDM. Navigation and Vessel Inspection (Servicio de Guarda Costas de EUA)

Ventajas

- La valoración del riesgo es del tipo cuantitativo simplificado y sigue el método de Fine (1971).
- Es sencilla y resulta fácil de aplicar.
- Considera específicamente riesgos de ataque terrorista, sabotaje, intrusión, etc.
- Está desarrollada específicamente para evaluación de amenazas en puertos y se aplica en varios países.

Desventajas

- Las consecuencias se valoran estrictamente en base al tamaño y destino (nacional o internacional) del buque y su carga y en el caso pésimo se valora la peligrosidad de la mercancía transportada. No existe desglose de consecuencias.
- Se valora la vulnerabilidad exclusivamente en base a la accesibilidad y la seguridad orgánica, sin considerar otros factores. Asimismo no se valora de forma pormenorizada la accesibilidad.

5.2.4.SECUREPORT. Puertos del Estado (España)

Ventajas

- La valoración del riesgo es del tipo cuantitativo simplificado y sigue el método de Fine (1971).
- Considera específicamente riesgos de ataque terrorista, sabotaje, intrusión, etc.
- Considera la probabilidad del suceso en la estimación del riesgo, hecho que dota de mayor credibilidad al resultado.
- Realiza un estudio detallado de las vulnerabilidades de la instalación.

Desventajas

- Es prolija y compleja de aplicar al contener numerosos índices y sub-índices, con complejas formas de valorarlos.
- Solo considera tres escenarios globales de amenaza; ataque con explosivos (de forma genérica), ataque bioquímico y ataque cibernético, dejando de lado otras amenazas más comunes que pueden resultar de interés en el análisis.
- Cuantificación muy pormenorizada de las vulnerabilidades y las consecuencias, lo que implica una evaluación y análisis complejo de cada situación de amenaza a valorar, con las dificultades que ello conlleva desde el punto de vista de la asignación de puntaje.
- La accesibilidad y la seguridad, como parte de las vulnerabilidades, se valoran de forma muy cualitativa, sin definir unas características generales aceptables para estas.

5.2.5. TRAM (IMO-ILO)

Ventajas

- La valoración del riesgo es del tipo cuantitativo simplificado y sigue el método de Fine (1971).
- Es sencilla y resulta fácil de aplicar.
- Desarrollada específicamente para evaluación de amenazas en puertos.
- Considera específicamente riesgos de ataque terrorista, sabotaje, intrusión, etc.
- Considera la probabilidad de suceso y lo hace en base a la información del objetivo y de la seguridad del puerto.

Desventajas

- La valoración de las vulnerabilidades es inespecífica, no valorándose pormenorizadamente sino de forma conjunta la accesibilidad y el grado de seguridad de la instalación para cada amenaza.
- Las consecuencias se valoran de forma muy global, no se valoran daños específicos a la vida humana o daños ambientales, etc. si bien parece que de forma implícita pudieran valorarse.

5.2.6. Resumen de la evaluación

Se resume a continuación la evaluación realizada entre las diferentes metodologías seleccionadas:

- AERONÁUTICA CIVIL (Colombia): esta metodología valora el riesgo mediante un análisis previo de las capacidades de la infraestructura que le permitan repeler un ataque, apoyándose en el historial de sucesos.

No realiza un análisis pormenorizado de la amenaza en base a una formulación, sino que estudia para cada amenaza sus diferentes aspectos y como resultado le asigna una probabilidad de suceso.

Asimismo solo valora las consecuencias en términos de pérdidas de operatividad de la instalación.

- CARVER (EUA): esta metodología Identifica muy bien las vulnerabilidades de la instalación, con lo que las medidas a tomar al respecto se pueden ajustar con detalle y se diseña para evaluar objetivos posibles de ataque, lo que le da una objetividad interesante al resultado desde un punto de vista de definición de los posibles ataques.

No permite valorar consecuencias directas sobre objetivos o población, desventaja importante, y tampoco evalúa probabilidades de suceso.

- **RBDM. Navigation and Vessel Inspection (Servicio de Guarda Costas de EUA):** es una metodología de uso sencillo y está diseñada de forma específica para evaluar riesgos en puertos, considerando asimismo riesgos como los del objeto de esta investigación. Las consecuencias se preestablecen en función del tipo de tráfico de las terminales y como en el caso anterior tampoco considera consecuencias de pérdidas humanas, además de no valorar o concretar las mismas (no son medibles).

Las vulnerabilidades se miden en base a la accesibilidad y la seguridad valorando estas en tres niveles.

- **SECUREPORT. Puertos del Estado (España):** es una metodología muy completa. Contempla múltiples índices y subíndices que la convierten en una metodología prolija y poco atractiva en su aplicación para los evaluadores de la seguridad. Se centra fundamentalmente en tres tipos de ataques y considera la probabilidad del suceso.

La accesibilidad y la seguridad solo se valoran de forma cualitativa, sin definir unas características generales aceptables para estas.

- **TRAM (IMO-ILO):** esta metodología es de sencillo uso y considera los mismos riesgos que el objeto de esta investigación.

Considera la probabilidad del suceso, pero en cambio la valoración de las vulnerabilidades y las consecuencias es muy general, sin detallar aspectos concretos a valorar.

5.2.7. Evaluación comparativa de parámetros

Se describen de forma resumida los parámetros que configuran cada una de las metodologías seleccionadas y que se comparan entre sí dentro del análisis realizado de las metodologías.

Aeronáutica Civil (OACI-Colombia)

- *Probabilidad:* Se define como la posibilidad de que se presenten en un evento.
- *Severidad o efecto:* Se define como el impacto que se puede presentar si sucede un evento

CARVER (Ejército de los EUA)

Esta metodología considera seis parámetros que a continuación se describen:

- *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
- *Accesibilidad*: es la facilidad con que un objetivo puede ser 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.
- *Recuperabilidad*: es una medida del tiempo requerido para reemplazar, reparar o evitar la destrucción o el daño infligido al objetivo, y varía en función de las fuentes y la antigüedad 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).
- *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.
- *Objetos 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

RBDM (Servicio de Guardacostas de EUA)

Esta metodología define tres parámetros con los que estima el riesgo, estos son:

- *Amenaza*: escenario de ataque potencial bajo circunstancia específicas que pueden ser combinados con objetivos críticos específicos para ser desarrollados y evaluados en el proceso de análisis de protección portuaria.
- *Vulnerabilidad*: 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.
- *Consecuencia*: nivel de daños producido en la instalación en función del tipo de mercancía movida y su peligrosidad.

SECUREPORT (Puertos del Estado)

La metodología española es muy prolija y considera tres parámetros que denomina “índices globales”, que a su vez se definen como el resultado de la valoración de otros subparámetros en cada uno de ellos. Los tres parámetros son:

- ID Índice de Verosimilitud,
- IV Índice de Vulnerabilidad,
- IC Índice de Consecuencias

Cada uno de los índices globales anteriores se aplica mediante una batería de 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 (Ministerio del Interior).
- *Índice de Carácter Simbólico (IAS)*, 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 (ITP)*, 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.

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.
- *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.

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.
- *Índice de Ineficiencia Operativa (IIO)*, 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.
- *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.
- *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.
- *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.
- *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.

TRAM (OIT-OMI)

La metodología TRAM considera tres parámetros que se describen a continuación:

- *Amenaza*: La probabilidad de un suceso ocurrido (seguridad en los puertos) basada en información específica obtenida o debido a características conocidas del objetivo potencial.

- *Vulnerabilidad: La vulnerabilidad del objetivo para cada amenaza se evalúa en base a las medidas de seguridad existentes, es decir al grado de accesibilidad a las instalaciones, la existencia de vigilancia, capacitación en seguridad formal, etc.)*
- *Impacto (o consecuencias): de cada incidente potencial que se produzca sobre el objetivo y en la terminal, caso de producirse. Se evalúa en base al daño producido al medio ambiente, a la economía del puerto, a la vida humana, etc.*

El objeto de esta comparativa es el de conocer las relaciones existentes entre las diferentes metodologías seleccionadas con el fin de poder posteriormente considerar aquellas que resulten de interés acorde con el tipo de propuesta que se pretende realizar.

Una vez analizadas las diferentes metodologías seleccionadas se efectúa una comparativa preliminar entre los diferentes parámetros que se definen en cada una de ellas, evaluándolos desde la perspectiva de la formulación propuesta en el Método de Fine, (1971) de evaluación del riesgo:

$$\text{Riesgo} = \text{Amenaza} \times \text{Vulnerabilidad} \times \text{Consecuencia}$$

Para ello se analizan y comparan los parámetros con los siguientes criterios:

- Objeto de los parámetros, descritos en el *Anexo 1. Metodologías consideradas*.
- Alcance de los índices descritos en las metodologías seleccionadas; similitudes y diferencias entre estos.
- Relaciones cualitativas entre los índices.

Se trata de identificar para cada metodología la relación entre los tres parámetros (amenaza, vulnerabilidad y consecuencia) que definen la evaluación del riesgo en el método simplificado, así como los índices que definen cada una de ellas, valorando como se abordan y con qué grado de detalle se evalúan. Los resultados de dicha comparativa se muestran en la Tabla 9.

Una vez realizado el análisis comparativo se relacionan en una columna los índices que definen las diferentes metodologías, indicados con aspas en las columnas, señalando así en que metodología se emplean.

Asimismo se señalan con un círculo aquellos índices que no se describen de forma explícita en cada metodología en columna, pero que se corresponden con alguno de los empleados en esta y que por tanto si se consideran, si bien denominados de otra forma y en algunos casos incluso con diferente alcance.

Tabla 9. Relaciones cualitativas entre parámetros de las metodologías seleccionadas

METODOLOGÍA PARÁMETROS	AERONÁUTICA CIVIL	CARVER	RBDM	SECUREPORT	TRAM
Amenaza-PROBABILIDAD	X	O	X	O	X
Vulnerabilidad (medidas de vigil. y accesos.)	X		X		X
Impacto-Ocurrencia-CONSECUENCIAS	X		X		X
Probabilidad general				X	O
Carácter simbólico		O		X	
Trascendencia a la protección				X	
Accesibilidad a la instalación-VULNERABILIDAD		O		X	O
Susceptibilidad a la destrucción				X	
Ineficiencia operativa-VULNERABILIDAD				X	O
Daños a la vida humana	O			X	
Daños económicos	O			X	
aseguren la funcionalidad				X	
Plazo de recuperabilidad		O		X	
Repercusión social y ambiental				X	
Criticidad		X		O	
Accesibilidad		X		O	O
Recuperabilidad		X		O	
Vulnerabilidad		X	O	O	O
Efecto sobre la población	O	X		O	
Objetivos reconocibles		X		O	

X parámetro de la metodología

O parámetro considerado implícitamente en la metodología

Fuente: Elaboración propia

Una vez analizadas todas las metodologías y sus parámetros característicos se elabora un cuadro resumen donde se indican las relaciones cualitativas entre los principales parámetros analizados, si bien agrupados ahora por su alcance, reflejando además aquellos otros que resultan diferentes a los tres básicos o fundamentales (amenaza, vulnerabilidad y consecuencia) y que valoran por tanto otros aspectos de interés para la evaluación del riesgo en un puerto.

El objeto de esta tabla resumen es mostrar que parámetros de interés para la investigación son considerados en cada metodología, así como su alcance al detallarse un segundo nivel de evaluación.

Se comprueba que además de los índices fundamentales definidos, existen otros característicos de la formulación de SECUREPORT que coinciden plenamente con los que considera la metodología CARVER, si bien esto es lógico teniendo en cuenta que aquella se desarrolló basándose en esta.

Así, entre los parámetros analizados, los asociados a los fundamentales resultan:

- Probabilidad general (amenaza)
- Vulnerabilidad (medidas de vigilancia y accesos)
- Consecuencias;
 - Daños a la vida humana
 - Repercusión social/ambiental

Tabla 10. Resumen de parámetros considerados en cada metodología

PARÁMETROS \ METODOLOGÍA	AERONÁUTICA CIVIL	CARVER	RBDM	SECUREPORT	TRAM
Probabilidad general (amenaza)	X		X	X	X
Trascendencia a la protección				X	
Vulnerabilidad (medidas vigilancia y accesos)	X	X	X	X	X
Consecuencias	X		X		X
- Daños a la vida humana /económicos				X	
- Repercusión social/ambiental		X		X	
Redundancia de elementos				X	
Criticidad - Carácter simbólico		X		X	
Recuperabilidad		X		X	
Objetivos reconocibles		X		X	

Fuente: Elaboración propia

Se describen a continuación a modo de resumen aquellos parámetros identificados que definen aspectos diferentes a los básicos o fundamentales. Estos son:

- Probabilidad general: valora de forma global las posibilidades de un ataque terrorista a las instalaciones y cuyo valor lo determina la Autoridad en materia de seguridad (Ministerio del Interior).
- Criticidad-carácter simbólico: valora el incremento de la probabilidad de presentación de un suceso que se produce en relación con el nivel general, debido al carácter simbólico de la instalación o elemento que se analiza, que pudiera hacerle convertirse en un blanco preferente del ataque.
- Trascendencia para la Protección, 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 o por que tengan que desarrollar acciones posteriores al suceso que minimicen las consecuencias del mismo
- Daños a la economía: valora la magnitud de las pérdidas económicas y el deterioro de los productos y servicios. Su estimación puede realizarse de forma compleja, valorando cuantitativamente los costes de inversión de reconstrucción y las repercusiones económicas por cese de una actividad, o bien de forma más sencilla a falta de datos estimando cuantitativamente la importancia estratégica del sistema productivo a que sirve la instalación y la importancia económica del mismo.

Este parámetro se describe literalmente en el ROM 0.0. Procedimiento general y bases de cálculo en el sistema portuario español.

- Redundancia de elementos: 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.

- Plazo de recuperabilidad: 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.
- Daños a la vida humana: este parámetro se valora en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.

Este parámetro se describe literalmente en el ROM 0.0. Procedimiento general y bases de cálculo en el sistema portuario español.

- Repercusión ambiental: Se valora la degradación en el lugar o sus alrededores. En este caso se considerará el daño al sistema marino y a la calidad de las aguas por vertidos incontrolados o accidentales, o contaminación aérea debida a hidrocarburos.

Este parámetro se describe literalmente en el ROM 0.0. Procedimiento general y bases de cálculo en el sistema portuario español.

- Repercusión pública y social: Valora la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

Este parámetro se describe literalmente en el ROM 0.0. Procedimiento general y bases de cálculo en el sistema portuario español.

- Objetivos reconocibles: Intenta valorar el grado en que un objetivo se puede reconocer sin confusión con otros objetivos o elementos. Los objetivos fácilmente reconocibles servirán siempre mejor a los propósitos de un terrorista.

Analizando los parámetros en base al método simplificado de Fine (1971), considerado como el esquema a seguir para la evaluación del riesgo, se comprueba que la valoración de la “amenaza”, que generalmente se realiza directamente a través de la probabilidad de suceso de esta, solo se considera en cuatro de las cinco metodologías consideradas. Así, la metodología CARVER no la considera en su evaluación, como ya se indicaba en su apartado correspondiente, exigiendo ésta una valoración posterior de la misma.

Sin embargo la metodología SECUREPORT incorpora un parámetro de “Probabilidad General” que valora la probabilidad de un ataque terrorista a la instalación. Este parámetro resulta interesante, sin embargo, y a juicio del autor de esta investigación, presenta una carencia importante, pues considera la probabilidad de suceso asociada exclusivamente a un ataque terrorista, obviando otras amenazas igualmente importantes y potencialmente mucho más presentes en las terminales portuarias.

Esta misma metodología el parámetro de “trascendencia para la protección” 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. A juicio del autor este índice no reporta una mayor garantía de seguridad ante ataques, pues es obvio que ante cualquier ataque las instalaciones de auxilio; bomberos, policía, centros de control, etc. deberán reforzarse rápidamente y sin embargo no por ello dejará de existir el riesgo del ataque. Además, y como ya se ha dicho, se obvian otras amenazas de interés.

Respecto a la “vulnerabilidad”, es considerada por igual en todas las metodologías, valorándose dos factores clave para la misma, como son la accesibilidad y la seguridad orgánica, si bien se define además el denominado “índice de carácter simbólico”, que valora la relevancia de la instalación a nivel local, nacional o internacional en función de la repercusión social que un siniestro de los contemplados (ataque convencional con explosivos, ataque con armas químicas y ataque cibernético) puede tener en ella, y que se vincula al “índice de probabilidad general”. Este concepto resulta difícil de valorar en la aplicación real, limitándose a ataques terroristas exclusivamente como amenazas a contemplar en la instalación, y por tanto no resulta de interés su incorporación a la propuesta metodológica, si bien resulta interesante el concepto de la importancia o relevancia operativa que tiene un elemento o una instalación ante una amenaza dada respecto de la operación portuaria.

La “consecuencia” no se considera en la metodología CARVER, como ya se ha visto, y ésta es considerada además de forma desigual en las metodologías restantes, valorándose de una forma directa con diferentes grados de gravedad en el caso de Aeronáutica Civil. En el caso de la metodología RBDM se asigna un nivel 1, 2 ó 3 a esta en base al tipo de terminal de que se trate, sobreentendiéndose por tanto que cada tipo de terminal lleva implícitas unas consecuencias diferentes, sin embargo estas no se concretan ni cuantifican como ya se indicó anteriormente.

Esta metodología contempla un parámetro denominado “objetivos reconocibles”, que identifica aquellos objetivos de mayor posibilidad de ataque. A juicio del autor de esta investigación este parámetro no resulta de mucho interés, puesto que una vez más, no solo se trata de que las instalaciones puedan ser atacadas, sino que se pueden producir otras amenazas como la inmigración ilegal en las mismas, para las cuales este parámetro no resulta de gran interés.

SECUREPORT por su parte evalúa las consecuencias de una amenaza dada desglosando muy pormenorizadamente estas entre pérdidas de vidas humanas, pérdidas ambientales, danos económicos a la actividad, incidencia en la recuperabilidad de la actividad, etc. Se considera de gran interés este desglose pormenorizado y que a juicio del autor, tiene un peso importante en el resultado de la evaluación. Sin embargo en dicha valoración se contempla el denominado “índice de redundancia de elementos” que considera 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. La valoración de la incidencia se determinará por el porcentaje en que las funciones afectadas queden cubiertas por otras instalaciones propias o ajenas, donde cada supuesto analizado se clasifica en función del porcentaje de redundancia. Este índice resulta de difícil valoración objetiva a juicio del autor y por eso resulta de escaso interés para la propuesta metodológica.

Por último, la metodología TRAM valora las consecuencias en los ámbitos de las pérdidas humanas, ambientales y económicas, si bien no se concreta el alcance detallado de estas.

5.2.7.1. Conclusiones de la evaluación comparativa de parámetros

Se puede afirmar que todas las metodologías consideradas se estructuran sobre las mismas bases de evaluación en todos sus parámetros, si bien existen matices en el alcance que ofrecen sus parámetros, a excepción de la metodología CARVER, la cual no evalúa o asigna la probabilidad del suceso ni estudia las consecuencias del suceso. Hay que decir en este sentido que el origen de la CARVER es un origen militar cuyo cometido exclusivo era detectar los puntos débiles de un objetivo para ser atacado posteriormente, en cuyo caso tienen sentido estas carencias.

Por otra parte parece que el uso de los parámetros relativos a las consecuencias definidos por SECUREPORT tienen un detalle importante en su evaluación, que resulta de interés para su consideración en la propuesta metodológica. Así se consideran de interés los parámetros definidos como:

- Daños económicos
- Daños a la vida humana
- Repercusión ambiental
- Repercusión pública y social

Tomando como referencia el denominado “índice de probabilidad general”, se considera un nuevo parámetro denominado “riesgo de la fachada”. Se trata de valorar el riesgo general para la seguridad, o lo que es lo mismo, el nivel de peligrosidad de cada fachada marítima, valorado en base a la disposición física del mismo en la costa española. La disposición del puerto en una fachada o en otra incide sensiblemente en los niveles de seguridad general ante posibles amenazas

Además y basándose en el “índice de carácter simbólico” se considera un nuevo parámetro denominado “relevancia operativa” de un elemento ante un escenario de amenaza dado, que evalúa la funcionalidad y relevancia operativa de las instalaciones o elementos que componen una terminal y su importancia para la operación portuaria.

5.3. Etapa 3. Identificación de nuevos parámetros

Se muestra a continuación los resultados de la Etapa 3. Identificación de nuevos parámetros.

5.3.1.Resultado de la Encuesta al Sistema Portuario Español

A continuación se muestran los resultados comentados de cada una de las preguntas planteadas, si bien se ofrecen las respuestas de forma anónima dado lo delicado de algunas cuestiones y la garantía dada a los encuestados de confidencialidad en sus respuestas.

A la pregunta número 1; *¿Conoce la Metodología de Evaluación del Riesgo que se aplica para los puertos de interés general españoles a través de la plataforma SECUREPORT?*, todos menos uno de los encuestados conocían la metodología empleada y no solo la aplicación que la gestiona.

A la pregunta número 2; *¿Considera que existen riesgos frecuentes para las personas en su terminal que no estén recogidos en SECUREPORT?*, todos los expertos consultados respondieron que NO consideran la existencia de riesgos frecuentes para las personas, independientemente del tipo de tráfico que las terminales gestionen.

A la pregunta numero 3; *¿Y para las mercancías?*, los expertos consideran que todos los riesgos se encuentran contemplados actualmente.

A la pregunta número 4; *Según usted, ¿Cuáles son los escenarios de amenaza a la seguridad más factibles que se pueden dar en su terminal?*, los encuestados respondieron que las amenazas potenciales en sus instalaciones son:

- Intrusiones a la instalación.
- Robo en las terminales de contenedores.
- Tráfico de estupefacientes.
- Polizones en buque.
- Tráfico ilegal de personas.
- Introducción ilegal de objetos.
- Sabotaje perpetrado por personal relacionado con la AP o ajenas a la instalación
- Instalación de explosivos en el interior de la instalación portuaria.
- Impacto sobre la instalación portuaria mediante empleo de un buque/aeroplano.

- Incendio provocado.
- Amenazas a la mercancía; robo, deterioro, etc.
- Intento de intrusión en el buque por inmigración ilegal.
- Ataques a personas; agresiones, asesinatos, etc.
- Dispersión de sustancias químicas peligrosas.

Como se comprueba todas estas amenazas se enmarcan en el esquema de amenazas planteadas inicialmente como de interés para la investigación; intrusión, atentados, sabotaje, robos, tráfico de personas y mercancías, etc.

A la pregunta número 5; *¿Cuáles han sido los escenarios de amenaza más frecuentes?*, los encuestados respondieron de diferente manera:

- No han sufrido ninguna amenaza a la instalación (5)
- Los mismos descritos en la pregunta anterior (10)

A la pregunta número 6; *A su juicio, ¿son más frecuentes los riesgos asociados a la seguridad de la mercancía (robo, destrucción, etc.) o a la seguridad de las personas?*, los expertos respondieron de forma mayoritaria (7) que los riesgos son mayoritarios para las mercancías, si bien 4 de ellos respondieron que a las personas y algunos (4) no respondieron a dicha pregunta.

A la pregunta número 7; *Valore la seguridad de la accesibilidad de su terminal*, las respuestas fueron;

- Alta seguridad; difícil accesibilidad (9)
- Regular seguridad, accesibilidad relativamente sencilla (4)
- Baja seguridad, fácil accesibilidad (2)

A la pregunta número 8; *Defina el sistema de accesibilidad existente en su terminal y de que se compone; tipo de vallado, características, sistema de barreras, si existe control de tarjetas, de personas, etc.*, las respuestas se agrupan así y se cita el número de instalaciones entre paréntesis:

- Vallado $\geq 2\text{m}$ de altura con muro de hormigón y vallado superior (13)
- Control general de accesos, con lector de matrícula provisto de barreras (13)
- Sistema de tarjetas para identificación personal (13)
- Iluminación perimetral (3)
- Sistema de Control Cerrado de Televisión, CCTV (9)
- Arcos detectores y scanner para control de operaciones de embarque de pasajeros y equipajes (7)

Como se comprueba en general todas las instalaciones tienen los sistemas básicos; cierre perimetral y un control de accesos con lector de matrículas y barreras. Si bien no todos disponen de Sistema CCTV o de iluminación perimetral (o al menos no lo declaran en la encuesta).

No se da información sobre otros sistemas de detección como cámaras nocturnas o sistemas de detección y movimiento.

A la pregunta número 9; *¿Existen elementos vulnerables en la terminal (edificios, zonas de tránsito, aparcamientos...) de fácil alcance/acceso a través de terminales contiguas?*, 10 de los consultados consideran que no existen elementos vulnerables en sus instalaciones, mientras que otros 5 si estiman su existencia que se detalla así:

- Las zonas de tránsito y aparcamiento de vehículos en el interior de la instalación presentan mayor riesgo para la instalación portuaria, en ella transitan personas que acceden a través de autobuses, taxis, etc.(3)
- En algunos casos, a través de la zona de maniobra (2).

A la pregunta número 10; *A su juicio, ¿la disposición de las instalaciones dentro de la terminal influye en la posibilidad de recibir algún tipo de ataque o por el contrario no influye?*, las respuestas facilitadas por los expertos se agrupan así:

- Si influyen (9)
- No influyen (2)
- NS/NC (4)

A la pregunta número 11; *Ordene las principales instalaciones en función de la relevancia que a su juicio tienen para la seguridad, de mayor a menor (mayor relevancia equivale a más susceptibilidad a ataques o amenazas a la seguridad,* los encuestados consideran que las principales instalaciones a proteger son, por este orden:

1. Terminales de pasajeros
2. Terminales de graneles líquidos
3. Terminales de contenedores y recintos de mercancías peligrosas
4. Centro de control portuario
5. Centros de transformación
6. Redes de distribución de energía eléctrica
7. Redes de telefonía y fibra óptica.

A la pregunta número 12; *¿Considera que los problemas de conflictividad laboral inciden en la seguridad de sus instalaciones?*, las respuestas fueron:

- Bastante (2)
- Algo (9)
- Nada (4)

Estas respuestas concuerdan con alguna de las respuestas ofrecidas a la pregunta número 4, donde se consideran posibles sabotajes por parte de empleados de la Autoridad Portuaria.

A la pregunta número 13; *¿La formación del equipo de control y vigilancia de la terminal es la adecuada?*, la respuesta común a todos los puertos fue que sí, la formación del equipo de seguridad es adecuada.

A la pregunta número 14; *¿Cuántos años de experiencia media tiene dicho equipo?*, los valores recogidos se disponen como sigue:

- Valor mínimo: 2 años (2)
- Valor máximo: 15 años (3)
- Valor típico: 7 años (10)

Lo que resulta en un **Valor medio: 7,9 años**

A la pregunta número 15; *En caso de amenaza a la seguridad, ¿cuál es su tiempo medio de respuesta?*, las respuestas fueron:

- Menos de 5 minutos (8)
- Aproximadamente 5 minutos (7)
- Más de 5 minutos (0)

El resultado arroja una respuesta evidente de la rápida reacción de los servicios de seguridad operativa de la instalación.

A la pregunta número 16; *¿Se han efectuado inspecciones de las instalaciones portuarias por parte de la Comisión Europea con el fin de controlar la aplicación efectiva del Reglamento (CE) Nº 725/2004?*, las respuestas fueron:

- Si (12)
- No (1)
- NS/NC (2)

A la pregunta número 17; *¿Cuál ha sido el grado de satisfacción de dicha inspección?*, las respuestas fueron:

- Satisfactorio (9)
- Aceptable (3)

- NS/NC (3)

A la pregunta número 18; *¿Considera suficientes las medidas implantadas para la mejora de la seguridad en función del riesgo real de su instalación?*, las respuestas fueron:

- Si (12)
- No (3)

5.3.1.1. Conclusiones de la Encuesta al Sistema Portuario Español

Las principales conclusiones que se obtienen de las encuestas son:

- En general existen mayores riesgos de amenazas para la mercancía que para las personas.
- El riesgo de intrusión difiere de unos puertos a otros, influyendo claramente en la existencia del mismo la ubicación del puerto en la costa española, resultando de mayor frecuencia de amenaza en los puertos del sur de España y en particular los puertos frontera con el Magreb.
- El riesgo potencial de amenazas es mayor según el tipo de mercancía que mueve la terminal, incidiendo por tanto el tipo de mercancía movida en un mayor riesgo de amenazas.

Las terminales que presentan mayor riesgo son, según los encuestados, por orden las de Cruceros, seguidas de las de Graneles Líquidos, y las de Contenedores.

- La disposición de las instalaciones dentro de la terminal incide directamente en las posibilidades de recibir un ataque.

5.3.2. Análisis de estadísticas de seguridad

Los resultados del análisis de las estadísticas de seguridad se sintetizan en la siguiente tabla:

Tabla 11. Resumen de estadísticas de seguridad en Sistema Portuario Español

	2009		2010		TOTAL	
INMIGRACIÓN ILEGAL	Nº inmigrantes		Nº inmigrantes		TOTAL	
	594		1147		1741	
INTRUSIONES	Nº intrusos		Nº intrusos		TOTAL	
	600		1267		1867	
ATAQUES TERRORISTAS	Nº ataques		Nº ataques		TOTAL	
	1		0		1	
CONFLICTOS SOCIO-LABORALES	Nº días	Nº interrup. O.P.	Nº días	Nº interrup. O.P.	TOTAL DÍAS	TOTAL INTERRUPT.
	34	20	79	43	113	63
SABOTAJE	Nº ataques		Nº ataques		TOTAL	
	3		0		3	

Fuente: Elaboración propia

Como se aprecia del análisis de la estadística, los actos delictivos de mayor frecuencia en los puertos en el periodo estudiado resultaron ser la “intrusión en el puerto” y la “inmigración ilegal” en el puerto con un total de 1741 inmigrantes ilegales detectados en el periodo estudiado.

A la vista de las cifras y datos disponibles, los puertos que poseen un mayor riesgo de intrusión y de llegada de inmigrantes irregulares son los puertos comerciales españoles con líneas regulares de pasajeros con destino o procedentes del Magreb, que fundamentalmente son todos aquellos situados en el norte de África y en el sur de la Península. Lo que denota que en función del puerto de procedencia de los buques la amenaza es mayor o menor. En este caso es evidente que los puertos del sur de la Península y norte de África resultan más peligrosos como puertos origen de la mercancía/pasaje. Además se debe incluir al Puerto de Santander o el de Bilbao en esta lista de puertos conflictivos debido a sus conexiones marítimas históricas con Reino Unido que les convierten en puertos de interés para el inmigrante ilegal.

Por otra parte y según un informe elaborado por la EUROPOL sobre situación y tendencias del terrorismo en la Unión Europea. (TE-SAT) la amenaza de los islamistas, así como etno-nacionalistas separatistas y el terrorismo, sigue siendo alta. El terrorismo separatista vasco en España y Francia, y el terrorismo separatista corso en Francia, convierten a estos países en los más afectados de la UE. En el Reino Unido, los grupos disidentes republicanos irlandeses incitan a participar en la delincuencia y la violencia. Los ataques terroristas de izquierda en la UE también han aumentado. En Grecia, el uso de la violencia por la *Epanastatikós Agónas* o Lucha Revolucionaria se ha intensificado.

El escenario reflejado no permite descartar, más bien al contrario, favorece el que se puedan producir movimientos de terroristas, armas o explosivos a través de las líneas marítimas comerciales que unen los puertos de los países citados, como mediante el uso de embarcaciones deportivas o de recreo.

La utilización de explosivos en el atentado perpetrado el 30-07-2009 y el hecho de que hubiera ocurrido en una isla genera la inquietud sobre la vía utilizada para su introducción desde el territorial peninsular o continental. Las condiciones de seguridad impuestas en la aviación civil parecen hacer descartar la vía aérea como forma de introducción del explosivo en la isla, quedando por tanto la vía marítima como la más probable para ello, abriéndose dos posibilidades a contemplar: La utilización de una embarcación de recreo o alguna de las líneas de buques de transbordo rodado de pasajeros que llegan a las islas desde Barcelona, Valencia o Denia (Alicante).

Esta última posibilidad pone en evidencia las carencias y falta de efectividad de los controles de seguridad en los embarques de pasajeros y vehículos en los puertos de origen citados, y la ausencia de controles de seguridad al desembarque en el destino, a lo que hay que añadir la falta de control sobre la mercancía que transportan esos

buques al no estar sometida a control fiscal por tratarse de un movimiento en el interior del territorio nacional. A esta misma situación no son ajenos los restantes puertos con tráfico de ferris de pasajeros y vehículos en régimen de pasaje, apreciándose varias causas que la provocan, de las que destacan:

- a) La carencia de recursos humanos y materiales necesarios para el desempeño de las funciones de seguridad portuaria, que se acusa en las Unidades que prestan ese servicio.
- b) La falta de procedimientos homogeneizados para realizar los controles de seguridad al embarque de tripulantes, pasajeros y vehículos en los buques de transbordo rodado.
- c) La ausencia habitual de controles de seguridad al desembarque de personas y vehículos en buques de transbordo rodado procedentes de puertos nacionales.
- d) La ausencia habitual de controles de seguridad sobre la mercancía que embarca o desembarca en buques de travesías nacionales.

No obstante la realidad actual apunta a una práctica desarticulación del aparato militar de ETA y, al menos en la actualidad y tras la tregua indefinida actual, no parece que la banda terrorista tenga posibilidades reales de seguir atentando, en tanto en cuanto se encuentra prácticamente descabezada y sin apoyos políticos y sociales.

Por otra parte, varios sucesos acontecidos durante el año 2009 en terceros países señalan un recrudecimiento de las acciones terroristas islamistas fuera de territorios en los que existe presencia activa de fuerzas o alianzas militares de lucha contrterrorista, siendo objetivo prioritario de esas acciones, una vez más, el transporte aéreo de pasajeros y el territorio norteamericano, lo que ha supuesto un aumento de las medidas de seguridad aeroportuaria para protegerse de hechos de esa naturaleza, que pueden generar el **desvío de los objetivos de las acciones terroristas hacia el transporte marítimo de pasajeros** al poder considerarlo más vulnerable, habida cuenta de que los procedimientos de protección contra la introducción de artefactos explosivos en los buques son menos exhaustivos y rigurosos, en especial en los de trasbordo rodado.

Por su parte, el secuestro de varios cooperantes españoles en Mauritania en el mismo año debe alertar por el incremento de actividad terrorista en el Magreb, con el que España cuenta con un buen número de conexiones marítimas, tanto de mercancías como de pasajeros, a través de los puertos del Norte de África.

Los conflictos socio-laborales supusieron en el periodo estudiado un total de 63 días de interrupción de las operaciones portuarias en el Sistema Portuario español, lo cual no supone un número elevado de días, si bien este tipo de conflictos puede llegar a suponer pérdidas económicas importantes por el cese de la actividad temporal, así como pérdidas indirectas derivadas de posibles sabotajes.

Por último los actos de sabotaje citados supusieron el acto delictivo de menor incidencia en los puertos, registrándose tan solo 3 actos de sabotaje en el periodo de estudio considerado, si bien de cierta consideración.

Se ha considerado el sabotaje a los medios físicos o electrónicos de los propios sistemas, o a las comunicaciones de los Centros de Control o de los Cuerpos de Seguridad presentes en el puerto, al tratarse de las violaciones que denotan la mayor debilidad de los sistemas, al mismo tiempo que constituyen por sí mismas una situación de riesgo al poder ser paso previo a la realización de actos criminales.

Se desprenden del análisis de los boletines las carencias existentes en la seguridad real de los accesos a las terminales, especialmente importantes en las terminales de pasaje al estar estas generalmente llenas de gente durante varias horas cada día. Estos accesos y las zonas de pre-embarque no presentan un grado aceptable de seguridad en general, siendo un objetivo claro y sencillo para cualquier acto terrorista que causaría numerosas bajas y heridos en caso de producirse. El altísimo número de intrusiones en algunos puertos demuestra que este hecho es una realidad.

Los puertos del sur de la Península Ibérica y los del norte de África son los puertos con mayor riesgo de ingreso ilegal. Asimismo y al tener dichos puertos una mayor accesibilidad y existir, de forma generalizada, la ausencia de controles en los desembarques de personas y vehículos, éstos se convierten en puertos de mayor riesgo para otros actos delictivos como los atentados terroristas (que se suceden necesariamente a través de la intrusión en la instalación), especialmente a la luz de la situación actual en Oriente Medio y el conflicto político-religioso que actualmente se vive en esa zona del planeta.

Como complemento a este análisis se deben añadir las observaciones pertinentes aportadas por parte de responsables de la Jefatura del Servicio de Costas y Fronteras respecto del funcionamiento de la seguridad en los puertos comerciales españoles, y que fueron facilitadas después de recoger la información.

Se incluyen a continuación:

- Existen disfunciones entre la valoración que se hace del riesgo por parte de las AAPP y la realizada que se comprueba “in situ” por parte de la Guardia Civil en los puertos.
- No se han definido como han de ser las instalaciones respecto de la seguridad, en función del tipo de tráfico que muevan. Fallos en la definición de seguridad en accesos, controles, tipos de verjas, CCTV, etc. Por ejemplo; que no haya áreas de pre embarque en las zonas de ferris.
- Pendientes desde abril 2010 de la regulación mediante normativa que homogenice los procedimientos, estándares, etc. de definición de las medidas

a tomar para mejorar la seguridad; procedimientos de acreditación de las personas, procedimientos de acreditación de aprisionamientos, etc.

- Las terminales de carga rodada y de pasajeros son la que tienen mayores vulnerabilidades.

5.3.2.1. Conclusiones del análisis de las estadísticas de seguridad

Como principales conclusiones del análisis de las estadísticas de seguridad se puede afirmar que los actos delictivos se dan en mayor medida en unas fachadas marítimas que en otras, resultando en general los puertos de la fachada sur de la Península los de mayor probabilidad de suceso de los actos delictivos estudiados, si bien estos mismos actos delictivos se suceden también en el resto de fachadas del litoral español, aunque en menor medida.

Se comprueba que las terminales más susceptibles de ataques terroristas son las terminales de carga rodada y de pasajeros. La seguridad en los accesos a las terminales en general y a las de pasajeros en particular, no es adecuada en general y actualmente no existen criterios homogéneos que describan las necesidades de vigilancia y control y los requisitos de los cierres perimetrales, etc. para cada tipo de terminal. Consecuentemente la valoración actual de la seguridad en los accesos no parece la adecuada y conviene revisar este parámetro con el ánimo de mejorar su evaluación, haciéndola más precisa.

Asimismo se puede afirmar que entre las amenazas de interés para la mercancía y/o las personas, se encuentran:

- Inmigración ilegal
- Robo (previa intrusión en la instalación)
- Sabotaje (previa intrusión en la instalación)
- Ataque con explosivos/armas de fuego
- Conflictos laborales

5.3.3. Principales amenazas a considerar

En el *Capítulo 2 Antecedentes*, se detallaron las principales amenazas para la seguridad en las instalaciones portuarias. En base a los resultados obtenidos en la investigación, se consideran como las principales amenazas a considerar:

- Inmigración ilegal (polizones y el tráfico ilegal de personas)
- El contrabando marítimo
- La piratería
- El Terrorismo

- El bio-terrorismo
- El ciberterrorismo

En base a las amenazas potenciales descritas y al objetivo de esta investigación, se consideran de interés para la misma las amenazas que puedan suponer un deterioro de la infraestructura portuaria y los servicios del puerto, considerándose por tanto de interés las siguientes amenazas:

- Inmigración ilegal (los polizones y el tráfico ilegal de personas)
- El Terrorismo (exceptuando el ciberterrorismo)

Se descarta como amenaza de interés la piratería dado que esta se produce a los buques y en alta mar, y por tanto fuera del ámbito de afección a las instalaciones portuarias, marco en el que se centra esta investigación.

Asimismo se descarta el interés del ciberterrorismo por los objetivos que este implica, los sistemas informáticos, que generalmente buscan dificultar la operación portuaria paralizando esta o bien dañar la gestión informática del puerto; facturación, contabilidad, etc., con el fin de provocar el bloqueo y la paralización del funcionamiento del mismo, pero en ambos casos dichos riesgos no afectan en ningún caso a la seguridad de las infraestructuras portuarias.

Por su parte, el contrabando si bien es una amenaza por la entidad que tiene y el riesgo para la salud pública, no se considera de interés desde el punto de vista de un análisis de seguridad para las infraestructuras del puerto y una interrupción de la operación portuaria derivada de un ataque a estas.

Además existen otro tipo de amenazas de menor escala pero igualmente importantes, dada su frecuencia, como son el robo, el sabotaje, la conflictividad laboral, etc., que si bien no resultan “grandes amenazas”, desde un punto de vista del peligro, si suponen un peligro para la operación portuaria y la infraestructura.

Y por tanto las amenazas a considerar serán:

- Inmigración ilegal (polizones y tráfico ilegal de personas)
- Robo
- Sabotaje
- Ataque con explosivos/armas de fuego
- Ataque con armas químicas (bio-terrorismo)
- Conflictos laborales

5.3.4. Identificación preliminar de parámetros

Del análisis realizado se desprenden los siguientes aspectos de interés que dan lugar a la definición de varios parámetros que se integrarán formando la propuesta metodológica:

1. **Puerto/Fachada marítima.** Se constata mediante las encuestas y el análisis de las estadísticas que el riesgo que genera una amenaza dada en el puerto depende en gran medida de la localización del puerto en una u otra fachada marítima.
2. **Mercancía.** El riesgo de que se produzca una amenaza dada (probabilidad de suceso) se ve afectado asimismo por el tipo de mercancía objeto de la amenaza, y por tanto del tipo de terminal de que se trate, habiéndose comprobado mediante los resultados de las encuestas que los riesgos son mayores en unos tipos que en otros en opinión de los responsables de seguridad de los puertos.
3. **Accesibilidad.** Respecto de la vulnerabilidad existente en los accesos a los puertos, tal y como se refleja en las estadísticas y se desprende asimismo del análisis de las metodologías seleccionadas, se considera importante evaluar mejor aquellos aspectos relativos a la accesibilidad a la instalación
4. **Localización.** Del análisis se desprende también la importancia que tiene la localización de la terminal a evaluar en el conjunto del puerto, o en su caso la localización del activo dentro de una terminal concreta pues esto influye en su “factibilidad de ataque”.
5. **Elementos clave.** Algunos elementos de la terminal resultan clave para el funcionamiento de ésta y su daño o paralización supondría una merma de la operatividad de la terminal.
6. **Estadística de la amenaza.** Se evalúa la probabilidad de suceso de cada amenaza a considerar en base a la estadística de sucesos.

Una vez descritos los aspectos de interés a considerar estos se validan mediante la aplicación del criterio experto.

5.3.5. Propuesta preliminar de coeficientes de ponderación de los parámetros

Una vez definidos preliminarmente los parámetros a emplear, se considera el empleo de una serie de coeficientes para la ponderación de estos, cuyo funcionamiento se definirá a posteriori mediante el empleo del criterio experto. El objeto de dichos coeficientes es el de mejorar el resultado de la evaluación del riesgo, ajustando los valores obtenidos del mismo.

Para ello se considera adecuado inicialmente el empleo de hasta cuatro coeficientes, α , β , γ , y θ . De forma preliminar se propone su uso asociado a los diferentes parámetros, de forma que afecten al valor final de cada uno y por ende al valor de la amenaza, vulnerabilidad y consecuencias. Si bien su existencia, número, y valoración, se evalúan y deciden mediante la aplicación del criterio experto, que también se aplica para validar los parámetros propuestos anteriormente.

5.3.6. Aplicación del Criterio Experto

Se organizó un panel de expertos para consensuar las conclusiones iniciales de la investigación y validar así los resultados obtenidos. En este caso la validación supuso una propuesta definitiva de los parámetros a considerar, así como la validación y forma de empleo de los coeficientes que mejoran el resultado de la evaluación y su funcionamiento en la propuesta metodológica.

Una vez seleccionados los expertos y puesto en marcha el panel, se facilitó información relativa a la investigación a estos, asimismo se les enviaron dos cuestionarios consecutivos por separado. En la primera ronda se plantearon las conclusiones obtenidas y ya indicadas en el apartado 5.3.4. *Identificación preliminar de parámetros* y en el 5.3.5. *Propuesta de coeficientes de ponderación de los parámetros* con el fin de conocer la opinión de estos.

Las actividades y herramientas utilizadas se indican en la Figura 12, cuyo detalle se enuncia a continuación de la misma.

ACTIVIDADES	HERRAMIENTAS	RESULTADOS
Determinación de los objetivos de la encuesta	Encuestas	VALIDACIÓN DE PARÁMETROS Y COEFICIENTES
Selección de los expertos		
Diseño de una encuesta en dos rondas con el fin de encontrar una visión conjunta de los expertos		
Análisis de los resultados de las rondas de encuestas		

Figura 12. Panel de expertos. Actividades y herramientas.

Fuente: Elaboración propia

En el Anexo 3. Criterio Experto se muestran las encuestas realizadas a los expertos así como el resultado de las mismas.

5.3.6.1. Validación de los parámetros considerados

Se recogieron las opiniones de los expertos relativas a las propuestas planteadas así como de todos aquellos aspectos que estos consideraban mejorables. Posteriormente, y tras una segunda ronda, los expertos concluyeron que los parámetros a considerar debían plasmarse en los siguientes índices:

- **Riesgo intrínseco de la fachada marítima (P_T).** Se recoge la influencia de la fachada marítima mediante un índice denominado “riesgo intrínseco de la fachada marítima”, y que se deberá considerar como parte de la valoración que se realice de la “amenaza” a la instalación, valorándose la probabilidad de suceso para cada fachada en función de las estadísticas disponibles de seguridad. De esta manera, por ejemplo, un puerto ubicado en la costa cantábrica tendrá una probabilidad de amenaza de intrusión inferior a cualquier puerto dispuesto en la zona del Atlántico Sur o incluso del Mediterráneo Sur. Las fachadas marítimas a considerar para su valoración serán; Atlántica Norte, Atlántica Sur, Mediterránea o Cantábrica.
- **Riesgo intrínseco de la terminal (T).** Es evidente que la peligrosidad se puede asociar, desde un punto de vista de la probabilidad de suceso de una amenaza, a cada tipo de terminal en virtud del tipo de instalaciones que esta posee y del tipo de actividad que en ella se desarrolla. Se define un parámetro que considera este aspecto, denominado “riesgo intrínseco de la terminal”, y que se deberá considerar como parte de la valoración que se realice de la “amenaza” a la instalación, definiéndose de esta forma diferentes niveles de amenaza para cada tipo de terminal; contenedores, pasajeros, graneles líquidos, graneles sólidos, etc. basándose en las características particulares de cada tipo de mercancía.
- **Accesibilidad (I_{ac}).** Este factor se redefine, pues ya existía, si bien ahora trata de evaluar la vulnerabilidad de las instalaciones en base a diferentes aspectos físicos. Se evalúan las características del cerramiento, sistemas de vigilancia, etc., variando estas en función del tipo de terminal. Por ello se propone la definición del parámetro de accesibilidad con modificaciones en su valoración, de forma que esta se ajuste a situaciones específicas que garanticen la seguridad, valorándose para ello en este parámetro el tipo de vallado y la existencia de iluminación perimetral adecuada, los sistemas de control de accesos (lectores de matrículas, tarjetas de identificación personal, CCTV, arcos detectores, scanner para mercancías, sensores de movimiento, etc.).

- **Layout (I_{Lo}).** Se valora la disposición de la terminal respecto de los accesos al puerto pues ello implica una mayor vulnerabilidad. Además se considera la disposición de la instalación respecto de las terminales de graneles líquidos, debido a su peligrosidad ante un ataque con explosivos o disparos, cuyos efectos podrían alcanzar a otras instalaciones próximas.
- **Relevancia operativa de elementos (R_o).** Hay elementos particulares de la terminal que no pueden dañarse dada su importancia para un adecuado funcionamiento de esta, por ejemplo; las estructuras de acceso rodado ferroviario, así como los equipos de manipulación, centros de transformación y las instalaciones de almacenamiento (silos, tinglados, etc.) y que pueden sufrir los efectos de un ataque terrorista, dejando inutilizada una parte importante de la terminal, con las consiguientes consecuencias. Así, se realiza una lista de elementos con una relevancia operativa a considerar la cual será evaluada en función del tipo de amenaza a evaluar.
- **Riesgo particularizado (I_s).** Este índice considera la probabilidad que se asocia para cada tipo de amenaza evaluada en base a las estadísticas de seguridad del puerto en estudio.

5.3.6.2. Validación de los coeficientes considerados

Los expertos concluyeron que los coeficientes a considerar se definan de la siguiente manera:

- Se consideran coeficientes con el objeto de mejorar la valoración de los tres parámetros básicos de la evaluación del riesgo; amenaza, vulnerabilidad y gravedad o consecuencias, a través de los índices que los componen.
- Se consideran cuatro coeficientes; $\alpha, \beta, \gamma, \theta$ (que es el número máximo de índices definidos). Su función debería ser la valoración de la influencia de los tres parámetros (A, V, C) en el conjunto de la evaluación de forma desagregada, asignando un coeficiente a cada índice.
- Los coeficientes se analizan en el contexto de cada índice, como elementos dependientes entre si y asignándoles un peso a cada uno en función de la influencia que el índice al que afectan tiene para la amenaza que se evalúa
- Se valoran asignándoles valores comprendidos entre 0 y 1, de forma que la suma de los mismos sea de valor 1; $\alpha_i + \beta_i + \gamma_i + \theta = 1$

Con respecto a la valoración de dichos coeficientes, estos deberán ser evaluados inicialmente, una vez se implantara la metodología de evaluación del riesgo, y sus valores deberán ser permanentes en el tiempo, dado que su valoración se resuelve en base a la relación o peso, que supone cada índice en el conjunto de la metodología y en base a la amenaza a evaluar. Asimismo, y con el fin de definir sus valores de una

forma adecuada y no condicionada, estos sería conveniente que su valor no sea fijado por los responsables directos de la seguridad en los puertos.

5.4. Etapa 4. Elaboración de la Propuesta Metodológica

5.4.1. Propuesta metodológica

Una vez definidos los parámetros y coeficientes a emplear, se trata ahora de enunciar una propuesta metodológica que permita realizar una evaluación del riesgo en instalaciones portuarias considerando los resultados del análisis anterior, ajustándose a las necesidades descritas por los responsables de seguridad y en definitiva al resultado de la investigación. Para ello se ha considerado de interés el esquema metodológico empleado por SECUREPORT, metodología contrastada en su uso y de referencia en esta investigación, manteniendo el esquema de estimación del riesgo en base a los tres principales parámetros, *amenaza*, *vulnerabilidad* y *gravedad*, así como el formato de cálculo y de ponderación de cada parámetro definido.

Asimismo se han considerado como base para la asignación de puntuaciones de los índices los resultados obtenidos en las encuestas al Sector Portuario Español.

En base a la forma en que se evalúa el riesgo derivado de una amenaza en el método simplificado descrito por Fine (1971), se define y evalúa el riesgo de suceso en una instalación o terminal como se indica en la ecuación siguiente.

El indicador representa el riesgo simplificado de la instalación o terminal del puerto (m) asociado a una amenaza dada (i),

$$r_i^m = A_i \cdot V_i \cdot G_i$$

donde:

- r_i^m , es el riesgo simplificado en la instalación o terminal ante una amenaza dada,
- A_i , es la amenaza,
- V_i , es la vulnerabilidad,
- G_i , es la gravedad o consecuencias

Asimismo se define el **riesgo global o promedio**, de carácter cualitativo, en el puerto (K) como:

$$R_T^K = \frac{\sum_{i=1}^n r_i^m}{n}$$

donde:

- R_T^K = riesgo global o promedio del puerto

- r_i^m = riesgo de suceso de una amenaza dada
- n = número de amenazas evaluadas en el puerto

Si bien se han definido seis diferentes tipos de amenazas para esta investigación, en la evaluación del riesgo global de una instalación se pueden considerar más amenazas.

Cada uno de los parámetros anteriores, A_i , V_i y G_i se evalúan mediante una batería de índices que a continuación se describen.

El parámetro de amenaza A , se determina mediante:

$$A_i = (P_T \cdot \alpha_1 + T \cdot \beta_1 + I_s \cdot \gamma_1)$$

Redondeando su resultado al mayor número entero.

Los coeficientes de ponderación tendrán valores comprendidos entre 0-1, resultando su suma:

$$\alpha_1 + \beta_1 + \gamma_1 = 1$$

Siendo:

P_T=Riesgo intrínseco de la fachada. Se trata de valorar el riesgo general contra la seguridad, denominado “*riesgo intrínseco de la fachada*”, es decir la probabilidad de amenaza para cada puerto, valorado en base a la disposición física del mismo en la costa española y al riesgo general que se comprueba que tiene cada instalación del Sistema Portuario en las estadísticas. La disposición del puerto en una fachada o en otra incide sensiblemente en los niveles generales de seguridad general ante posibles amenazas a la instalación. Las fachadas marítimas a considerar para su valoración serán; Cantábrica, Atlántica Norte, Canarias, Estrecho y Mediterránea. En el Estrecho se consideran comprendidos los puertos gestionados por las Autoridades Portuarias de Huelva, Cádiz, Algeciras, Málaga, Motril, Almería, Ceuta y Melilla.

Los niveles de probabilidad de amenaza para cada fachada marítima se valoran como sigue:

- **3 Puntos** Alta
- **2 Puntos** Media
- **1 Punto** Baja

El valor asignado a cada fachada será el mismo para todos los puertos de esta, y puede variar en el tiempo y en función de las condiciones de seguridad de los puertos. Por lo tanto lo deberá fijar el responsable de la seguridad a nivel nacional de los puertos públicos.

T= Riesgo intrínseco de la terminal/instalación portuaria. Se trata de considerar el “*riesgo intrínseco del tipo de terminal o instalación*”, es decir la probabilidad de amenaza que se asocia o define para cada tipo de terminal en función del tipo de mercancía que ésta mueve. Es evidente que la peligrosidad se puede asociar, desde un punto de vista de la probabilidad de suceso, a cada tipo de terminal en virtud del tipo de instalaciones que esta posee y del tipo de actividad que en ella se desarrolla. Así pues, se definen diferentes niveles de amenaza para cada tipo de terminal; contenedores, pasajeros, graneles líquidos, graneles sólidos, etc. basándose en las características particulares de cada tipo de mercancía, zonas de servicios, accesos, edificios, etc.

Los niveles de amenaza para cada tipo de terminal marítima se valoran como sigue:

- **3 Puntos** Alta
- **2 Puntos** Media
- **1 Punto** Baja

El valor asignado a cada tipo de terminal puede variar con el tiempo y las condiciones de seguridad de los puertos, y por lo tanto lo deberá fijar el Administrador del Puerto o los responsables de la seguridad a nivel nacional en puertos públicos.

I_s= Riesgo particularizado. Este índice considera el “*riesgo particular*” de ataque, es decir la probabilidad que se asocia o define para cada tipo de amenaza evaluada en base a las estadísticas de seguridad del puerto. Para ello se consideran las siguientes amenazas, ya descritas en el apartado 5.3.3. *Principales amenazas a considerar*:

- Inmigración ilegal (polizones y tráfico ilegal de personas)
- Robo
- Sabotaje
- Ataque con explosivos/armas de fuego
- Ataque con armas químicas (bio-terrorismo)
- Conflictos laborales

Los valores que pueden tomar se asignarán a cada amenaza en función de su frecuencia de presentación en cada puerto, pudiendo así variar en el tiempo y debiendo ser revisados cada vez que los datos estadísticos denoten un cambio en el nivel de amenaza. Su valor lo deberá definir cada puerto en base a las estadísticas de incidentes de seguridad en el puerto, con el siguiente criterio de puntuación:

- **3 Puntos** Alta
- **2 Puntos** Media

- **1 Punto** Baja

El parámetro de vulnerabilidad V , se determina mediante la obtención de los índices de accesibilidad, layout y de relevancia operativa. Una vez obtenidos estos, el valor del Índice de Vulnerabilidad resultará como:

$$V = (I_{ac} \cdot \alpha_2 + I_{Lo} \cdot \beta_2 + I_{Ro} \cdot \gamma_2)$$

Redondeando el resultado al mayor número entero más próximo.

Los coeficientes de ponderación tendrán valores comprendidos entre 0-1, resultando su suma:

$$\alpha_2 + \beta_2 + \gamma_2 = 1$$

Iac= Índice de accesibilidad. Este índice se redefine, pues ya existía, si bien ahora trata de evaluar la vulnerabilidad de las instalaciones en base a la valoración de diferentes aspectos físicos y operativos, evaluándose para ello los siguientes aspectos:

- Características del cerramiento; altura y facilidad de acceso
- Sistema de control de accesos adecuados:
 - Lector de matrículas
 - Tarjetas de identificación personal
 - Sistema CCTV
 - Alarmas de intrusión,
 - Sensores de movimiento
 - Arcos detectores y scanner
- Experiencia del equipo de seguridad. Este aspecto de gran relevancia, puesto que la experiencia del equipo, así como la disponibilidad o no de patrullas armadas en las terminales pueden reducir considerablemente el riesgo de acceso a la instalación.

Valoración de la Accesibilidad para Terminales de Pasajeros

La valoración de la accesibilidad se realizará utilizando una escala que tendrá los cuatro niveles siguientes en la terminal:

4 ptos. Mala protección del perímetro y/o sistemas de control de accesos y vigilancia no operativos con equipo de seguridad muy poco experimentado. El cerramiento perimetral es <2m de altura y escalable, los controles de accesos no

existen, incluidos los de vehículos, mercancías, equipajes, etc. Los sistemas de vigilancia perimetral funcionan pero no son completos; falta alguno de ellos; sistema CCTV o sensores de movimiento o alarmas de intrusión. El equipo de seguridad tiene una experiencia de entre 2-5 años.

3 ptos. Protección regular del perímetro, sistemas de control de accesos y vigilancia operativos y equipo de seguridad poco experimentado. El cerramiento perimetral es escalable y los controles de accesos son incompletos; lectores de matrícula en acceso a la terminal, arcos detectores y scanner de equipajes, pero no existe control de acceso de personas a la Estación Marítima y zonas de pre-embarque. Los sistemas de vigilancia perimetral funcionan pero no son completos, falta alguno de ellos; sistema CCTV o sensores de movimiento o alarmas de intrusión. La experiencia del equipo de seguridad está entre 2-5 años.

2 ptos. Buena protección del perímetro y sistemas de control de accesos y vigilancia operativos con equipo de seguridad experimentado. El cerramiento perimetral no es escalable y los controles de accesos son completos; lectores de matrícula en acceso a la terminal, arcos detectores y scanner de equipajes, existe control de acceso de personas a la Estación Marítima y zonas de pre-embarque. Los sistemas de vigilancia perimetral funcionan y son completos; sistema CCTV, sensores de movimiento, alarmas de intrusión, etc. La experiencia del equipo de seguridad está entre 5-10 años.

1 pto. Máxima protección del perímetro, sistemas de seguridad de control de accesos operativos y equipo de seguridad muy experimentado. Además existen patrullas armadas permanentemente con posibilidad de intervención rápida, (menos de 5 minutos) en caso de detección de intrusos. La experiencia del equipo de seguridad es superior a 10 años.

Valoración de la Accesibilidad para Terminales de Graneles Líquidos, Graneles Sólidos y Contenedores

4 ptos. Mala protección del perímetro y/o sistemas de control de accesos y vigilancia no operativos con equipo de seguridad muy poco experimentado. El cerramiento perimetral es escalable y los controles de accesos no existen, incluidos los de vehículos y mercancías. Los sistemas de vigilancia perimetral funcionan pero no son completos; falta alguno de ellos; sistema CCTV o sensores de movimiento o alarmas de intrusión. El equipo de seguridad tiene una experiencia de entre 2-5 años.

3 ptos. Protección regular del perímetro, sistemas de control de accesos y vigilancia operativos y equipo de seguridad poco experimentado. El cerramiento perimetral es escalable y los controles de accesos son incompletos; lectores de matrícula en acceso a la terminal, pero no existe control de acceso de personas. Los sistemas de vigilancia perimetral funcionan pero no son completos, falta alguno de

ellos; sistema CCTV o sensores de movimiento o alarmas de intrusión. La experiencia del equipo de seguridad está entre 2-5 años.

2 ptos. Buena protección del perímetro, sistemas de control de accesos y vigilancia operativos y equipo de seguridad experimentado. El cerramiento perimetral no es escalable y los controles de accesos son completos; lectores de matrícula en acceso a la terminal, el control de acceso de personas se realiza con tarjeta. Los sistemas de vigilancia perimetral funcionan pero no están completos, faltando alguno de ellos; sistema CCTV o sensores de movimiento o alarmas de intrusión. La experiencia del equipo de seguridad está entre 5-10 años.

1 pto. Máxima protección del perímetro, sistemas de seguridad de control de accesos operativos y equipo de seguridad muy experimentado. Además existen patrullas armadas permanentemente con posibilidad de intervención rápida (menos de 5 minutos) en caso de detección de intrusos. La experiencia del equipo de seguridad es superior a 10 años.

I_{Lo}= Índice layout. Este índice evalúa la influencia que tiene en la seguridad de un elemento o instalación su disposición próxima a los accesos al puerto (próximo al exterior), así como la proximidad a otras instalaciones de alto riesgo de ataque.

Valoración del Layout.

La valoración del Layout se realizará utilizando una escala que tendrá los cuatro niveles siguientes:

4 ptos. La infraestructura o servicio a proteger está muy próxima a los accesos al puerto y/o a otras instalaciones con alto riesgo de ataque. La infraestructura se sitúa a menos de 100 metros de los accesos al puerto y contigua a otra instalación de alto riesgo. Las instalaciones de alto riesgo pueden ser por ejemplo las terminales de energía; graneles líquidos, contenedores con mercancías peligrosas, etc.

3 ptos. La infraestructura o servicio a proteger está cercana a los accesos al puerto y/o separada de otras instalaciones con alto riesgo de ataque. La infraestructura se sitúa a menos de 100 metros de los accesos al puerto y a menos de 100 m de otra instalación de alto riesgo.

2 ptos. La infraestructura o servicio a proteger está separada de los accesos al puerto y/o próxima a otras instalaciones con alto riesgo de ataque. La infraestructura se sitúa a menos de 300 metros de los accesos al puerto y/o a más de 100 m de otra instalación de riesgo.

1 pto. La infraestructura o servicio a proteger está lejos de los accesos al puerto y/o separada de otras instalaciones con alto riesgo de ataque. La infraestructura se sitúa a más de 300 metros de los accesos al puerto y a más de 300 m de otra instalación de riesgo.

I_{RO}= Índice de Relevancia Operativa. Este índice evalúa la importancia que tienen para la operación portuaria determinadas instalaciones o elementos cuya paralización, en base a una amenaza dada, resultaría relevante para la misma. Un índice no exhaustivo de elementos podría ser el siguiente:

- Infraestructuras de comunicación interna; estructuras, túneles, vías férreas, etc.
- Sistemas de comunicación; telecomunicaciones, fibra óptica, etc.
- Redes de distribución: energía, electricidad, agua, etc.
- Equipos de manipulación de mercancías; grúas portuarias, grúas pórtico, maquinaria auxiliar, etc.
- Instalaciones de almacenamiento; terminales marítimas, tinglados, almacenes, silos, etc.

Valoración de la Relevancia Operativa

La valoración de la Relevancia Operativa se realizará utilizando una escala que tendrá cuatro niveles siguientes:

- **4 puntos** Muy alta
- **3 puntos** Alta
- **2 puntos** Media
- **1 punto** Baja

El parámetro de Gravedad, G, se ha valorado en base a las definiciones descritas en el *artículo 2 Definiciones*, de la *Ley 8/2011 de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*, en lo relativo a la evaluación a realizar para las infraestructuras críticas, entre las que se encuentran los puertos comerciales.

Asimismo, para su definición se ha estimado de interés la consideración de los denominados “Índices de Repercusión”, definidos en la *ROM 0.0: Procedimiento general y bases de cálculo, Criterios Generales*, normativa actualizada de uso en el sistema portuario español, considerándose para su definición en esta metodología de evaluación su alcance y método de evaluación de las consecuencias de una amenaza, si bien los valores de cada nivel de amenaza se cuantifican de forma diferente y en algún caso se han adaptado al alcance de una instalación más amplia que meramente una obra marítima. Dichos índices recogen la importancia económica, social y ambiental de las partes del puerto, valorándolos mediante su carácter general y operativo. El carácter se determinará en función de varios índices cuyo valor se calculará de forma aproximada según el método descrito a continuación.

Así el índice de gravedad G se determina mediante la obtención de cuatro subíndices; repercusión a la vida humana, repercusión económica, repercusión ambiental y repercusión pública y social. Una vez obtenidos estos, el valor del índice de gravedad resultará como:

$$G = (IRE \cdot \alpha_3 + IRH \cdot \beta_3 + IRA \cdot \gamma_3 + IPS \cdot \theta)$$

Redondeando el resultado al mayor número entero más próximo..

Los coeficientes de ponderación tendrán valores comprendidos entre 0-1, resultando su suma:

$$\alpha_2 + \beta_2 + \gamma_2 + \theta = 1$$

Los índices se calculan como se indica a continuación:

IRE= Repercusión económica. Valora la magnitud de las pérdidas económicas y el deterioro de los productos y servicios. Según se describe en la misma, este índice de calcula en base a la estimación de:

$$IRE = \frac{C_{RD} + C_{RI}}{C_0}$$

donde, (C_{RD}), valora cuantitativamente las repercusiones económicas por reconstrucción del elemento, (C_{RI}), por cese o afección de las actividades económicas directamente relacionadas con el esperables, en el caso de producirse la destrucción o la pérdida de operatividad total de la misma y, (C_0), es un parámetro de adimensionalización. Estos costes se determinarán de acuerdo con los siguientes criterios:

C_{RD} , Coste de inversión de las obras de reconstrucción de la infraestructura o instalación a su estado previo, en el año en que se valoren los costes por cese o afección de las actividades económicas directamente relacionadas con la instalación. A falta de estudios de detalle, simplificadaamente, podrá considerarse que este coste es igual a la inversión inicial debidamente actualizada al año citado.

C_{RI} , Repercusiones económicas por cese e influencia de las actividades económicas directamente relacionadas con la instalación, ya sean oferentes de servicios creados tras su puesta en servicio o demandantes y causadas por daños en los bienes defendidos. Se valorará en términos de pérdida de Valor Añadido Bruto (VAB), a precios de mercado durante el periodo que se estime dure la reconstrucción, tras la destrucción o pérdida de operatividad de la instalación, considerando que ésta se produce una vez consolidadas las actividades económicas directamente relacionadas con la obra.

A falta de estudios de detalle, se considerará, en general que la consolidación de actividades económicas directamente relacionadas con la obra se produce transcurridos un cierto número de años desde su entrada en servicio que, a efectos de estas Recomendaciones y salvo justificación en otro sentido, será cinco años. De manera análoga, el periodo de reconstrucción se establecerá en un año.

El VAB es lo que el conjunto de actividades económicas aporta a una economía y representa la diferencia entre inputs y outputs del proceso productivo asociado al conjunto de actividades. Esta diferencia está constituida por la fuerza laboral empleada y por los excedentes empresariales generados. En la contabilidad macroeconómica y de acuerdo con el Sistema Europeo de Cuentas, el VAB se calcula como la suma de las remuneraciones de asalariados (sueldos y salarios brutos y cotizaciones sociales) y el excedente bruto de explotación (descontándose de los costes de la cuenta de resultados de amortizaciones). Su valoración a precios de mercado requiere sumar, a los agregados macroeconómicos anteriores, los impuestos netos ligados a la producción (impuestos brutos menos subvenciones).

C_0 , *Parámetro económico de adimensionalización*. Su valor depende de la estructura económica y del nivel de desarrollo económico del país donde se vaya a construir la obra, variando, en consecuencia, con el transcurso del tiempo, tomándose, en España, para el año horizonte en los que se valoran los costes C_{RD} y C_{RI} , $C_0 = 3$ M Euros.

Evaluación aproximada a falta de datos.

En aquellos casos en los que no se realice una determinación detallada de C_{RI} , bien por razones de complejidad desproporcionada respecto a la magnitud de la infraestructura bien por falta de estudios previos, el valor del IRE podrá estimarse cualitativamente por el método descrito en el Anejo correspondiente de la ROM 0.0, y que se resume aquí:

En aquellos casos en los cuales no se realice una determinación detallada de C_{RI} , bien por razones de complejidad desproporcionada respecto a la magnitud de la obra, bien por falta de estudios previos, el cociente C_{RI}/C_0 , podrá estimarse cualitativamente y de forma aproximada, mediante la ecuación siguiente.

$$C_{RI}/C_0 = (C) \cdot [(A) + (B)]$$

Coefficiente del ámbito del sistema, (A)

El ámbito del sistema productivo al que sirve el elemento se valorará asignando los siguientes valores en función de que aquel sea un ámbito,

- Local, (1)
- Regional, (2)

- Nacional/Internacional, (5)

Coefficiente de la importancia estratégica, (B)

La importancia estratégica del sistema económico y productivo al que sirve el elemento se valorará asignando los siguientes valores en función de que aquella sea,

- Irrelevante, (0)
- Relevante, (2)
- Esencial, (5)

Coefficiente de la importancia económica, (C)

La importancia del elemento/instalación para el sistema económico y productivo al que sirve se valorará asignando los siguientes valores en función de que aquella sea,

- Irrelevante, (0)
- Relevante, (1)
- Esencial, (2)

Clasificación en función del IRE:

- E3, instalación con repercusión económica alta: $IRE > 20$
- E2, instalación con repercusión económica media: $5 < IRE \leq 20$
- E1, instalación con repercusión económica baja: $IRE \leq 5$
- E0, instalación sin repercusión económica significativa: $IRE \leq 3$

Asignándose los siguientes valores para la cuantificación de la repercusión económica:

- **4 ptos.** E3, repercusión económica alta
- **3 ptos.** E2, repercusión económica media
- **2 ptos.** E1, repercusión económica baja
- **1 pto.** E0, repercusión económica insignificante

IRH= Repercusión a la vida humana. Se valora en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública. Se asignarán los siguientes valores en función de dicha posibilidad y alcance (en la evaluación de este subíndice se deberá tener en cuenta la existencia, o no, de sistemas y planes de evacuación de las instalaciones).

- **4 ptos.** Catastrófica, la pérdida de vidas humanas y daños a las personas es tan grave que afecta a la capacidad de respuesta regional.

- **3 ptos.** Alta, el número potencial de víctimas mortales o heridos con lesiones muy graves es seguro, afectando a más de 20 personas.
- **2 ptos.** Baja, el número potencial de víctimas mortales o heridos con lesiones muy graves es posible pero poco probable (accidental), afectando a menos de 5 personas.
- **1 pto.** Remota, es improbable que se produzcan daños a personas.

IRA= Repercusión ambiental. Se valora la degradación en el lugar o sus alrededores. En este caso se considerará el daño al sistema marino y a la calidad de las aguas por vertidos incontrolados o accidentales, o contaminación aérea debida a hidrocarburos.

- **4 ptos.** Alto, daños irreversibles al ecosistema.
- **3 ptos.** Medio, daños importantes pero reversibles (en menos de cinco años).
- **2 ptos.** Bajo, daños leves reversibles (en menos de un año) o pérdidas de elementos de escaso valor.
- **1 pto.** Remoto, es improbable que se produzcan daños ambientales.

IPS= Repercusión pública y social. Valora la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

- **4 ptos.** Muy Alta, alarma social muy alta debido a valores de los subíndices IRH, catastrófico e IRA, muy alto.
- **3 ptos.** Alta, alarma social alta debida a valores de los subíndices IRH e IRA muy altos.
- **2 ptos.** Media, alarma social media asociada a valores de los subíndices IRH y/o IRA altos.
- **1 pto.** Baja, no hay indicios de que pueda existir una alarma social significativa asociada al fallo de la instalación.

5.4.2. Criterios de valoración de los coeficientes

La valoración de los coeficientes se realiza mediante panel de expertos, y en base al peso considerado para cada índice (PT , T , I_S ...). y cada tipo de amenaza contemplada (escenario). Es decir, los coeficientes **se valoran desde la perspectiva de la amenaza a evaluar, de forma exclusiva, sin considerar la ubicación del puerto, el tipo de instalación, etc.** De esta forma, un mismo coeficiente α_1 tendrá un peso o valor diferente para una amenaza de ataque con bomba en una terminal de pasajeros,

que para una terminal de graneles sólidos o para el sabotaje en una instalación eléctrica. La asignación de los pesos es por tanto independiente de la valoración de cada índice, la cual valora la realidad física y operativa de la terminal, mientras que los coeficientes se evalúan acorde con las amenazas e independientemente de las características de la instalación de que se trate. En base a los resultados de la aplicación del criterio experto, se obtuvieron los siguientes pesos para los coeficientes.

Tabla 12. Matrices de riesgo específico

INMIGRACIÓN ILEGAL			ROBO		
Índice	Coeficiente	VALOR	Índice	Coeficiente	VALOR
PT	$\alpha 1$	0,43	PT	$\alpha 1$	0,21
T	$\beta 1$	0,20	T	$\beta 1$	0,44
IS	$\gamma 1$	0,37	IS	$\gamma 1$	0,35
lac	$\alpha 2$	0,62	lac	$\alpha 2$	0,60
llo	$\beta 2$	0,27	llo	$\beta 2$	0,26
lro	$\gamma 2$	0,11	lro	$\gamma 2$	0,14
IRE	$\alpha 3$	0,18	IRE	$\alpha 3$	0,57
IRH	$\beta 3$	0,37	IRH	$\beta 3$	0,11
IRA	$\gamma 3$	0,02	IRA	$\gamma 3$	0,07
IPS	θ	0,43	IPS	θ	0,25

SABOTAJE			ATAQUE CON EXPLOSIVOS/ARMAS CONV.		
Índice	Coeficiente	VALOR	Índice	Coeficiente	VALOR
PT	$\alpha 1$	0,25	PT	$\alpha 1$	0,29
T	$\beta 1$	0,43	T	$\beta 1$	0,47
IS	$\gamma 1$	0,32	IS	$\gamma 1$	0,24
lac	$\alpha 2$	0,34	lac	$\alpha 2$	0,45
llo	$\beta 2$	0,18	llo	$\beta 2$	0,24
lro	$\gamma 2$	0,48	lro	$\gamma 2$	0,31
IRE	$\alpha 3$	0,40	IRE	$\alpha 3$	0,22
IRH	$\beta 3$	0,22	IRH	$\beta 3$	0,40
IRA	$\gamma 3$	0,14	IRA	$\gamma 3$	0,10
IPS	θ	0,24	IPS	θ	0,28

ATAQUE CON ARMAS QUÍMICAS			CONFLICTOS LABORALES		
Índice	Coeficiente	VALOR	Índice	Coeficiente	VALOR
PT	$\alpha 1$	0,30	PT	$\alpha 1$	0,26
T	$\beta 1$	0,45	T	$\beta 1$	0,30
IS	$\gamma 1$	0,25	IS	$\gamma 1$	0,44
Iac	$\alpha 2$	0,43	Iac	$\alpha 2$	0,20
Ilo	$\beta 2$	0,25	Ilo	$\beta 2$	0,20
Iro	$\gamma 2$	0,32	Iro	$\gamma 2$	0,60
IRE	$\alpha 3$	0,14	IRE	$\alpha 3$	0,47
IRH	$\beta 3$	0,33	IRH	$\beta 3$	0,10
IRA	$\gamma 3$	0,20	IRA	$\gamma 3$	0,08
IPS	θ	0,33	IPS	θ	0,35

Fuente: Elaboración propia

5.4.3. Criterios de evaluación del riesgo

Los criterios de evaluación se han fijado siguiendo el mismo esquema de base que se emplea en otras metodologías simplificadas de estimación del riesgo, referenciadas anteriormente en esta investigación (*Anexo 1. Metodologías consideradas*).

Una vez definidos los índices de evaluación del riesgo, se deben definir ahora los criterios de evaluación del riesgo en base a los valores resultantes del riesgo específico (r_i), y del riesgo global (R_T).

El rango de valores enteros que pueden alcanzar los índices es el siguiente:

- Índice de amenaza (A); entre 1 y 3 puntos
- Índice de vulnerabilidad (V); entre 1 y 4 puntos
- Índice de gravedad (G); entre 1 y 4 puntos

Los resultados obtenidos para cada riesgo se redondean al entero más próximo. De esta manera el resultado de la evaluación del riesgo específico (r_i) estará comprendido entre un valor mínimo de 1 punto y un valor máximo de 48 puntos.

Los resultados de la evaluación se representan gráficamente de manera que se establezca la clasificación del riesgo. Se definen tres matrices de valoración, en función de los valores del índice de amenaza (A), que toma valores de 1, 2 y 3 puntos. Las matrices indican en columna los diferentes valores que se obtienen para la

Gravedad (G) y en fila los diferentes valores que se obtienen para la Vulnerabilidad (V).

Las matrices de riesgo se presentan a continuación.

Tabla 13. Matrices de riesgo específico

MATRIZ DE RIESGO ESPECÍFICO (A=1)				
INDICES	G=1	G=2	G=3	G=4
V=4	4	8	12	16
V=3	3	6	9	12
V=2	2	4	6	8
V=1	1	2	3	4

MATRIZ DE RIESGO ESPECÍFICO (A=2)				
INDICES	G=1	G=2	G=3	G=4
V=4	8	16	24	32
V=3	6	12	18	24
V=2	4	8	12	16
V=1	2	4	6	8

MATRIZ DE RIESGO ESPECÍFICO (A=3)				
INDICES	G=1	G=2	G=3	G=4
V=4	12	24	36	48
V=3	9	18	27	36
V=2	6	12	18	24
V=1	3	6	9	12

Fuente: Elaboración propia

Como se aprecia en las matrices, se obtienen valores comprendidos entre 1 y 16 para el caso en el que el valor de la amenaza sea 1, valores comprendidos entre 2 y 32

para el caso en que el valor de la amenaza sea de 2, y valores comprendidos entre 3 y 48 en el caso de que el valor de la amenaza sea de 3.

Por su parte, la evaluación del riesgo global de la instalación (R_T) se obtiene como el valor promedio de los valores obtenidos para cada riesgo específico evaluado.

5.4.4. Evaluación del riesgo

La evaluación del riesgo se realiza en base a la comparación del riesgo ($r_1, r_2, \dots$) que se obtiene para cada caso en estudio con los resultados de las matrices definidas, con unos criterios de aceptación definidos previamente.

Para ello se establecen diferentes categorías del riesgo que se recogen en la tabla siguiente.

Tabla 14. Evaluación del riesgo

Categoría del riesgo	Puntuación	Acciones requeridas
Intolerable	$r \geq 16$	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en lo posible debe mitigarse
Elevado	$9 < r \leq 12$	Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados
Admisible	$6 \leq r \leq 9$	Aceptable pero la amenaza debe ser evaluada periódicamente
Insignificante	$r \leq 4$	Aceptable

Fuente: Elaboración propia

En base a estas categorías del riesgo se comprueba que existen 22 situaciones de riesgo intolerable, 8 situaciones peligrosas, 9 situaciones de riesgo admisible, y 9 situaciones de riesgo insignificante.

Capítulo | 6

Aplicación a las Instalaciones
de un Puerto

6. APLICACIÓN A LAS INSTALACIONES DE UN PUERTO

6.1. Objeto

Una vez descritos los parámetros que definen la propuesta metodológica de evaluación del riesgo en puertos, se va a aplicar a modo de ejemplo, a un puerto del Sistema Portuario Español. Para ello se ha escogido el Puerto de Melilla, debido a sus características, a su representatividad para la seguridad en el conjunto del sistema portuario y a su localización en el norte de la costa de África, posición que le convierte en un puerto de interés ante cualquier ataque o incidente de los considerados en el estudio. Otra motivación para su selección es que dicho puerto fue el seleccionado asimismo por el proyecto SEDUCE (CDTI, 2011) como infraestructura portuaria para la evaluación de las amenazas derivadas del uso de explosivos, lo que permitirá comparar los resultados de la aplicación de la metodología con aquellos.

6.2. Amenazas evaluadas

Se seleccionaron para su evaluación seis situaciones de amenaza definidas en diferentes instalaciones del puerto. Estas son:

1. Inmigración ilegal: Intrusos penetran en la Terminal de Pasajeros con el objetivo de subir a un buque como polizones con destino a un puerto europeo y efectúan numerosos destrozos en la terminal; rotura de cerramientos, puertas, sistemas de control de acceso, etc.).
2. Robo: Intrusos penetran en las instalaciones de la Terminal de Contenedores, abren varios contenedores y roban mercancía de estos.
3. Sabotaje: Intrusos penetran en las instalaciones del puerto con la intención de sabotear las grúas de la Terminal de Contenedores.
4. Ataque con explosivos: Intrusos penetran en las instalaciones del puerto con la intención de atacar con explosivos las instalaciones de la Terminal de Pasajeros.
5. Ataque con armas químicas. Se produce el ataque con armas químicas en la Terminal de Pasajeros del puerto.

6. Conflictos laborales. Los trabajadores realizan una huelga en reclamación de mejoras salariales y algunos piquetes realizan daños a las grúas del patio de la Terminal de Contenedores y cables de suministro eléctrico.

6.3. Evaluación del riesgo

La evaluación se realizó mediante el empleo de una hoja de cálculo, donde se valoraron cada uno de los diferentes índices en función del conocimiento previo que se tiene de las instalaciones del puerto y de sus sistemas de seguridad, descritos en el proyecto SEDUCE (2011).

Se han tomado las siguientes consideraciones previas a la evaluación:

- El análisis se centra en definir varias amenazas en diferentes terminales del Puerto. Se han considerado las siguientes terminales por considerarse las de mayor interés para el cálculo global del riesgo:
 - Terminal de Pasajeros y,
 - Terminal de Contenedores
- El índice T se ha valorado en base a los resultados enunciados de peligrosidad de las terminales. Los valores que se han asignado para cada terminal son:
 - Terminal de Pasajeros, T=3 y,
 - Terminal de Contenedores, T=2
- El índice PT se considerado de valor alto (3) debido a la ubicación del Puerto en la fachada del Estrecho.
- Se estima una accesibilidad muy limitada a ambos tipos de terminal debido al sistema de vigilancia que este Puerto posee y que se encuentra entre los mejores del Sistema Portuario Español.
- El CRD (Coste de inversión de las obras de reconstrucción de la infraestructura o instalación) a su estado previo se han supuesto de diferentes importes en base a la amenaza de que se trate.

A continuación se presenta el resultado de la evaluación para cada amenaza considerada.

AMENAZA 1. INMIGRACIÓN ILEGAL

AMENAZA 1				PUERTO DE MELILLA. TERMINAL DE PASAJEROS. Inmigración ilegal: Intrusos penetran con el objetivo de subir a un buque como polizones con destino a un puerto europeo y efectuan numerosos destrozos en la terminal; rotura de cerramientos, puertas, etc)			
		Valor real	Valor redondeado				
A		2,8	3				
PT	3	α1	0,43	Fachada de alto riesgo			
T	2	β1	0,20	Terminal de rieso medio			
IS	3	γ1	0,37	Amenaza de alto riesgo en este puerto			
V		1,9	2				
Iac	2	α2	0,62	El cerramiento perimetral no es escalable y los controles de accesos son completos; lectores de matrícula en acceso a la terminal, el control de acceso de personas se realiza con tarjeta. Los sistemas de vigilancia perimetral funcionan pero no están completos.			
Ilo	2	β2	0,27	Se sitúa a menos de 300 m de los accesos al puerto.			
Iro	1	γ2	0,11	Bajo			
G		1,7	2				
IRE	3	α3	0,18				
$C_{R1}/C_0 = (A+B) \cdot C$				alta: IRE > 20 media: 5 < IRE ≤ 20 baja: IRE ≤ 5 sin repercusión significativa: IRE ≤ 3			
A	5				$IRE = \frac{C_{R1} + C_{R2}}{C_0}$		
B	5						
C	2						
CRD	0,1						
Co	3				CRD= 0,1 M€, reconstrucción elementos Co= 3 M€ (fijado por la ROM 0.0)		
IRH	2	β3	0,37	Baja, número potencial de víctimas mortales o heridos con lesiones muy graves es posible pero poco probable (accidental), afectando a menos de 5 personas.			
IRA	1	γ3	0,02	Remoto, es improbable que se produzcan daños ambientales.			
IPS	1	φ	0,43	Baja, no hay indicios de que pueda existir una alarma social significativa asociada al fallo de la instalación			
Riesgo específico (r1)		12		RIESGO ELEVADO			
MATRIZ DE RIESGO ESPECIFICO (A=3)						Acciones requeridas	
INDICES	G=1	G=2	G=3	G=4	Categoría del riesgo	Puntuación	
V=4	12	24	36	48	Intolerable	r ≥ 16	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en lo posible debe mitigarse
V=3	9	18	27	36	Elevado	9 < r ≤ 12	Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados
V=2	6	12	18	24	Admisible	6 ≤ r ≤ 9	Aceptable pero la amenaza debe ser evaluada periódicamente
V=1	3	6	9	12	Insignificante	r ≤ 4	Aceptable

AMENAZA 2. ROBO

Amenaza 2				<p>PUERTO DE MUELLA. TERMINAL DE CONTENEDORES. Robo: intrusos penetran en las instalaciones anulando varias cámaras y forzando varios contenedores, robando mercancía de estos.</p>
	Valor real	Valor redondeado		
A	1,9	2		
PT	3	0,21		
T	2	0,44		
IS	1	0,35		
V	1,6	2		
Iac	2	0,60		
Ilo	1	0,26		
IRo	1	0,14		
G	2,1	2		<p>Puerto de alto riesgo general en esta fachada</p> <p>Terminal de riesgo medio (contenedores)</p> <p>Amenaza de bajo riesgo en este puerto</p> <p>El cerramiento perimetral no es escalable y los controles de accesos son completos; lectores de matrícula en acceso a la terminal, el control de acceso de personas se realiza con tarjeta. Los sistemas de vigilancia perimetral funcionan pero no están completos.</p> <p>La terminal se dispone lejos de los accesos al puerto y separada de otras instalaciones con alto riesgo de ataque.</p> <p>Bajo, ningún elemento de relevancia se ve afectado</p>
IRE	3	0,57		
$C_{RI}/C_0 = (A+B)^{-1} \cdot C$				
A	2			
B	5			
C	2			
CRD	2			
Co	3			
IRH	1	0,11		
IRA	1	0,07		
IPS	1	0,25		
Riesgo específico (r2)			8	<p>alta: IRE > 20</p> <p>media: 5 < IRE ≤ 20</p> <p>baja: IRE ≤ 5</p> <p>sin repercusión significativa: IRE ≤ 3</p>
				<p>CRD= 2 M€, reconstrucción elementos</p> <p>Co= 3 M€ (fijado por la ROM 0.0)</p>
				<p>Remota, es improbable que se produzcan daños a personas</p> <p>Remoto, es improbable que se produzcan daños ambientales.</p> <p>Baja, no hay indicios de que pueda existir una alarma social significativa asociada al fallo de la instalación</p>
Riesgo admisible			8	<p>E3, repercusión económica alta</p> <p>E2, repercusión económica media</p> <p>E1, repercusión económica baja</p> <p>E0, repercusión económica insignificante</p>
MATRIZ DE RIESGO ESPECÍFICO (A=2)				<p>Categoría del riesgo</p> <p>Puntuación</p> <p>Acciones requeridas</p> <p>Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en lo posible debe mitigarse</p> <p>Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados</p> <p>Aceptable pero la amenaza debe ser evaluada periódicamente</p> <p>Aceptable</p>
INDICES	G=1	G=2	G=3	G=4
V=4	8	16	24	32
V=3	6	12	18	24
V=2	4	8	12	16
V=1	2	4	6	8

AMENAZA 3. SABOTAJE

Amenaza 3				<div>PUERTO DE MEJILLA. TERMINAL DE CONTENEDORES. Sabotaje: Intrusos penetran en las instalaciones del puerto y sabotean varias de las grúas del muelle.</div> <div>Puerto de alto riesgo general en esta fachada</div> <div>Terminal de riesgo medio (contenedores)</div> <div>Amenaza de alto riesgo en este puerto</div> <div>Buena protección del perímetro y sistemas de control de accesos y vigilancia operativos con equipo de seguridad experimentado.</div> <div>La terminal se dispone lejos de los accesos al puerto y separada de otras instalaciones con alto riesgo de ataque.</div> <div>Alta, sabotean varias grúas del muelle</div> <div>alta: IRE > 20 media: 5 < IRE ≤ 20 baja: IRE ≤ 5 sin repercusión significativa: IRE ≤ 3</div> <div><div>CRD= 2 M€, reconstrucción elementos</div><div>Co= 3 M€ (fijado por la ROM 0.0)</div></div> <div>Remota, es improbable que se produzcan daños a personas.</div> <div>Remoto, es improbable que se produzcan daños ambientales.</div> <div>Baja, no hay indicios de que pueda existir una alarma social significativa asociada al fallo de la instalación</div> <div>RIESGO ADMISIBLE</div> <div>14,7 ≤ 20 MEDIA</div> <div>$IRE = \frac{C_{ro} + C_{ri}}{C_g}$</div> <div>E3, repercusión económica alta</div> <div>E2, repercusión económica media</div> <div>E1, repercusión económica baja</div> <div>E0, repercusión económica insignificante</div>
		Valor real	Valor redondeado	
A		2,3	2	
	PT	3	0,25	
	T	β1	0,43	
	IS	γ1	0,32	
V		2,3	2	
	Iac	α2	0,34	
	Ilo	β2	0,18	
	Iro	γ2	0,48	
G		1,8	2	
	IRE	3	0,40	
$C_R/C_O = (A+B)^2 \cdot C$				
	A	2		
	B	5		
	C	2		
	CRD	2		
	Co	3		
	IRH	1	0,22	
	IRA	1	0,14	
	IPS	1	0,24	
Riesgo específico (r3)			8	

MATRIZ DE RIESGO ESPECÍFICO (A=2)				
INDICES	G=1	G=2	G=3	G=4
V=4	8	16	24	32
V=3	6	12	18	24
V=2	4	8	12	16
V=1	2	4	6	8

Categoría del riesgo	Puntuación	Acciones requeridas
Intolerable	r2 16	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en lo posible debe mitigarse
Elevado	9<r3 12	Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados
Admisible	6<r3 9	Aceptable pero la amenaza debe ser evaluada periódicamente
Insignificante	r4 4	Aceptable

AMENAZA 4. ATAQUE CON EXPLOSIVOS

AMENAZA 4				PUERTO DE MEULLA. TERMINAL DE PASAJEROS. Ataque con explosivos: Intrusos penetran en las instalaciones del puerto con la intención de atacar con explosivos la zona de pre-embarque de la terminal.				
		Valor real	Valor redondeado					
A		2,5	3					
PT		3	α1	0,29	Puerto de alto riesgo general en esta fachada			
T		3	β1	0,47	Terminal de riesgo alto (Pasajeros)			
IS		1	γ1	0,24	Amenaza de bajo riesgo (actualmente) en este puerto			
V			2,7	3	Buena protección del perímetro y sistemas de control de accesos y vigilancia operativos con equipo de seguridad experimentado.			
Iac		3	α2	0,45	Se sitúa a menos de 300 m de los accesos al puerto.			
ILO		3	β2	0,24	Media, la explosión afecta a algunos elementos importantes para el funcionamiento de la estación marítima.			
IRO		2	γ2	0,31				
G			2,3	2				
IRE		2	α3	0,22	<div>alta: IRE > 20 media: 5 < IRE ≤ 20 baja: IRE ≤ 5 sin repercusión significativa: IRE ≤ 3</div>			
$C_{IR}/C_0=(A+B)^{-C}$		4						
A		2						
B		2						
C		1						
CRD		1		<div>CRD= 1 M€, reconstrucción elementos Co= 3 M€ (fijado por la ROM 0.0)</div>				
Co		3						
IRH		3	β3	0,40	Alta, el número potencial de víctimas mortales o heridos con lesiones muy graves es segura, afectando a más de 20 personas			
IRA		1	γ3	0,10	Remoto, es improbable que se produzcan daños ambientales			
IPS		2	φ	0,28	Media, alarma social media asociada a valores de los subíndices IRH y/o IRA altos			
Riesgo específico (r4)				RIESGO INTOLERABLE				

C _{IR} = $\frac{C_{I0} + C_{IR}}{C_0}$		4,3 ≤ 20 BAJA	
alta: IRE > 20 media: 5 < IRE ≤ 20 baja: IRE ≤ 5 sin repercusión significativa: IRE ≤ 3			
CRD=		1	M€, reconstrucción elementos
Co=		3	M€ (fijado por la ROM 0.0)

C _{IR} = $\frac{C_{I0} + C_{IR}}{C_0}$		4,3 ≤ 20 BAJA	
alta: IRE > 20 media: 5 < IRE ≤ 20 baja: IRE ≤ 5 sin repercusión significativa: IRE ≤ 3			
CRD=		1	M€, reconstrucción elementos
Co=		3	M€ (fijado por la ROM 0.0)

Alta, el número potencial de víctimas mortales o heridos con lesiones muy graves es segura, afectando a más de 20 personas	
Remoto, es improbable que se produzcan daños ambientales	
Media, alarma social media asociada a valores de los subíndices IRH y/o IRA altos	

RIESGO INTOLERABLE	
--------------------	--

Categoría del riesgo	Puntuación	Acciones requeridas
Intolerable	r≥ 16	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en lo posible debe mitigarse
Elevado	9<r≤12	Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados
Admisible	6<r≤9	Aceptable pero la amenaza debe ser evaluada periódicamente
Insignificante	r≤4	Aceptable

MATRIZ DE RIESGO ESPECÍFICO (A=3)				
INDICES	G=1	G=2	G=3	G=4
V=4	12	24	36	48
V=3	9	18	27	36
V=2	6	12	18	24
V=1	3	6	9	12

AMENAZA 5. ATAQUE CON ARMAS QUÍMICAS

Amenaza 5				PUERTO DE MELILLA. TERMINAL DE PASAJEROS. Ataque con armas químicas: Se produce un ataque con armas químicas en la terminal de pasajeros.			
		Valor real	Valor redondeado				
A		2,5	3				
PT		α1	0,30	Puerto de alto riesgo general en esta fachada			
T		β1	0,45	Terminal de riesgo alto (Pasajeros)			
IS		γ1	0,25	Amenaza de bajo riesgo (actualmente) en este puerto			
V		1,8	2				
Iac		α2	0,43	El cerramiento perimetral no es escalable y los controles de accesos son completos; lectores de matrícula en acceso a la terminal, el control de acceso de personas se realiza con tarjeta. Los sistemas de vigilancia perimetral funcionan pero no están completos.			
ILO		β2	0,25	Se sitúa a menos de 300 m de los accesos al puerto.			
IRO		γ2	0,32	Importancia media, puesto que se paralizarían algunas operaciones portuarias			
G		2,5	2				
IRE		α3	0,14				
$C_{R0}/C_0=(A+B)/C$		4					
A		2					
B		2					
C		1					
CRD		0,01					
Co		3					
IRH		β3	0,33	Alta, el número potencial de víctimas mortales o heridos con lesiones muy graves es segura, afectando a más de 20 personas			
IRA		γ3	0,20	Bajo, daños leves reversibles (en menos de un año) o pérdidas de elementos de escaso valor			
IPS		φ	0,33	Media, alarma social media asociada a valores de los subíndices IRH y/o IRA altos			
Riesgo específico (r5)			12	RIESGO ELEVADO			

AMEMAZA 6. CONFLICTOS LABORALES

AMENAZA 6				PUERTO DE MELILLA. TERMINAL DE CONTENEDORES. Conflicto laboral: Los trabajadores realizan una huelga en reclamación de mejoras salariales y algunos piquetes realizan daños a las gruas del patio de la terminal y cables de suministro eléctrico.			
		Valor real	Valor redondeado				
A		1,8	2	Puerto de alto riesgo general en esta fachada			
PT	3	α1	0,26	Terminal de riesgo medio (contenedores)			
T	2	β1	0,30	Amenaza de bajo riesgo (actualmente) en este puerto			
IS	1	γ1	0,44				
V		2,4	2				
Iac	2	α2	0,20	El cerramiento perimetral no es escalable y los controles de accesos son completos; lectores de matrícula en acceso a la terminal, el control de acceso de personas se realiza con tarjeta. Los sistemas de vigilancia perimetral funcionan pero no están completos.			
Ilo	1	β2	0,20	La terminal se dispone lejos de los accesos al puerto y separada de otras instalaciones con alto riesgo de ataque.			
Iro	3	γ2	0,60	Alta, dañan varios neumáticos de las gruas portico y cortan cables de suministro eléctrico			
G		2,0	2				
IRE	3	α3	0,47				
$C_{RI}/C_{RI}=(A+B)/C$		14		14,1 ≤ 20 MEDIA			
A	2			alta: IRE > 20			
B	5			media: 5 < IRE ≤ 20			
C	2			baja: IRE ≤ 5			
CRD	0,2			sin repercusión significativa: IRE ≤ 3			
Co	3						
IRH	1	β3	0,10	CRD= 0,2 M€, reconstrucción elementos			
IRA	2	γ3	0,08	Co= 3 M€ (fijado por la ROM 0.0)			
IPS	1	φ	0,35				
Riesgo específico (r6)			8				
MATRIZ DE RIESGO ESPECÍFICO (A=2)							
INDICES	G=1	G=2	G=3	G=4	Categoría del riesgo		
V=4	8	16	24	32	Intolerable	r ≥ 16	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en lo posible debe mitigarse
V=3	6	12	18	24	Elevado	9 < r ≤ 12	Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados
V=2	4	8	12	16	Admisible	6 < r ≤ 9	Aceptable pero la amenaza debe ser evaluada periódicamente
V=1	2	4	6	8	Insignificante	r ≤ 4	Aceptable
				Acciones requeridas			
				E3, repercusión económica alta			
				E2, repercusión económica media			
				E1, repercusión económica baja			
				E0, repercusión económica insignificante			
				4 Puntos			
				3 Puntos			
				2 Puntos			
				1 Puntos			

6.4. Resultados

La evaluación realizada muestra que el resultado para los riesgos específicos será el siguiente:

Tabla 15. Resultados para el riesgo específico

Fuente: Elaboración propia

r1	12	Elevado
r2	8	Admisible
r3	8	Admisible
r4	18	Intolerable
r5	12	Elevado
r6	8	Admisible

Según su puntuación, valorada sobre 48 puntos máximos y ordenándolos de mayor a menor, los riesgos resultan:

1. $r_4 \equiv$ Ataque con explosivos a la terminal de pasajeros, 18 ptos.
2. $r_1 \equiv$ Inmigración ilegal en terminal de pasajeros: 12 ptos,
3. $r_5 \equiv$ Ataque con armas químicas en la terminal de pasajeros, 12 ptos.
4. $r_2 \equiv$ Robo en terminal de contenedores; 8 ptos,
5. $r_3 \equiv$ Sabotaje de grúas portacontenedores, 8 ptos,
6. $r_6 \equiv$ Conflicto laboral (huelga) en la terminal de contenedores, 8 ptos.

A la vista de los resultados obtenidos, se concluye que los riesgos de mayor relevancia en las instalaciones del puerto son los de ataque con explosivos en la terminal de pasajeros junto con el de inmigración ilegal, y el ataque con armas químicas, también en la terminal de pasajeros, siendo los de mayor relevancia los catalogados como *riesgos elevados* (r_1 y r_5), resultados muy acordes con la realidad de un puerto cuya situación geográfica implica un mayor grado de peligrosidad, y cuya accesibilidad a la Estación Marítima es alta (los tres riesgos más altos se asocian a amenazas en la terminal de pasajeros), a pesar de tener unos buenos sistemas de video vigilancia.

Las amenazas de ataque con explosivos y de ataque con armas químicas en la terminal de pasajeros muestran valores altos (18 ptos. y 12 ptos.) debido a las debilidades sistémicas de este tipo de instalaciones, independientemente de su ubicación en uno u otro puerto. Se trata por tanto de riesgos que difícilmente pueden

evitarse actualmente, si bien mediante video vigilancia y la presencia policial pueden disminuirse de forma importante.

El riesgo de inmigración ilegal resulta elevado para la operación y la seguridad de la instalación, pues se trata de un problema continuo en este puerto y que supone una dificultad a la larga para la operación normal del puerto en su conjunto, además de ser un problema para la ciudad de Melilla.

Los riesgos de inmigración ilegal y ataque con armas químicas resultan elevados y solo se aceptarán cuando los esfuerzos para prevenir/mitigar el impacto son muy elevados, y en todo caso deberán intentar rebajarse mediante las correspondientes medidas en el Plan de Seguridad del Puerto.

Las amenazas con menor puntuación (r_2 , r_3 y r_6) se producen en la terminal de contenedores, de menor riesgo general que la terminal de pasajeros según las encuestas realizadas. Todas ellas son consideradas de *riesgo admisible*, si bien deben ser evaluadas periódicamente.

El robo en contenedores se clasifica como *riesgo admisible* dado que la instalación tiene un buen sistema de protección perimetral y de accesos, y por tanto se deduce que se trata de un riesgo posible pero no habitual y de ahí que resulte con dicha calificación. No obstante como se indica en el cuadro de valoración del riesgo conviene evaluar periódicamente la amenaza para valorar posibles acciones correctoras si el problema persiste.

El riesgo de sabotaje de las grúas de muelle de la terminal de contenedores se evalúa de la misma manera que el anterior y su resultado (8 ptos) indica una posibilidad de dicho suceso, si bien en un grado bajo. En este caso los adecuados sistemas de control de accesos y de video vigilancia del puerto impiden que esta amenaza sea elevada.

El riesgo asociado a la amenaza de conflictos laborales resulta de escasa relevancia también, a pesar de que los riesgos económicos podrían ser elevados potencialmente, debido a que en este puerto los conflictos laborales no son habituales.

Una vez evaluados los riesgos específicos se calcula el Riesgo Global del puerto. Este se obtiene como el valor promedio de los riesgos específicos obtenidos.

El resultado del **Riesgo Global** del puerto será:

$$R_T = 11 \text{ ptos,}$$

Considerado por tanto como un **riesgo elevado**. Este resultado parece coherente con un puerto que, a pesar de tener un buen sistema de seguridad no puede evitar que algunas amenazas resulten elevadas por el hecho de disponerse en la fachada marítima del Estrecho, de mayor probabilidad de riesgo general que otras.

Por otra parte y si se comparan los resultados obtenidos con los que muestra el proyecto SEDUCE (CDTI, 2011) para el mismo puerto en aquellas amenazas evaluadas del mismo tipo, como son el sabotaje de las grúas o la colocación de explosivos en la Estación Marítima, se comprueba que en el primer caso el valor del riesgo que se deduce de la metodología aquí mostrada, es ligeramente inferior al de SEDUCE que figura como Nivel de Riesgo 2, “Serio”, mientras que el nivel de riesgo que resulta aquí para el segundo tipo de amenaza valorada, el ataque con explosivos a la Estación Marítima, es Intolerable, y para SEDUCE el mismo ataque resulta de Nivel de Riesgo 1, “Intolerable” también.

6.5. Análisis de sensibilidad de los coeficientes

Un análisis de sensibilidad intenta evaluar el impacto que los datos de entrada o de las restricciones especificadas a un modelo definido, en el resultado final o en las variables de salida del modelo (Turban, 2001).

Una vez definidos los coeficientes mediante el criterio experto, y aplicados a la evaluación del riesgo de las seis amenazas consideradas en la investigación en el Puerto de Melilla, se realiza un análisis de sensibilidad de los coeficientes considerados, con el fin de evaluar como varían los resultados obtenidos en base a escenarios de valoración diferente. Se trata por tanto de encontrar un rango de validez de los valores resultantes del criterio experto.

Para ello se han considerados dos escenarios diferentes para cada parámetro; amenaza (A), vulnerabilidad (V) y gravedad (G), y para cada una de las seis amenazas consideradas. De esta forma en el Escenario 1 se definen criterios de valoración diferentes a los tres índices correspondientes a cada parámetro, y se mantienen el resto con sus valores de experto, debiendo sumar siempre uno entre todos los coeficientes. En el escenario 2 se modifica de nuevo el criterio de los índices, pero en sentido opuesto al primer escenario con el fin de definir un intervalo de validez y variando así el peso de estos. De la misma forma se actúa con los escenarios 3 y 4 y escenarios 5 y 6.

La conclusión que se desprende es que los valores considerados en los rangos propuestos en el análisis, son valores coherentes con los resultados del Criterio Experto, y por tanto se mantienen los criterios de valoración y ponderación para los coeficientes propuestos por los expertos. De esta manera se obtiene un rango de valores en el cual los valores asignados por criterio experto no modifican el resultado.

En las páginas siguientes se muestra el resultado del análisis de sensibilidad realizado.

AMENAZA 1. INMIGRACION ILEGAL

Categoría del riesgo	Puntuación	Acciones requeridas
Inabordable	≥ 16	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en lo posible debe mitigarse.
Elevado	9<r≤12	Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados.
Admisible	6<r≤9	Aceptable pero la amenaza debe ser evaluada periódicamente.
Insignificante	r≤4	Aceptable

Escenario 2				
	A	Valor real	Valor redondeado	
PT	3	α1	0,20	
T	2	β1	0,30	
IS	3	γ1	0,50	
V		1,9	2	
Iac	2	α2	0,62	
Ilo	2	β2	0,27	
Iro	1	γ2	0,11	
G		1,7	2	
IRE	3	α3	0,18	
IRH	2	β3	0,37	
IRA	1	γ3	0,02	
IPS	1	φ	0,43	
Riesgo específico (r1)			12	

Escenario 4				
	A	Valor real	Valor redondeado	
PT	3	α1	0,43	
T	2	β1	0,20	
IS	3	γ1	0,37	
V		1,7	2	
Iac	2	α2	0,50	
Ilo	2	β2	0,20	
Iro	1	γ2	0,30	
G		1,7	2	
IRE	3	α3	0,18	
IRH	2	β3	0,37	
IRA	1	γ3	0,02	
IPS	1	φ	0,43	
Riesgo específico (r1)			12	

Escenario 6				
	A	Valor real	Valor redondeado	
PT	3	α1	0,43	
T	2	β1	0,20	
IS	3	γ1	0,37	
V		1,9	2	
Iac	2	α2	0,62	
Ilo	2	β2	0,27	
Iro	1	γ2	0,11	
G		1,8	2	
IRE	3	α3	0,25	
IRH	2	β3	0,30	
IRA	1	γ3	0,10	
IPS	1	φ	0,35	
Riesgo específico (r1)			12	

Escenario 1				
	A	Valor real	Valor redondeado	
PT	3	α1	0,70	
T	2	β1	0,10	
IS	3	γ1	0,20	
V		1,9	2	
Iac	2	α2	0,62	
Ilo	2	β2	0,27	
Iro	1	γ2	0,11	
G		1,7	2	
IRE	3	α3	0,18	
IRH	2	β3	0,37	
IRA	1	γ3	0,02	
IPS	1	φ	0,43	
Riesgo específico (r1)			12	

Escenario 3				
	A	Valor real	Valor redondeado	
PT	3	α1	0,43	
T	2	β1	0,20	
IS	3	γ1	0,37	
V		2,0	2	
Iac	2	α2	0,70	
Ilo	2	β2	0,30	
Iro	1	γ2	0,00	
G		1,7	2	
IRE	3	α3	0,18	
IRH	2	β3	0,37	
IRA	1	γ3	0,02	
IPS	1	φ	0,43	
Riesgo específico (r1)			12	

Escenario 5				
	A	Valor real	Valor redondeado	
PT	3	α1	0,43	
T	2	β1	0,20	
IS	3	γ1	0,37	
V		1,9	2	
Iac	2	α2	0,62	
Ilo	2	β2	0,27	
Iro	1	γ2	0,11	
G		1,5	2	
IRE	3	α3	0,00	
IRH	2	β3	0,50	
IRA	1	γ3	0,00	
IPS	1	φ	0,50	
Riesgo específico (r1)			12	

Amenaza 1. Inmigración ilegal				
	A	Valor real	Valor redondeado	
PT	3	α1	0,43	
T	2	β1	0,20	
IS	3	γ1	0,37	
V		1,9	2	
Iac	2	α2	0,62	
Ilo	2	β2	0,27	
Iro	1	γ2	0,11	
G		1,7	2	
IRE	3	α3	0,18	
IRH	2	β3	0,37	
IRA	1	γ3	0,02	
IPS	1	φ	0,43	
Riesgo específico (r1)			12	

AMENAZA 2. ROBO

Categoría del riesgo	Puntuación	Acciones requeridas
Intolerable	r2 r6	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en lo posible debe mitigarse.
Elevado	9-r5 r12	Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados.
Admisible	6-r5 r9	Aceptable pero la amenaza debe ser evaluada periódicamente.
Insignificante	r4	Aceptable.

Escenario 2				
A	Valor real	Valor redondeado		
	1,8	2,0		
PT 3	$\alpha 1$	0,24		
T 2	$\beta 1$	0,36		
IS 1	$\gamma 1$	0,40		
V	1,6	2		
Iac 2	$\alpha 2$	0,60		
Ilo 1	$\beta 2$	0,26		
Iro 1	$\gamma 2$	0,14		
G	2,1	2		
IRE 3	$\alpha 3$	0,57		
IRH 1	$\beta 3$	0,11		
IRA 1	$\gamma 3$	0,07		
IPS 1	ϕ	0,25		
Riesgo específico (r2)		8		
RIESGO ADMISIBLE				

Escenario 1				
A		Valor real	Valor redondeado	
		2,0	2	
PT	3	$\alpha 1$	0,15	
T	2		0,65	
IS	1	$\gamma 1$	0,20	
V		1,6	2	
Iac	2	$\alpha 2$	0,60	
Ilo	1	$\beta 2$	0,26	
IRo	1	$\gamma 2$	0,14	
G		2,1	2	
IRE	3	$\alpha 3$	0,57	
IRH	1	$\beta 3$	0,11	
IRA	1	$\gamma 3$	0,07	
IPS	1	ϕ	0,25	
Riesgo específico (r2)				8
RIESGO ADMISIBLE				

Amenaza 2. Robo				
A	Valor real	Valor redondeado		
	1,9	2		
PT 3	$\alpha 1$	0,21		
T 2	$\beta 1$	0,44		
IS 1	$\gamma 1$	0,35		
V	1,6	2		
Iac 2	$\alpha 2$	0,60		
Ilo 1	$\beta 2$	0,26		
Iro 1	$\gamma 2$	0,14		
G	2,1	2		
IRE 3	$\alpha 3$	0,57		
IRH 1	$\beta 3$	0,11		
IRA 1	$\gamma 3$	0,07		
IPS 1	ϕ	0,25		
Riesgo específico (r2)				
			RIESGO ADMISIBLE	
			8	

Escenario 4				
	A	Valor real	Valor redondeado	
	PT	3	1,9	2
	T	2	$\alpha 1$	0.21
	IS	1	$\beta 1$	0.44
	V		$\gamma 1$	0.35
			1,7	2
	Iac	2	$\alpha 2$	0.65
	Ilo	1	$\beta 2$	0.30
	Iro	1	$\gamma 2$	0.05
	G		2,1	2
	IRE	3	$\alpha 3$	0.57
	IRH	1	$\beta 3$	0.11
	IRA	1	$\gamma 3$	0.07
	IPS	1	ϕ	0.25
	Riesgo específico (r2)			8
	RIESGO ADMISIBLE			

Escenario 3				
		Valor real	Valor redondeado	
A		1,9	2	
PT	3	$\alpha 1$	0,21	
T	2	$\beta 1$	0,44	
IS	1	$\gamma 1$	0,35	
V		1,5	2	
Iac	2	$\alpha 2$	0,50	
Ilo	1	$\beta 2$	0,20	
Iro	1	$\gamma 2$	0,30	
G		2,1	2	
IRE	3	$\alpha 3$	0,57	
IRH	1	$\beta 3$	0,11	
IRA	1	$\gamma 3$	0,07	
IPS	1	ϕ	0,25	
Riesgo específico (r2)				8
RIESGO ADMISIBLE				

Escenario 5				
A	Valor real	Valor redondeado		
PT 3	2,1	2		
T 2	α_1	0,43		
IS 1	β_1	0,20		
V 1	γ_1	0,37		
Iac 2	1,6	2		
Ilo 1	α_2	0,62		
Iro 1	β_2	0,27		
G 1,9	γ_2	0,11		
IRE 3	α_3	2		
IRH 1	β_3	0,45		
IRA 1	γ_3	0,08		
IPS 1	ϕ	0,09		
Riesgo específico (r2)	1	0,38		
RIESGO ADMISIBLE				

Escenario 6				
	Valor real	Valor redondeado		
A	2,1	2		
PT 3	$\alpha 1$	0,43		
T 2	$\beta 1$	0,20		
IS 1	$\gamma 1$	0,37		
V	1,6	2		
Iac 2	$\alpha 2$	0,62		
Ilo 1	$\beta 2$	0,27		
Iro 1	$\gamma 2$	0,11		
G	2,2	2		
IRE 3	$\alpha 3$	0,60		
IRH 1	$\beta 3$	0,16		
IRA 1	$\gamma 3$	0,04		
IPS 1	ϕ	0,20		
Riesgo específico (r2)		8		
RIESGO ADMISIBLE				

Escenario 5				
	Valor real	Valor redondeado		
A	2,1	2		
PT 3	$\alpha 1$	0,43		
T 2	$\beta 1$	0,20		
IS 1	$\gamma 1$	0,37		
V	1,6	2		
Iac 2	$\alpha 2$	0,62		
Ilo 1	$\beta 2$	0,27		
Iro 1	$\gamma 2$	0,11		
G	1,9	2		
IRE 3	$\alpha 3$	0,45		
IRH 1	$\beta 3$	0,08		
IRA 1	$\gamma 3$	0,09		
IPS 1	ϕ	0,38		
Riesgo específico (r2)		8		
RIESGO ADMISIBLE				

AMENAZA 3. SABOTAJE

Categoría del riesgo	Puntuación	Acciones requeridas
Intolerable	r2 r6	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe actuar y en lo posible debe mitigarse.
Elevado	9-rs12	Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy grandes.
Admisible	6-rs9	Aceptable pero la amenaza debe ser evaluada periódicamente
Insignificante	r4	Aceptable

Escenario 2			
Valor real		Valor real	Valor redondeado
A	2,3	2,4	2,0
PT	3	α1	0,36
T	2	β1	0,40
IS	2	γ1	0,24
V	2,3	2,3	2
Iac	2	α2	0,34
Ilo	1	β2	0,18
Iro	3	γ2	0,48
G	1,8	1,8	2
IRE	3	α3	0,40
IRH	1	β3	0,22
IRA	1	γ3	0,14
IPS	1	φ	0,24
Riesgo específico (r3)		Riesgo ADMISIBLE	8

Escenario 4			
Valor real		Valor real	Valor redondeado
A	2,3	2,3	2
PT	3	α1	0,25
T	2	β1	0,43
IS	2	γ1	0,32
V	2,5	2,5	2
Iac	2	α2	0,27
Ilo	1	β2	0,13
Iro	3	γ2	0,60
G	1,8	1,8	2
IRE	3	α3	0,40
IRH	1	β3	0,22
IRA	1	γ3	0,14
IPS	1	φ	0,24
Riesgo específico (r3)		Riesgo ADMISIBLE	8

Escenario 6			
Valor real		Valor real	Valor redondeado
A	2,3	2,3	2
PT	3	α1	0,25
T	2	β1	0,43
IS	2	γ1	0,32
V	2,3	2,3	2
Iac	2	α2	0,34
Ilo	1	β2	0,18
Iro	3	γ2	0,48
G	2,0	2,0	2
IRE	3	α3	0,50
IRH	1	β3	0,13
IRA	1	γ3	0,16
IPS	1	φ	0,21
Riesgo específico (r3)		Riesgo ADMISIBLE	8

Escenario 1			
Valor real		Valor real	Valor redondeado
A	2,2	2,2	2
PT	3	α1	0,20
T	2	β1	0,46
IS	2	γ1	0,34
V	2,3	2,3	2
Iac	2	α2	0,34
Ilo	1	β2	0,18
Iro	3	γ2	0,48
G	1,8	1,8	2
IRE	3	α3	0,40
IRH	1	β3	0,22
IRA	1	γ3	0,14
IPS	1	φ	0,24
Riesgo específico (r3)		Riesgo ADMISIBLE	8

Escenario 3			
Valor real		Valor real	Valor redondeado
A	2,3	2,3	2
PT	3	α1	0,25
T	2	β1	0,43
IS	2	γ1	0,32
V	2,2	2,2	2
Iac	2	α2	0,38
Ilo	1	β2	0,22
Iro	3	γ2	0,40
G	1,8	1,8	2
IRE	3	α3	0,40
IRH	1	β3	0,22
IRA	1	γ3	0,14
IPS	1	φ	0,24
Riesgo específico (r3)		Riesgo ADMISIBLE	8

Escenario 5			
Valor real		Valor real	Valor redondeado
A	2,3	2,3	2
PT	3	α1	0,25
T	2	β1	0,43
IS	2	γ1	0,32
V	2,3	2,3	2
Iac	2	α2	0,34
Ilo	1	β2	0,18
Iro	3	γ2	0,48
G	1,7	1,7	2
IRE	3	α3	0,35
IRH	1	β3	0,27
IRA	1	γ3	0,03
IPS	1	φ	0,35
Riesgo específico (r3)		Riesgo ADMISIBLE	8

Amenaza 3. Sabotaje			
Valor real		Valor real	Valor redondeado
A	2,3	2,3	2
PT	3	α1	0,25
T	2	β1	0,43
IS	2	γ1	0,32
V	2,3	2,3	2
Iac	2	α2	0,34
Ilo	1	β2	0,18
Iro	3	γ2	0,48
G	1,8	1,8	2
IRE	3	α3	0,40
IRH	1	β3	0,22
IRA	1	γ3	0,14
IPS	1	φ	0,24
Riesgo específico (r3)		Riesgo ADMISIBLE	8

AMENAZA 4. ATAQUE CON EXPLOSIVOS

Categoría del riesgo			Puntuación		Acciones requeridas	
Intolerable			12-16		Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en la posible debe mitigarse	
Elevado			9-11		Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados	
Admisible			6-8		Aceptable pero la amenaza debe ser evaluada periódicamente	
Insignificante			1-5		Aceptable	

Escenario 2			Valor real		Valor redondeado	
A			2,5		3,0	
PT 3			α1		0,35	
T 3			β1		0,40	
IS 1			γ1		0,25	
V			2,7		3	
Iac 3			α2		0,45	
ILO 3			β2		0,24	
IRO 2			γ2		0,31	
G			2,3		2	
IRE 2			α3		0,22	
IRH 3			β3		0,40	
IRA 1			γ3		0,10	
IPS 2			φ		0,28	
Riesgo específico (r4)			RIESGO INTOLERABLE		18	

Escenario 4			Valor real		Valor redondeado	
A			2,5		3	
PT 3			α1		0,29	
T 3			β1		0,47	
IS 1			γ1		0,24	
V			2,7		3	
Iac 3			α2		0,55	
ILO 3			β2		0,18	
IRO 2			γ2		0,27	
G			2,3		2	
IRE 2			α3		0,22	
IRH 3			β3		0,40	
IRA 1			γ3		0,10	
IPS 2			φ		0,28	
Riesgo específico (r4)			RIESGO INTOLERABLE		18	

Escenario 6			Valor real		Valor redondeado	
A			2,5		3	
PT 3			α1		0,29	
T 3			β1		0,47	
IS 1			γ1		0,24	
V			2,7		3	
Iac 3			α2		0,45	
ILO 3			β2		0,24	
IRO 2			γ2		0,31	
G			2,2		2	
IRE 2			α3		0,26	
IRH 3			β3		0,36	
IRA 1			γ3		0,15	
IPS 2			φ		0,23	
Riesgo específico (r4)			RIESGO INTOLERABLE		18	

Escenario 1			Valor real		Valor redondeado	
A			2,7		3	
PT 3			α1		0,20	
T 3			β1		0,65	
IS 1			γ1		0,15	
V			2,7		3	
Iac 3			α2		0,45	
ILO 3			β2		0,24	
IRO 2			γ2		0,31	
G			2,3		2	
IRE 2			α3		0,22	
IRH 3			β3		0,40	
IRA 1			γ3		0,10	
IPS 2			φ		0,28	
Riesgo específico (r4)			RIESGO INTOLERABLE		18	

Escenario 3			Valor real		Valor redondeado	
A			2,5		3	
PT 3			α1		0,29	
T 3			β1		0,47	
IS 1			γ1		0,24	
V			2,7		3	
Iac 3			α2		0,39	
ILO 3			β2		0,27	
IRO 2			γ2		0,34	
G			2,3		2	
IRE 2			α3		0,22	
IRH 3			β3		0,40	
IRA 1			γ3		0,10	
IPS 2			φ		0,28	
Riesgo específico (r4)			RIESGO INTOLERABLE		18	

Escenario 5			Valor real		Valor redondeado	
A			2,5		3	
PT 3			α1		0,29	
T 3			β1		0,47	
IS 1			γ1		0,24	
V			2,7		3	
Iac 3			α2		0,45	
ILO 3			β2		0,24	
IRO 2			γ2		0,31	
G			2,4		2	
IRE 2			α3		0,17	
IRH 3			β3		0,48	
IRA 1			γ3		0,05	
IPS 2			φ		0,30	
Riesgo específico (r4)			RIESGO INTOLERABLE		18	

Amenaza 4. Ataque con explosivos			Valor real		Valor redondeado	
A			2,5		3	
PT 3			α1		0,29	
T 3			β1		0,47	
IS 1			γ1		0,24	
V			2,7		3	
Iac 3			α2		0,45	
ILO 3			β2		0,24	
IRO 2			γ2		0,31	
G			2,3		2	
IRE 2			α3		0,22	
IRH 3			β3		0,40	
IRA 1			γ3		0,10	
IPS 2			φ		0,28	
Riesgo específico (r4)			RIESGO INTOLERABLE		18	

AMENAZA 5. ATAQUE CON ARMAS QUÍMICAS

Categoría del riesgo	Puntuación	Acciones requeridas
Intolerable	r3 r6	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe evitar y en lo posible debe mitigarse.
Elevado	9 or r12	Solo se acepta si los esfuerzos para prevenir/mitigar el impacto son muy elevados.
Admisible	6 or r9	Aceptable pero la amenaza debe ser evaluada periódicamente.
Insignificante	r4	Aceptable

Escenario 2			
Valor real		Valor redondeado	
A	2,50	3,0	
PT	3	α1	0,35
T	3	β1	0,40
IS	1	γ1	0,25
V	1,8	2	
Iac	2	α2	0,43
Ilo	1	β2	0,25
IRo	2	γ2	0,32
G	2,5	2	
IRE	2	α3	0,14
IRH	3	β3	0,33
IRA	1	γ3	0,20
IPS	3	φ	0,33
Riesgo específico (r5)		RIESGO ELEVADO	
		12	

Escenario 1			
Valor real		Valor redondeado	
A	2,6	3	
PT	3	α1	0,25
T	3	β1	0,55
IS	1	γ1	0,20
V	1,8	2	
Iac	2	α2	0,43
Ilo	1	β2	0,25
IRo	2	γ2	0,32
G	2,5	2	
IRE	2	α3	0,14
IRH	3	β3	0,33
IRA	1	γ3	0,20
IPS	3	φ	0,33
Riesgo específico (r5)		RIESGO ELEVADO	
		12	

Amenaza 5. Ataque con armas químicas			
Valor real		Valor redondeado	
A	2,5	3	
PT	3	α1	0,30
T	3	β1	0,45
IS	1	γ1	0,25
V	1,8	2	
Iac	2	α2	0,43
Ilo	1	β2	0,25
IRo	2	γ2	0,32
G	2,5	2	
IRE	2	α3	0,14
IRH	3	β3	0,33
IRA	1	γ3	0,20
IPS	3	φ	0,33
Riesgo específico (r5)		RIESGO ELEVADO	
		12	

Escenario 4			
Valor real		Valor redondeado	
A	2,5	3	
PT	3	α1	0,30
T	3	β1	0,45
IS	1	γ1	0,25
V	1,7	2	
Iac	2	α2	0,40
Ilo	1	β2	0,30
IRo	2	γ2	0,30
G	2,5	2	
IRE	2	α3	0,14
IRH	3	β3	0,33
IRA	1	γ3	0,20
IPS	3	φ	0,33
Riesgo específico (r5)		RIESGO ELEVADO	
		12	

Escenario 3			
Valor real		Valor redondeado	
A	2,5	3	
PT	3	α1	0,30
T	3	β1	0,45
IS	1	γ1	0,25
V	1,9	2	
Iac	2	α2	0,50
Ilo	1	β2	0,12
IRo	2	γ2	0,38
G	2,5	2	
IRE	2	α3	0,14
IRH	3	β3	0,33
IRA	1	γ3	0,20
IPS	3	φ	0,33
Riesgo específico (r5)		RIESGO ELEVADO	
		12	

Escenario 5			
Valor real		Valor redondeado	
A	2,5	3	
PT	3	α1	0,30
T	3	β1	0,45
IS	1	γ1	0,25
V	1,8	2	
Iac	2	α2	0,43
Ilo	1	β2	0,25
IRo	2	γ2	0,32
G	2,48	2	
IRE	2	α3	0,12
IRH	3	β3	0,34
IRA	1	γ3	0,20
IPS	3	φ	0,34
Riesgo específico (r5)		RIESGO ELEVADO	
		12	

Escenario 6			
Valor real		Valor redondeado	
A	2,5	3	
PT	3	α1	0,30
T	3	β1	0,45
IS	1	γ1	0,25
V	1,8	2	
Iac	2	α2	0,43
Ilo	1	β2	0,25
IRo	2	γ2	0,32
G	2,3	2	
IRE	2	α3	0,22
IRH	3	β3	0,28
IRA	1	γ3	0,25
IPS	3	φ	0,25
Riesgo específico (r5)		RIESGO ELEVADO	
		12	

Escenario 5			
Valor real		Valor redondeado	
A	2,5	3	
PT	3	α1	0,30
T	3	β1	0,45
IS	1	γ1	0,25
V	1,8	2	
Iac	2	α2	0,43
Ilo	1	β2	0,25
IRo	2	γ2	0,32
G	2,48	2	
IRE	2	α3	0,12
IRH	3	β3	0,34
IRA	1	γ3	0,20
IPS	3	φ	0,34
Riesgo específico (r5)		RIESGO ELEVADO	
		12	

AMENAZA 6. CONFLICTOS LABORALES

Categoría del riesgo	Puntuación	Acciones requeridas
Intolerable	r2 16	Se corresponde con los casos en que el valor del riesgo no es aceptable, se debe actuar y en lo posible debe mitigarse.
Elevado	9-cr12	Se debe aceptar si los esfuerzos para prevenir/mitigar el impacto son muy elevados.
Admisible	6-cr9	Aceptable pero la amenaza debe ser evaluada periódicamente
Insignificante	r4	Aceptable

Escenario 2				
	Valor real	Valor redondeado		
A	1,9	2,0		
PT 3	α1	0,30		
T 2	β1	0,31		
IS 1	γ1	0,39		
V	2,4	2		
Iac 2	α2	0,20		
Ilo 1	β2	0,20		
Iro 3	γ2	0,60		
G	2,0	2		
IRE 3	α3	0,47		
IRH 1	β3	0,10		
IRA 2	γ3	0,08		
IPS 1	φ	0,35		
Riesgo específico (r4)		8	RESGO ADMISIBLE	

Escenario 1				
	Valor real	Valor redondeado		
A	1,7	2		
PT 3	α1	0,17		
T 2	β1	0,35		
IS 1	γ1	0,48		
V	2,4	2		
Iac 2	α2	0,20		
Ilo 1	β2	0,20		
Iro 3	γ2	0,60		
G	2,0	2		
IRE 3	α3	0,47		
IRH 1	β3	0,10		
IRA 2	γ3	0,08		
IPS 1	φ	0,35		
Riesgo específico (r4)		8	RESGO ADMISIBLE	

Amenaza 6. Conflictos laborales				
	Valor real	Valor redondeado		
A	1,8	2		
PT 3	α1	0,26		
T 2	β1	0,30		
IS 1	γ1	0,44		
V	2,4	2		
Iac 2	α2	0,20		
Ilo 1	β2	0,20		
Iro 3	γ2	0,60		
G	2,0	2		
IRE 3	α3	0,47		
IRH 1	β3	0,10		
IRA 2	γ3	0,08		
IPS 1	φ	0,35		
Riesgo específico (r6)		8	RESGO ADMISIBLE	

Escenario 4				
	Valor real	Valor redondeado		
A	1,8	2		
PT 3	α1	0,26		
T 2	β1	0,30		
IS 1	γ1	0,44		
V	2,3	2		
Iac 2	α2	0,25		
Ilo 1	β2	0,23		
Iro 3	γ2	0,52		
G	2,0	2		
IRE 3	α3	0,47		
IRH 1	β3	0,10		
IRA 2	γ3	0,08		
IPS 1	φ	0,35		
Riesgo específico (r4)		8	RESGO ADMISIBLE	

Escenario 3				
	Valor real	Valor redondeado		
A	1,8	2		
PT 3	α1	0,26		
T 2	β1	0,30		
IS 1	γ1	0,44		
V	2,45	2		
Iac 2	α2	0,17		
Ilo 1	β2	0,19		
Iro 3	γ2	0,64		
G	2,0	2		
IRE 3	α3	0,47		
IRH 1	β3	0,10		
IRA 2	γ3	0,08		
IPS 1	φ	0,35		
Riesgo específico (r4)		8	RESGO ADMISIBLE	

Amenaza 6. Conflictos laborales				
	Valor real	Valor redondeado		
A	1,8	2		
PT 3	α1	0,26		
T 2	β1	0,30		
IS 1	γ1	0,44		
V	2,4	2		
Iac 2	α2	0,20		
Ilo 1	β2	0,20		
Iro 3	γ2	0,60		
G	2,10	2		
IRE 3	α3	0,55		
IRH 1	β3	0,02		
IRA 2	γ3	0,00		
IPS 1	φ	0,43		
Riesgo específico (r4)		8	RESGO ADMISIBLE	

Escenario 6				
	Valor real	Valor redondeado		
A	1,8	2		
PT 3	α1	0,26		
T 2	β1	0,30		
IS 1	γ1	0,44		
V	2,4	2		
Iac 2	α2	0,20		
Ilo 1	β2	0,20		
Iro 3	γ2	0,60		
G	2,0	2		
IRE 3	α3	0,45		
IRH 1	β3	0,12		
IRA 2	γ3	0,10		
IPS 1	φ	0,33		
Riesgo específico (r4)		8	RESGO ADMISIBLE	

Escenario 5				
	Valor real	Valor redondeado		
A	1,8	2		
PT 3	α1	0,26		
T 2	β1	0,30		
IS 1	γ1	0,44		
V	2,4	2		
Iac 2	α2	0,20		
Ilo 1	β2	0,20		
Iro 3	γ2	0,60		
G	2,10	2		
IRE 3	α3	0,55		
IRH 1	β3	0,02		
IRA 2	γ3	0,00		
IPS 1	φ	0,43		
Riesgo específico (r4)		8	RESGO ADMISIBLE	

Amenaza 6. Conflictos laborales				
	Valor real	Valor redondeado		
A	1,8	2		
PT 3	α1	0,26		
T 2	β1	0,30		
IS 1	γ1	0,44		
V	2,4	2		
Iac 2	α2	0,20		
Ilo 1	β2	0,20		
Iro 3	γ2	0,60		
G	2,10	2		
IRE 3	α3	0,55		
IRH 1	β3	0,02		
IRA 2	γ3	0,00		
IPS 1	φ	0,43		
Riesgo específico (r4)		8	RESGO ADMISIBLE	

Capítulo 7

Conclusiones y Futuras Líneas de Investigación

7.CONCLUSIONES Y FUTURAS LÍNEAS DE INVESTIGACIÓN

7.1. Conclusiones

El objeto de la investigación aquí desarrollada es el desarrollo de una nueva propuesta metodológica de evaluación del riesgo en instalaciones portuarias, concretándose estos riesgos en aquellos que suponen una amenaza de destrucción de las instalaciones o una merma en la capacidad de operación portuaria, no habiéndose considerado riesgos muy específicos, como el riesgo cibernético o el contrabando que si bien supone un acto delictivo no suele implicar destrucción de las infraestructuras. En ambos casos no se produce destrucción de la infraestructura o detrimento de la capacidad operativa del puerto, al menos directamente.

Los puertos son, desde 2004, una infraestructura más segura debido a la implementación de sus Planes de Seguridad, diseñados para garantizar la operación portuaria y la seguridad de las infraestructuras y servicios que en ellos se ofrecen. Para ello la OMI-OIT desarrollo una metodología de evaluación previa de los riesgos que pueden darse en las instalaciones portuarias que se consideró adecuada si bien estas dos organizaciones dejan abierta la posibilidad de modificarlas en función de las particularidades de cada país.

En 2011 se desarrolla una Ley de Infraestructuras Críticas en España como resultado de una Directiva Europea que, como sucede de forma general en otros países como EUA, intenta proteger las principales infraestructuras de servicio del país ante nuevas amenazas globales como el terrorismo internacional, el crimen organizado, etc. Con esta premisa se considera interesante recoger aquellas metodologías que se desarrollan para la evaluación de cualquier tipo de infraestructura crítica, es decir, metodologías generalistas.

Se detecta así que existen varias metodologías de evaluación de riesgos y algunas específicas para instalaciones portuarias y que si bien algunas siguen un esquema de análisis del riesgo similar, otras en cambio se basan en modelización numérica o en análisis completamente teóricos y subjetivos, presentando consecuentemente notables diferencias entre sus alcances y formas de interpretación de los tres parámetros básicos; amenazas, vulnerabilidades y consecuencias.

En este sentido se considera que la investigación aquí desarrollada aporta varias mejoras al análisis que actualmente se realiza de las amenazas.

A continuación se presentan las principales conclusiones de la investigación

- A pesar de la implantación de planes de seguridad desde hace 10 años existen vulnerabilidades no consideradas adecuadamente, por ello su análisis necesita seguir ajustándose como se comprueba en el desarrollo de la investigación.
- Existen muchas interrelaciones entre situaciones de amenaza y vulnerabilidades del puerto que aún deben concretarse para poder así considerarlas en una evaluación del riesgo más ajustada cada vez a la realidad, huyendo así de situaciones de riesgo irreales y de reducido interés.
- En ocasiones la percepción de algunos riesgos por parte de los responsables de seguridad de las terminales, resulta diferente que la que manifiestan los responsables de la seguridad en los puertos.
- La disposición geográfica del puerto en la costa puede ser determinante ante la existencia de una amenaza, si bien este aspecto puede variar en el tiempo en un sentido o en otro. Para ello las medidas de prevención y mitigación serán muy importantes.
- Se comprueba que la probabilidad de amenaza es mayor en unas terminales que en otras en función del tipo de carga que estas muevan. No se pueden por tanto evaluar una misma amenaza de la misma manera en diferentes tipos de instalaciones.
- Del análisis estadístico se deduce que la probabilidad de suceso de diferentes amenazas varía notablemente de unas a otras, si bien esta puede modificarse en el tiempo.
- La clave para prevenir la mayoría de las amenazas es la accesibilidad al puerto, de ahí la importancia de mejorar su valoración ante estas, dado que las mayoría de las amenazas consideradas tienen su origen en una intrusión a las instalaciones portuarias.
- Para una adecuada evaluación de la accesibilidad es necesario definir tres factores; el tipo de cierre perimetral, los sistemas de control de acceso y la experiencia del equipo de seguridad.
- Se comprueba que la vulnerabilidad de una instalación se incrementa en parte cuando se dispone próxima a los accesos al puerto y/o a terminales de alto riesgo (terminales de GL, mercancías peligrosas, etc.).
- Las instalaciones o elementos a proteger tienen una relevancia para la operación, y la vulnerabilidad asociada a estos depende del tipo de instalación/elemento que se trate en relación a la amenaza que se evalúe.
- Se considera que la metodología para la evaluación del riesgo aquí formulada consigue sus objetivos, resultando ser además una metodología actual y

ajustada a la realidad diaria de un puerto, dado que recoge las opiniones de los responsables de seguridad del Sistema Portuario Español, estadísticas de seguridad (datos reales), que permiten determinar que situaciones se dan, con frecuencias y localizaciones mayoritarias, y por último aporta la opinión de expertos en la materia.

7.2. Futuras líneas de investigación

Entre las futuras líneas de investigación se incluyen las siguientes:

- La ampliación del estudio evaluando las amenazas derivadas de fallos en la seguridad del acceso al puerto a través del buque, que pudieran generar situaciones de riesgo para la instalación portuaria.
- Se debería seguir estudiando la posibilidad de incrementar los parámetros considerados para ajustar más los tres parámetros a resultados aún más precisos.
- La incorporación de la denominada “resiliencia” (capacidad de recuperación de la infraestructura afectada) a la propuesta metodológica con el fin de relativizar el resultado y hacerlo aún más realista.

Bibliografía

BIBLIOGRAFÍA

- Agarwal, J., & Blockley, D. I. (2007). Structural integrity: hazard, vulnerability and risk. *International Journal of Materials and Structural Integrity*, 1(1/2/3), 117. Retrieved from <http://www.inderscience.com/link.php?id=13867>
- Akintoye, A. S., & MacLeod, M. J. (1997). Risk analysis and management in construction. *International Journal of Project Management*, 15(1), 31–38. [https://doi.org/10.1016/S0263-7863\(96\)00035-X](https://doi.org/10.1016/S0263-7863(96)00035-X)
- Asamblea General de Naciones Unidas. (2011). Resolución A/57/292. Derechos humanos de los migrantes, 12193.
- Baker, A. B., Eagan, R. J., Falcone, P. K., Harris, J. M., Herrera, G. V, Hines, W. C., ... Wyss, G. D. (2002). *A Scalable Systems Approach for Critical Infrastructure Security*. Alburquerque. Retrieved from <http://www.doe.gov/bridge%0A>
- Bakir, N. O. (2007). *A brief analysis of threats and vulnerabilities in the maritime domain. Managing critical infrastructure risks*.
- Bichou, K. (2008). *Security and Risk-Based Models in Shipping and Ports: Review and Critical Analysis*. (OECD/ITF, Ed.). London.
- BOE núm. 102. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas. (2011). España: BOE núm. 102.
- Bonadonna, F. D. (2011). "Small Boats , Weak States , Dirty Money : Piracy and Maritime Terrorism in the Modern World ," Martin N . Murphy , (New York : Columbia University Press , 2009), 4(2), 133–134.
- Bush, B., Dauelsberg, L., LeClaire, R., Powell, D., DeLand, S., Samsa, M. (2005). Critical Infrastructure Protection Decision Support System (CIP/DSS) Project Overview. In Los Alamos National Laboratory (Ed.) (pp. 1–13). Boston.
- Cardona, O. D. (2001). *Estimación holística del riesgo sísmico utilizando sistemas dinámicos complejos*. Universidad Politécnica de Catalunya.
- Chalk, P. (2008). *The Maritime Dimension of International Security. Terrorism, Piracy, and Challenges for the United States (RAND CORPORATION)*.
- Consejo de Europa. Directiva 2008/114/CE del Consejo de Europa sobre la identificación y designación de infraestructuras críticas europeas., Diario Oficial de la Unión Europea 75–82 (2008). Retrieved from <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:ES:NOT>
- COUNTERACT. (2009). *COUNTERACT, Cluster Of User Networks in Transport and Energy Relating to Anti-terrorist ACTivities. Deliverable 4. CONSOLIDATED RESEARCH AND POLICY RECOMMENDATIONS* (EC Contract Number SSP4/2005/TREN/05/FP6/S07.48891). Brussels.
- Dirección de Seguridad y Supervisión Aeroportuaria. (2010). *PROCEDIMIENTO DE EVALUACION DE RIESGO DE LA SEGURIDAD DE LA AVIACION CIVIL PARA AEROPUERTOS*. Bogotá.

Dirección General de Protección Civil. (2010a). *GUIA TÉCNICA. Métodos cualitativos para el análisis de riesgos*. (Dirección General de Protección Civil, Ed.). Madrid.

Dirección General de Protección Civil. (2010b). *GUIA TECNICA Métodos cuantitativos para el análisis de riesgos*. (Dirección General de Protección Civil, Ed.). Madrid.

EURACOM. (2007). *EUropean Risk Assessment and Contingency planning Methodologies for interconnected networks. Deliverable D2.1. Common areas of Risk Assessment Methodologies*. Brussels.

European Commission. (2005). *GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION*. (European Commission, Ed.). Brussels.

Ezell, B. C. (2007). Infrastructure vulnerability assessment model (I-VAM). *Risk Analysis*, 27(3), 571–583. <https://doi.org/10.1111/j.1539-6924.2007.00907.x>

Federal Ministry of the Interior, Germany). Protection of Critical Infrastructures – Baseline Protection Concept (2008). Retrieved from www.bmi.bund.de

Fine, W. T. (1971). *Mathematical Evaluations for controlling hazards*. (NAVAL ORDNANCE LABORATORY, WHITE OAK, MARYLAND, Ed.). Maryland.

Fritzson, A., Ljungkvist, K., Boin, A., Rhinard, M. (2007). Protecting Europe ' s Critical Infrastructures: Problems and Prospects. *Journal of Contingencies and Crisis Management*, 15(1), 30–41.

Gómez, R. (2015). *A Methodology proposal to obtain operational parameter forecasts and operational risk assessment in container Terminals*. Universidad Politécnica de Madrid.

Greenberg, M. D., Chalk, P., Willis, H. H., Khilko, I., & Ortiz, D. S. (2006). *Maritime Terrorism - Risk and Liability*. <https://doi.org/MG-520-CTRMP>

Gronalt, M., Häuslmayer, H., Jammerneegg, W., Schindlbacher, E., & Weishäupl, M. (2005). A risk assessment approach for inland container terminals.

GUIAR. (2012). MÉTODOS GENERALIZADOS DE ANÁLISIS DE RIESGOS. Retrieved from http://www.unizar.es/guiar/1/Accident/An_riesgo/An_riesgo.htm

Hillson, D. (2002). Extending the risk process to manage opportunities. *International Journal of Project Management*, 20, 235–240.

Hsieh, C. (2014). Disaster risk assessment of ports based on the perspective of vulnerability. *Natural Hazards*, 74(2), 851–864. <https://doi.org/10.1007/s11069-014-1214-4>

Hunt, A. R., & Kellerman, K. F. (1998). Development of an analysis tool for performing civil aviation security risk assessment.

Ibáñez, I. (2006). *Bioterrorismo: la amenaza latente*. (CEU Ediciones, Ed.). Madrid: Instituto Universitario de Estudios Europeos. Universidad de San Pablo. CEU.

INTERNATIONAL MARITIME ORGANIZATION. (1997). *RESOLUTION A.871(20). GUIDELINES ON THE ALLOCATION OF RESPONSIBILITIES TO SEEK THE SUCCESSFUL RESOLUTION OF STOWAWAY CASES*.

INTERNATIONAL MARITIME ORGANIZATION. (1999). MSC/Circ.622/Rev.1 16. PIRACY AND ARMED ROBBERY AGAINST SHIPS. Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships.

INTERNATIONAL MARITIME ORGANIZATION. (2002a). MSC/Circ.623/Rev.3 29. PIRACY AND ARMED ROBBERY AGAINST SHIPS. Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships.

INTERNATIONAL MARITIME ORGANIZATION. (2002b). Resolution A.920(22). REVIEW OF SAFETY MEASURES AND PROCEDURES FOR THE TREATMENT OF PERSONS RESCUED AT SEA.

INTERNATIONAL MARITIME ORGANIZATION. (2002c). RESOLUTION A.922(22). CODE OF PRACTICE FOR THE INVESTIGATION OF THE CRIMES OF PIRACY AND ARMED ROBBERY AGAINST SHIPS, 2002(January).

INTERNATIONAL MARITIME ORGANIZATION. (2002d). *REVIEW OF MEASURES AND PROCEDURES TO PREVENT ACTS OF TERRORISM WHICH THREATEN THE SECURITY OF PASSENGERS AND CREWS AND THE SAFETY OF SHIPS* (Vol. 584).

ISO. (2009). ISO_Guide 73_2009(en), Risk management — Vocabulary.

ISO. UNE-ISO 31000:2009. Gestión del riesgo. Principios y directrices (2010). España: AENOR.

Kumar, S., & Verruso, J. (2008). Risk Assessment for the Security of Inbound Containers at U.S. Ports: A Failure, Mode, Effects, and Criticality Analysis Approach. *Transportation Journal*, 26–41.

Kumpulainen, S. (2006). Vulnerability concepts in hazard and risk assessment. *Special Paper of the Geological Survey of Finland*, (42), 65–74.

Levine, C. (2004). The concept of vulnerability in disaster research. *Journal of Traumatic Stress*, 17(5), 395–402. <https://doi.org/10.1023/B:JOTS.0000048952.81894.f3>

López, A. J. (2008). Estimación de frecuencia de eventos peligrosos. Retrieved from <http://www.monografias.com/trabajos15/frecuencia-riesgos/frecuencia-riesgos.shtml>

Mabrouki, C., Bellabdaoui, A., & Mousrij, A. (2013). Risk Analysis and Assessment by Multicriteria Approach Based in RO-RO Port Terminal . Case Study. *IJCSI International Journal of Computer Science Issues*, 10(3), 37–45.

Ministerio de Asuntos Exteriores y Cooperación de España. CÓDIGO INTERNACIONAL para la protección de los buques y de las instalaciones portuarias (Código PBIP) (2004). Madrid, España: BOE núm. 202.

Ministerio de la Presidencia de España. 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. (2007). España: BOE núm. 304.

Mitchell, C. L., Col, L. T., Augustine, S., & Leavenworth, F. (2007). *COUNTERING MARITIME TERRORISM IN THE CARIBBEAN SEA AND THE ATLANTIC OCEAN: IMPLICATIONS OF POSSIBLE MARITIME TERRORISM IN THE CARIBBEAN A*

thesis presented to the Faculty of the U . S . Army Command and General Staff College in partial fulfillment of the. University of the West Indies, St. Augustine.

Molina, R. (2014). *Caracterización de la agitación local y la respuesta oscilatoria de un buque mediante el uso de técnicas de visión artificial. Aplicación al análisis de los umbrales operativos en líneas de atraque y amarre*. Universidad Politécnica de Madrid.

Nelson, E. S. (2012). Maritime Terrorism and Piracy: Existing and Potential Threats. *Global Security Studies, Winter 2012, Volume 3, Issue 1, 3(1)*, 15–28.

Nicholls, R. J., Hoozemans, F. M. J., & Marchand, M. (1999). Increasing flood risk and wetland losses due to global sea-level rise: Regional and global analyses. *Global Environmental Change*, 9(SUPPL.). [https://doi.org/10.1016/S0959-3780\(99\)00019-9](https://doi.org/10.1016/S0959-3780(99)00019-9)

Organización Marítima Internacional. Solas. Edición Refundida 2002 (2002). Reino Unido: International Maritime Organization.

Organización Marítima Internacional, & Organización Internacional del Trabajo. (2003). Repertorio de recomendaciones prácticas sobre protección en los puertos.

Özcan, G. (2008). *A Generic Risk and Vulnerability Assessment Framework for International Construction Projects*. Middle East Technical University.

Papa, P. (2013). US and EU strategies for maritime transport security : A comparative perspective. *Transport Policy*, 28, 75–85. <https://doi.org/10.1016/j.tranpol.2012.08.008>

Parlamento Europeo, C. E. REGLAMENTO (CE) N° 725/2004 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 31 de marzo de 2004 relativo a la mejora de la protección de los buques y las instalaciones portuarias, Pub. L. No. L 129/6 (2004). European Community: Diario Oficial de la Unión Europea.

Project Management Institute (PMI). (2000). *A Guide to Project Management Body of Knowledge* (2000th ed.). Pennsylvania: Project Management Institute, Inc. Retrieved from www.pmi.org

RAND. (2009). *RAND_Database_of_Worldwide_Terrorism_Incidents*.

Sánchez, R., García, R., Manosalva, M. T., Rezende, S., & Sgu, M. (2004). *Protección marítima y portuaria en América del Sur*.

Sanchidrián, C. (2008). VIII CURSO DE TRANSPORTE MARÍTIMO Y GESTION PORTUARIA. La seguridad, el Código ISPS y la Legislación Comunitaria. In Universidad Politécnica de Madrid (Ed.). Madrid: Universidad Politécnica de Madrid.

Sarewitz, D., Pielke, R., & Keykhah, M. (2003). Vulnerability and risk: Some thoughts from a political and policy perspective. *Risk Analysis*, 23(4), 805–810. <https://doi.org/10.1111/1539-6924.00357>

Standards Australia/Standards New Zealand. Risk Management Guidelines Companion to AS/NZS 4360:2004. (Standards Australia/Standards New Zealand, Ed.) (2005). Australia & New Zealand.

Taylor, M. (2002). *Identifying Vulnerability*. Boston. Retrieved from www.aisc-corp.com

Turban, E.; Aronson, J.E. (2001). *Decision Support Systems and Intelligent Systems*. Editorial Prentice Hall Sexta Edición

U. S. Coast Guard. (2003). *NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 11-02. RECOMMENDED SECURITY GUIDELINES FOR FACILITIES*. (United States Coast Guard, Ed.). Washington, DC.

UIRR. (2007). *UIRR Risk Analysis. Guidelines for Combined Transport Terminals*. Brussels.

UNDRO. (1979). *Natural Disasters and Vulnerability Analysis*. Geneve. Retrieved from <http://archive.org/details/naturaldisasters00offi>

UNISDR. (2009). *Terminología sobre Reducción del Riesgo de Desastres*. Ginebra. Retrieved from www.unisdr.org/publications

Unnik, H. Van. (2011). Crimen Organizado en Puertos Europeos. Riesgos criminales y amenazas terroristas. In *Security in European Seaports*. Vigo.

USA Goverment. Uniting and Strengthening America By Providing Appropriate Tools Required (Usa Patriot Act) Act of 2001, Usa Patriot Act 1–132 (2001). USA.

US Department of Defense. (2006). *Risk management guide for DoD Acquisition*. Retrieved from http://www.dau.mil/publications/publicationsDocs/RMG_6Ed_Aug06.pdf

Utnea, I. B., Hokstad, P., Kjøllec, G., Vatna, J., Tøndeld, I. A., Bertelsene, D., Fridheim, H., Røstum, J. (2008). *Risk and Vulnerability Analysis of Critical Infrastructures -The DECRIS Approach*. Oslo.

Van de Voort, M., Willis, H., Ortiz, D., & Martonosi, S. (2007). CHAPTER 5. Applying risk assessment to secure the containerized supply chain. In Springer Netherlands (Ed.), *Managing Critical Infrastructure Risks* (pp. 79–95). Springer Netherlands.

Velásquez, C. A., Cardona, O. D., Mora, M. G., Yamin, L. E., Vela, C. A., Carreño, M. L., & Barbat, A. H. (2014). Hybrid loss exceedance curve (HLEC) for disaster risk assessment. *Natural Hazards*, 72(2), 455–479. <https://doi.org/10.1007/s11069-013-1017-z>

Vesely, W. E., Goldberg, F. F., Roberts, N. H., & Haasl, D. F. (1981). *Fault Tree Handbook*. (U.S. Nuclear Regulatory Commission, Ed.). Washington D.C.

Victoria Department of Transport (Australia). (2012). *Security Risk Assessment for Transport Operators*. Melbourne: State of Victoria. Retrieved from www.transport.vic.gov.au

Vilko, J. P. P., & Hallikas, J. M. (2012). Risk assessment in multimodal supply chains. *International Journal of Production Economics*, 140(2), 586–595. <https://doi.org/10.1016/j.ijpe.2011.09.010>

Yang, Z. L., Wang, J., Bonsall, S., & Fang, Q. G. (2009). Use of fuzzy evidential reasoning in maritime security assessment. *Risk Analysis*, 29(1), 95–120. <https://doi.org/10.1111/j.1539-6924.2008.01158.x>

Yang, Z., Ng, A. K. Y., & Wang, J. (2014). A new risk quantification approach in port facility security assessment. *Transportation Research Part A*, 59, 72–90. <https://doi.org/10.1016/j.tra.2013.10.025>

Yeo, G., Pak, J., & Yang, Z. (2013). Analysis of dynamic effects on seaports adopting port security policy. *Transportation Research Part A*, 49, 285–301. <https://doi.org/10.1016/j.tra.2013.01.039>

Zhang, Y., Siu, J., & Lam, L. (2015). Estimating the economic losses of port disruption due to extreme wind events. *Ocean and Coastal Management*, 116, 300–310. <https://doi.org/10.1016/j.ocecoaman.2015.08.009>

Zhang, Y., Siu, J., & Lam, L. (2016). Estimating economic losses of industry clusters due to port disruptions. *Transportation Research Part A*, 91, 17–33. <https://doi.org/10.1016/j.tra.2016.05.017>

Anexo 1

Metodologías Consideradas

1. Metodologías consideradas	1
1.1. Aeronáutica Civil (Colombia)	1
1.2. BMI. Protection of Critical Infrastructures (Alemania)	6
1.3. CARVER (Criticality, Accessibility, Recoverability, Vulnerability, Effect on Population, Recognizability). Ejército de los EUA.....	18
1.4. CIP/DSS (Critical Infrastructure Protection Decision Support System).....	21
1.5. Cluster of User Networks in Transport and Energy Relating to Anti-terrorist Activities (COUNTERACT)	27
1.6. DECRIS. SINTEF (Noruega)	41
1.7. Directrices para terminales de transporte combinado. Union of Combined Road-rail transport companies (UIRR)	44
1.8. European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks (EURACOM)	54
1.9. FAA. Federal Aviation Administration (EUA)	62
1.10. RAM. Risk Assessment Methodology (Sandia National Laboratories, 2003)	65
1.11. RBDM. Navigation and Vessel Inspection. Servicio de Guarda Costas de EUA, 2003	70
1.12. SECUREPORT. Puertos del Estado, 2004.....	78
1.13. Terminales de Contenedores Interiores (Austria), 2008.	92
1.14. TRAM. Organización Internacional del Trabajo (OIT) y Organización Marítima Internacional (OMI), 2003.....	95

ÍNDICE DE FIGURAS

Figura 1. Las cinco fases de la gestión del riesgo y la crisis. Fuente: BMI	8
Figura 2. Arquitectura del CIP/DSS. Fuente: CIP/DSS.....	24
Figura 3. Matriz de interdependencia de subsectores para modelos urbanos en el prototipo CIP / DSS	26
Figura 4. Ejemplo de gráfico de valoración de amenazas en FFCC. COUNTERACT	33
Figura 5. Ejemplo de matriz de evaluación. COUNTERACT.	34
Figura 6. Matriz de indicadores del riesgo. COUNTERACT	37
Figura 7. Riesgo por niveles en función de la localización. COUNTERACT	38
Figura 8. Riesgo por niveles en función del tipo de ataque. COUNTERACT	38
Figura 9. Matriz de evaluación de la vulnerabilidad. UIRR.....	53
Figura 10. Tabla de valoración del riesgo (UIRR).....	54
Figura 11. Los siete pasos de la metodología EURACOM.....	56
Figura 12. Análisis metodológico. RAM.....	66
Figura 13. Parte superior de un árbol de fallos genéricos de las instalaciones. RAM ...	67
Figura 14. Diseño y esquema del proceso de evaluación. RAM.....	69
Figura 15. Diagrama de flujo de RBDM	71
Figura 16. Matrices de criterio de evaluación. SECUREPORT.....	92

ÍNDICE DE TABLAS

Tabla 1. Clasificación de la probabilidad. Aeronáutica Civil.....	4
Tabla 2. Definiciones de Efectos. Aeronáutica Civil	5
Tabla 3. Probabilidad de suceso. Aeronáutica Civil.....	5
Tabla 4. Probabilidad de suceso. Herramienta de Evaluación. Aeronáutica Civil.....	6
Tabla 5. Niveles de riesgo y escala. Aeronáutica Civil	6
Tabla 6. Escala de medida de la Probabilidad de ocurrencia. COUNTERACT.....	30
Tabla 7. Escala de medida del Impacto/gravedad. COUNTERACT	31
Tabla 8. Categorías del Riesgo. COUNTERACT	32
Tabla 9. Acciones requeridas. COUNTERACT	32
Tabla 10. Ejemplos de aspectos clave a considerar. COUNTERACT	36
Tabla 11. Evaluación de la vulnerabilidad. COUNTERACT	40
Tabla 12. Clasificación de sensibilidad en caso de que el riesgo adicional consiste en un ataque a la Terminal se considere como un objetivo en sí mismo. UIRR	47
Tabla 13. Clasificación de sensibilidad caso de que el riesgo adicional consiste en el robo de sustancias peligrosas. UIRR	48
Tabla 14. Definición de zonas (UIRR)	49
Tabla 15. Escala de peligrosidad (UIRR)	50
Tabla 16. Nivel de peligrosidad (UIRR).....	50
Tabla 17. Ejemplo de escala de riesgos obtenida. UIRR.....	52
Tabla 18. Valoración del riesgo. FAA.....	64
Tabla 19. Categoría de las consecuencias y valores asociados. RAM	67
Tabla 20. Categoría de las consecuencias y valores asociados. RAM	70
Tabla 21. Listado de escenarios posibles. RBDM	72
Tabla 22. Niveles de Consecuencia. RBDM	73
Tabla 23. Puntuación de vulnerabilidad. RBDM.....	74
Tabla 24. Matriz de Vulnerabilidad y Consecuencia. RBDM	76

Tabla 25. Esquema para determinación de escenarios que requieren medidas correctoras.
RBDM 77

Tabla 26. Valoración de SMR MAX y RMR MAX. SECUREPORT..... 85

Tabla 27. Valoración de SLR MAX y RLR MAX. SECUREPORT 85

Tabla 28. Índice Redundancia de elementos. Escala de valoración de la incidencia. SECUREPORT
..... 88

Tabla 29. Índice plazo de Recuperabilidad. Escala de valoración de la incidencia. SECUREPORT
..... 88

Tabla 30. Estructura de las Consecuencias. RAM..... 93

Tabla 31. Evaluación del equipamiento. RAM 94

Tabla 32. Matriz de amenaza y riesgo. TRAM 96

1. Metodologías consideradas

Se describen a continuación las metodologías seleccionadas para la investigación, detallándose sus procesos, criterios y forma de expresar el resultado de la evaluación del riesgo para cada una de ellas.

1.1. Aeronáutica Civil (Colombia)

La metodología del análisis de riesgo seguida en los aeropuertos colombianos consta de seis etapas que se identifican como:

1. Identificar los peligros
2. Evaluar los riesgos
3. Analizar las medidas de control
4. Tomar decisiones de control
5. Implementar el control de riesgos
6. Supervisar y evaluar

Las amenazas que serán evaluadas bajo el esquema de análisis de riesgo son:

- Apoderamiento de Aeronave
- Secuestro
- Terrorismo
- Narcotráfico
- Contrabando
- Polizón
- Tráfico de Personas
- Robo

Se entiende por riesgo: la representación que describe la eventual ocurrencia de situaciones, condiciones o eventos capaces de generar perjuicio al desarrollo de una actividad o al cumplimiento de su propósito. El riesgo existe como una potencialidad (futuro), y se describe mediante la ecuación:

$$\text{Riesgo} = \text{Probabilidad} \times \text{Ocurrencia}$$

1.1.1. Identificar los peligros

Para ello se deberán seguir los pasos descritos a continuación:

Analizar la capacidad instalada

Por cada amenaza se debe identificar el peligro, teniendo en cuenta:

- Infraestructura del Aeropuerto (Cerramiento, Puertas de Acceso)
- Sistema de Control de Acceso
- Iluminación, Comunicaciones
- Número de personal operativo AVSEC
- Esquemas de coordinación con otras fuerzas no permanentes en el Aeropuerto
- Capacitación y Sensibilización en Seguridad Aeroportuaria

Buscar patrones o conductas tiempo pasado

- Revisar estadísticas de actos de interferencia ilícita del Aeropuerto en los dos últimos años
- Analizar la situación socioeconómica de la Región, amenazas puntuales en el tiempo.

Averiguar con el personal operativo que es importante

Consultar con los diferentes actores del Aeropuerto (Tw, Sanidad, Bomberos, Personal Administrativo), su percepción de la seguridad aeroportuaria, clasificándola en niveles alto, medio o bajo

Buscar fuentes de información

Para identificar peligros:

- Referencias a nivel global, informes de inteligencia organismos de seguridad del estado Análisis con la Policía Nacional, Ejército Nacional, Armada Nacional, DAS, DIAN de la información suministrada sobre las condiciones de seguridad de la región.
- Técnicas tradicionales (auditorias, inspecciones, reportes, entrevistas)
- Personal operativo
- Lecciones aprendidas de eventos afrontados (base de datos, estadísticas y archivos)

Herramientas para identificación de peligros

- Diagramas lógicos (aspectos positivos y negativos de la seguridad en el aeropuerto)
- ¿Qué pasa si sucede un evento?, ¿Cómo se reacciona?

- Análisis de cambio (alternativas para mitigar los peligros)
- Simulación y prognosis (previsión con base en la simulación de ocurrencia de algún suceso)
- Análisis de causa-efecto
- Ensayos y simulacros tiempo real
- Análisis operacional

Resumiendo, ¿cómo se identifican los peligros?:

- Registros históricos (amenazas puntuales, situación socioeconómica de la región, informes de inteligencia)
- Experiencias
- Análisis (debilidades de administración AVSEC, vulnerabilidad infraestructura)
- Efectivo sistema de información (Reportes)

1.1.1.1.1. Evaluar los riesgos

Es medir el impacto de cada peligro en términos de pérdida potencial y costos, basados en la matriz de **probabilidad y severidad** (efecto) de acuerdo al grado de exposición.

Probabilidad

Se define como la posibilidad de que se presenten en un evento y se califica como.

Tabla 1. Clasificación de la probabilidad. Aeronáutica Civil

No.	PROBABILIDAD	DEFINICIÓN
1	FRECUENTE (A)	<u>Ocorre frecuentemente</u> durante la misión o en el servicio, se espera que ocurra prolongadamente durante el periodo de tiempo de servicio o la misión. Siempre ocurre.
2	PROBABLE (B)	<u>Ocorre varias veces</u> durante la misión o en el servicio, se espera a que ocurra en periodos específicos en el cumplimiento de la misión o en el servicio.
3	OCASIONAL (C)	<u>Ocorre alguna vez</u> durante el desarrollo de la misión o en el servicio, puede ser esporádico e irregular. Poco común en la misión o servicio.
4	NO FRECUENTE (D)	<u>Posible que ocurra en la vida</u> , se puede presentar en la misión o en el servicio, pero con una posibilidad muy remota. No espere que se le presente en la misión o servicio. Hechos aislados usualmente no ocurre
5	POCO PROBABLE (E)	<u>Se puede asumir que no ocurrirá en la vida</u> : Su ocurrencia no es imposible pero se puede asumir que casi nunca ocurrirá durante una misión específica o en el servicio.

Fuente: Aeronáutica Civil (Colombia)

Severidad o efecto

Se define como el impacto que se puede presentar si sucede un evento.

Tabla 2. Definiciones de Efectos. Aeronáutica Civil

No.	EFEECTO	DEFINICIÓN
1	CATASTRÓFICO (I)	No se completa la misión con éxito: muerte, pérdida de equipo, lesión permanente, daño colateral. Nos lleva a un ACCIDENTE .
2	CRITICO (II)	Significativamente se degrada la misión: lesión permanente o parcial, superior a 3 meses, daño al equipo sustancial, daño colateral significativo. Suceso RELES .
3	MODERADO (III)	Degrada la misión en un menor grado: con lesiones menores pero se presenta daño del equipo o sistema. Suceso RECIL/EVOT .
4	INSIGNIFICANTE (III)	Poco impacto en la misión: el equipo o sistema no presenta daño, no hay daños colaterales. No hay lesiones, pero la novedad es de interés para la Prevención. NOPER

Fuente: Aeronáutica Civil (Colombia)

1.1.1.1.2. Resultados de la evaluación

Al construir el análisis del riesgo, se obtiene una tabla como la siguiente:

Tabla 3. Probabilidad de suceso. Aeronáutica Civil

			PROBABILIDAD				
			Frecuente	Probable	Ocasional	No frecuente	Poco Probable
			A	B	C	D	E
E F E C T O	Catastrófico	I	1	2	6	8	12
	Critico	II	3	4	7	11	15
	Moderado	III	5	9	10	14	16
	Insignificante	IV	13	17	18	19	20

Fuente: Aeronáutica Civil (Colombia)

Y su grafica se representa así:

Tabla 4. Probabilidad de suceso. Herramienta de Evaluación. Aeronáutica Civil

			HERRAMIENTA DE EVALUACIÓN				
			PROBABILIDAD				
			Frecuente	Probable	Ocasional	No frecuente	Poco Probable
			A	B	C	D	E
E F E C T O	Catastrófico	I	Extremadamente				
	Critico	II	Alto	Alto			Bajo
	Moderado	III		Medio			
	Insignificante	IV					

Fuente: Aeronáutica Civil (Colombia)

Su valoración se presenta en la siguiente tabla:

Tabla 5. Niveles de riesgo y escala. Aeronáutica Civil

NIVEL DE RIESGO	ESCALA
EXTREMADAMENTE ALTO	1,2,3
ALTO	4,5,6,7,8
MEDIO	9,10,11,12,13
BAJO	14.15.16.17.18.19.20

Fuente: Aeronáutica Civil (Colombia)

Posteriormente se procedería a la analizar las medidas de control, implementar las medidas y evaluar finalmente su validez.

1.2. BMI. Protection of Critical Infrastructures (Alemania)

El objetivo de la metodología es reducir la vulnerabilidad de las infraestructuras críticas ante acontecimientos naturales y accidentes así como ataques terroristas y actos delictivos. En este contexto la metodología se concentra en la edificación, los aspectos organizativos y medidas de protección personales y técnicas. A fin de definir medidas

aplicables y factibles, se requiere conseguir un acuerdo básico del nivel de protección deseable y aceptable.

La estrategia para la gestión del riesgo y la crisis se constituye un proceso sistemático y se compone de cinco años fases que representan el alcance necesario del riesgo basado en procesos y la gestión de la crisis en una empresa privada o una autoridad gubernamental.

Las cinco fases son las siguientes: 1. Planificación preliminar para establecer un sistema de riesgos y gestión de crisis; 2. Análisis de riesgos; 3. Especificación de las medidas preventivas; 4. Implementación de un sistema de gestión de crisis; y 5. evaluación periódica de las fases 1 a 4.

1.2.1.Fase 1. Planificación preliminar

Una planificación preliminar a fondo crea las condiciones necesarias para establecer con éxito la gestión de riesgos y de crisis en una empresa privada o una autoridad gubernamental.

Antes de comenzar con el análisis algunas cuestiones fundamentales deben ser aclaradas, tales como el liderazgo de la organización, en particular como los líderes de la organización establecen la gestión de riesgos y de crisis; la aceptación del proceso; definición de las responsabilidades; disponibilidad de recursos y la definición de los objetivos de protección estratégicos.

Figura 1. Las cinco fases de la gestión del riesgo y la crisis. Fuente: BMI

La planificación se organiza así:

1. Establecimiento de la gestión del riesgo y la crisis
2. División de responsabilidades
3. Recursos
4. Aclaración de las obligaciones legales

5. Formulación de objetivos de protección estratégicos
6. Comunicación de los riesgos

1.2.2.Fase 2. Análisis de riesgos

Un análisis de riesgos estructura y objetiviza la información recopilada sobre las amenazas y riesgos. Aquí, los riesgos se refieren a procesos y sus componentes individuales. El análisis de riesgos estudia diferentes procesos y sus componentes y compara los diferentes riesgos para la organización. Esta comparación permite determinar la urgencia y la prioridad de las medidas que pueden tener una influencia significativa en el riesgo. De esta manera, el análisis de riesgos proporciona la base para la gestión limitada financiera y de personal recursos eficaz y eficiente

Comienza dividiendo la organización en procesos y sub-procesos. La propia organización decide el grado en que los sub-procesos se subdividen; por ejemplo, si una sala de control se identifica como parte de un proceso, se puede definir como un sub-proceso. También es posible dividir la misma sala de control en otros subprocesos. Cuantos más niveles de subprocesos haya, más esfuerzo requerirá el análisis de riesgos; sin embargo, también tendrá mayor valor informativo.

Componentes de sub-procesos son aquellos elementos que contribuyen a la función de un proceso. Estos elementos se denominan "Elementos de riesgo" en la metodología. Son individuos físicos o elementos virtuales que pueden ser perjudicados o dañados, con un impacto en el sub-proceso en cuestión.

Se consideran los siguientes elementos de riesgo:

Las personas (personal y otros en las instalaciones)

Es esencial para proteger a todo el mundo suficientemente en las instalaciones contra las amenazas o para llevarlos a un lugar seguro en caso de peligro inminente. Para ello, todas las organizaciones deben tomar precauciones para proporcionar la mejor protección posible para quienes estén en la zona, sobre todo antes de que la policía, bomberos y el personal de servicio emergencia lleguen en caso de emergencia y después de que se vayan.

El personal, en particular personal especializado, es un elemento de riesgo en el sentido de conservar funcionalidad de sub-procesos.

Superficies

Esto incluye todas las áreas al aire libre, incluyendo carreteras, almacenamiento y áreas de estacionamiento, espacios verdes y áreas esenciales para las operaciones.

Edificios

Estos incluyen todas las estructuras sobre y bajo tierra, como como naves de producción, almacenes y edificios administrativos así como aparcamientos.

Instalaciones y equipos

Instalaciones y equipos de sub-procesos se pueden encontrar en todas las áreas de una organización, en particular en lo siguiente:

- Suministro de electricidad,
- Suministro de gas natural,
- Calefacción urbana,
- Suministro de agua,
- La tecnología de la información (IT),
- La tecnología de las comunicaciones y
- Transporte (incluyendo vehículos y suministro de combustible).

Instalaciones específicas de la organización y equipos especiales

Esto incluye todas las instalaciones y equipos especializados.

Datos y archivos

Incluyen toda la información guardada en formato electrónico y en formato papel para mantener los sub-procesos en la organización.

El siguiente enfoque sistemático resulta importante para el desarrollo del concepto de protección:

- I. El establecimiento de categorías de peligro, diferenciadas según las áreas de catástrofes, incidentes resultantes de fallos técnicos o errores humanos, terrorismo o actos delictivos,
- II. Basado en lo anterior, definición de los respectivos niveles de protección,
- III. El desarrollo de escenarios de daños y amenazas,
- IV. El análisis de puntos débiles,
- V. La formulación de objetivos de protección como base para la definición de medidas de protección y medidas preventivas,
- VI. Definición del alcance requerido de la acción (coordinación entre medidas del sector privado y público),
- VII. Realización del alcance requerido definido de acción y
- VIII. Revisiones regulares de este análisis y proceso de planificación con los objetivos de gestión de calidad.

Los aspectos que considera la metodología son:

- **Evaluación de riesgos general** (situación de seguridad general, tamaño y composición del personal, calidad del equipo de seguridad, posiciones sociales de miembros de la dirección de la compañía, naturaleza de relaciones de distribución y actividades en el extranjero, criminalidad establecida hasta la fecha, etc).
- **Ubicación geográfica del área operacional y las instalaciones** (vulnerabilidad desde fuera y desde dentro, distancia desde el cierre de la zona de trabajo, visibilidad desde fuera, vías de tráfico interno y externo, proximidad a áreas industriales o infraestructuras críticas, aspectos geológicos [p. ej. riesgo de terremotos] y aspectos geográficos [p. ej. proximidad de ríos, topografía]).
- **Importancia de las instalaciones en los procesos de producción y servicios** (p. ej. daño económico, producción y déficits de entrega).
- **Carácter Simbólico de la empresa y/o instalaciones** (tipo de producción y almacenaje de materiales, gama de productos, importancia estratégica / económica de la compañía).
- **Interdependencias**, es decir interacción con otras infraestructuras.
- **Tipo, tipología y relaciones cooperativas** de las estructuras de gestión del riesgo implementadas por el operador.
- **Naturaleza estructural de la cooperación entre las instalaciones públicas y los operadores**, relativas a la planificación de las emergencias, la gestión de las crisis y en términos de prevención técnica.

Riesgos y áreas en peligro

Los riesgos a los que se enfrentan los operadores de infraestructuras críticas pueden dividirse en riesgos relacionados con catástrofes naturales, riesgos que relacionados con errores humanos o problemas técnicos y riesgos que se relacionan con terrorismo o actos delictivos. En esta conexión hay que notar que una instalación entera o las partes críticas de la seguridad de una instalación también se pueden afectar por los acontecimientos fuera de la instalación actual, en áreas operacionales vecinas o instalaciones de tráfico a las cuales un potencial de amenaza especial se aplica (reacción en cadena). Los posibles impactos a este respecto incluyen la extensión de incendios a instalaciones vecinas, el fallo de las provisiones después de acontecimientos catastróficos fuera de la instalación, etc. Acontecimientos que ocurren dentro en un corto plazo de tiempo entre uno y otro, como una segunda explosión, retardada o varios incidentes que ocurren al mismo tiempo en ubicaciones diferentes, también puede implicar un efecto exponencial previniendo medidas de reparación o rescate o provocando que los recursos se concentren en el lugar equivocado, por ejemplo (medidas de distracción).

Factores de riesgo

La descripción siguiente pretende ilustrar la complejidad y la heterogeneidad de los factores de riesgo que requieren ser considerados:

Factor de riesgo: errores técnicos y humanos

- Incendio
- Vertido de sustancias peligrosas
- Explosiones
- Accidentes de tráfico o industriales
- Accidentes aéreos

Factor de riesgo: terrorismo y actos criminales

- Mal función deliberada
- Manipulación
- Accidentes con vehículos
- Interferencias usando herramientas sencillas
- Interferencias usando herramientas pesadas
- Incendios provocados
- Uso de explosivos
- Colocación de bombas
- Impactos de aviones
- Efectos combinados
- Despliegue de armas biológicas

Factor de riesgo: organización

- Concentración de recursos vitales
- Externalización de infraestructuras que son críticas para la compañía

Factor de riesgo: naturaleza/ambiente

- Catástrofes:
 - Huracanes
 - Tsunamis
 - Terremotos
 - Movimientos de masas; avalanchas, deshielos...

- Epidemias

Factor de riesgo: comunicaciones

- Complejidad de sistemas
- Incremento de la dependencias de las comunicaciones
- Amplio red a nivel mundial de sistemas IT
- Ciclos cortos de innovación en IT
- Estandarización de tecnología y componentes
- Gestión de redes/interdependencias de infraestructuras críticas
- Internet como sistema del nervio de las infraestructuras críticas (conexión con la seguridad de comunicaciones)

Zonas de riesgo en las empresas

Las infraestructuras críticas, así como la producción individual o áreas de servicio dentro de una instalación, están sujetas a diferentes niveles de riesgo ante eventos naturales, errores humanos, fallos técnicos, terrorismo o actos delictivos. A nivel empresarial, los riesgos adicionales pueden surgir como resultado del recorte de empleos, la centralización y automatización de los procesos de control y seguimiento, los cambios en áreas de responsabilidad resultantes de la externalización o la inadecuada aplicación de las medidas necesarias, como resultado del incremento de costos. Así se identifican diferentes zonas de riesgo para los diferentes tipos de riesgos considerados

Análisis de la Criticidad

El análisis de la criticidad permite a una organización identificar qué procesos, a parte de todos los mencionados, tendrían consecuencias de gran alcance para la organización si fueran interrumpidos. Se deben tomar las medidas adecuadas para proteger suficientemente dichos procesos críticos. La identificación de los riesgos y, sobre todo, las medidas preventivas elegidas para reducir el riesgo deben concentrarse inicialmente en los elementos de riesgo de los subprocesos de los procesos críticos.

Se pueden utilizar los siguientes criterios para identificar procesos críticos:

Vida y salud

Si el proceso se interrumpe, ¿cuál será el impacto sobre la vida humana y la salud?

Periodo de tiempo

Si el proceso se interrumpe, ¿cuánto tiempo tarda en producirse un impacto en el producto / servicio general de la organización? Cuanto más corto es el tiempo, más crítico es el proceso.

Magnitud

¿Qué parte del producto / servicio en general se verá afectado si este proceso se interrumpe o se detiene por completo?

Contractual, reglamentario o legal relevancia

Si el proceso se interrumpe, ¿qué consecuencias contractuales, reglamentarias o consecuencias jurídicas tendrán para la organización?

Daños económicos

Si el proceso se interrumpe, ¿Cuál es el daño financiero a la organización?

El análisis de criticidad resulta en la identificación de todos los procesos críticos de una organización y que representan a los sub-procesos que operan en ellos, así como sus elementos de riesgo.

Identificación de riesgos

Los riesgos de una organización están determinados por las amenazas que se derivan en su ubicación y que pueden tener un impacto en sus elementos de riesgo, así como por la vulnerabilidad de estos elementos de riesgo. La combinación de la información pertinente sobre las amenazas y la vulnerabilidad en la identificación del riesgo de los elementos de que se trate y, cuando estén agregados, a los sub-procesos en cuestión. Los riesgos para los elementos se llaman sub-riesgos; riesgos agregados a los sub-procesos se denominan riesgos generales.

Análisis de amenazas y desarrollo de escenarios

Reconocer y documentar todas las amenazas relevantes es crucial para un análisis de riesgos con éxito. El primer paso en el análisis de amenazas y escenarios de desarrollo, por lo tanto debe ser la elaboración de una lista de las amenazas que puedan surgir en la ubicación de la organización. Esta lista completa debe describir la naturaleza general de las amenazas, su intensidad, duración y posibles efectos. Basándose en una lista específica de sitios de amenazas es posible desarrollar escenarios que contienen información adicional necesaria para el análisis de riesgos y gestión de crisis. Estos escenarios deben representar incidentes realistas que podrían resultar en crisis.

El responsable de seguridad debe determinar el número de escenarios que se incluirán en el análisis de riesgos. El objetivo es cubrir todas las posibles amenazas.

La siguiente información se recopila para cada escenario:

- **Exposición anticipada**

¿Qué sub-procesos y elementos de riesgo podrían ser afectados?

- **Intensidad anticipada**

¿Cómo será de fuerte el impacto en un subproceso y en sus elementos de riesgo?

- **Duración prevista**

¿Cuánto tiempo podría durar el incidente?

- **Previo aviso**

¿Cuánto tiempo se puede esperar entre el previo aviso y el incidente?

- **Efectos secundarios**

¿Qué efectos se derivarán de las dependencias del proceso?

¿Qué efectos psicológicos podría producir el incidente?

¿Qué tipo de impacto público o en los medios de comunicación podría tener el incidente?

- **Incidentes de referencia**

¿Qué incidentes comparables podrían ser examinados como información adicional?

- **Probabilidad de ocurrencia**

¿Qué posibilidades hay de que el incidente puede estimarse o identificarse?

A menudo, la probabilidad de un escenario con una determinada intensidad, escala y duración geográfica, el previo aviso y los efectos secundarios sólo pueden ser estimados. Por ejemplo, los registros históricos útiles para el cálculo de la probabilidad de un incidente se han mantenido sólo para ciertos eventos naturales o fallos de estructuras creadas por el hombre. En el desarrollo de escenarios, es aconsejable estimar la probabilidad de ocurrencia utilizando un sistema de clasificación.

Los escenarios seleccionados deben ser revisados, actualizados y añadidos a regularmente. Otros escenarios pertinentes pueden ser añadidos según sea necesario con el fin de identificar todos los riesgos posibles a la organización.

Análisis de vulnerabilidad

Junto con las posibles amenazas, la vulnerabilidad de los subprocesos y elementos de riesgo es decisiva para determinar cómo la organización se ve afectada y el daño que se produce. Cuanto más vulnerables subprocesos individuales y elementos de riesgo haya, mayor es el impacto de las amenazas en el producto o servicios de la organización.

Se emplea un catálogo de criterios para identificar la vulnerabilidad de subprocesos y elementos de riesgo individuales. La vulnerabilidad de cada elemento de riesgo en un

subproceso se estima utilizando el catálogo de criterios. Esto también se puede hacer usando un sistema de clasificación.

Se puede emplear la siguiente lista de criterios o añadir otros:

- Dependencia de los elementos de riesgo
- Dependencia de infraestructuras externas
- Dependencia de infraestructuras internas
- Robustez
- Nivel actual de protección
- Redundancia; sustitutos
- Esfuerzo restaurador
- Adaptabilidad
- Capacidad de amortiguación
- Dependencia de condiciones ambientales específicas

Cálculo del riesgo

Dentro del análisis del riesgo, los valores calculados, las estimaciones o los resultados de los escenarios y el análisis de vulnerabilidad están vinculados con los valores del riesgo o los resultados. Los valores de riesgo están unidos por medio de una función. Se entienden los sub-riesgos como una función de probabilidad de que el escenario en el cuestión se produzca y de la vulnerabilidad del elemento de riesgo.

El riesgo general de un sub-proceso es entonces el agregado de sub-riesgos para los elementos de riesgo en el subproceso

En principio los riesgos se pueden calcular de tres maneras diferentes:

- Cálculo cualitativo: Este método proporciona estimaciones aproximadas de los riesgos descritos en forma de texto, sin producir comparabilidad numérica.
- Cálculo semicuantitativo: Este método utiliza un sistema de clasificación para estimar los valores para los factores de riesgo individuales para que puedan ser comparadas en forma numérica.
- Cálculo cuantitativo: Este método calcula los factores de riesgo matemáticamente, por ejemplo mediante el uso de análisis de series de tiempo en el caso de probabilidad de ocurrencia, o el uso de modelos de simulación para identificar los impactos en una organización.

La elección del método depende de la cantidad de esfuerzo puede y debe ser gastado, y en lo que se dispone de información

Los valores de riesgo descritos calculados de esta manera pueden ser comparados entre sí. Dicha comparación es especialmente útil en el caso de análisis cualitativos y semi-cuantitativos, porque los valores y descripciones resultantes son cantidades no absolutas. Sin embargo, los resultados de los análisis cualitativos y semi-cuantitativos pueden ser muy valiosos en su relación mutua, es decir en una comparación interna.

El objetivo de esta comparación es identificar aquellos elementos de riesgo y sub-procesos que enfrentan los mayores riesgos.

La evaluación de riesgos debe indicar si los objetivos de la protección inicialmente definidos tienen pueden alcanzarse para los riesgos existentes.

Si hay demasiados sub-altos riesgos, los objetivos de protección operacionales deben ser formulados para servir de punto de partida para la adopción de medidas preventivas.

1.2.3.Fase 3. Medidas y estrategias preventivas

Las medidas de prevención ayudan a reducir los riesgos para los procesos críticos. Estos ayudan a lograr objetivos de protección operacionales y así elevar el umbral para posibles crisis en la organización. Esto puede reducir el número y / o la intensidad de los incidentes de crisis.

Las medidas preventivas deben ser objeto de un análisis de coste-beneficio destinado a reducir el riesgo global. Esto se hace mediante la comparación de los gastos potenciales y los costes directos e indirectos derivados de la organización de un incidente extremo. La combinación de los resultados de un análisis de riesgos con los de un análisis de coste-beneficio conduce a la selección de las medidas que son especialmente eficaces en el marco del presupuesto existente.

Sin embargo, las medidas para reducir los riesgos poco probables, pero que tendrían impactos dramáticos si ocurrieran, a menudo son imposibles de justificar basándose solo en el riesgo y el análisis de coste-beneficio. En tales casos, puede ser útil tener en cuenta los aspectos sociales y éticos, así como las condiciones del marco legal al decidir sobre las medidas de protección.

Las estrategias preventivas se aprovechan de las herramientas de prevención de riesgos, el desplazamiento de riesgos y aceptación del riesgo.

1.2.4.Gestión de la Crisis

Una crisis se define como una desviación de la situación normal que no puede ser manejada usando procedimientos normales de funcionamiento. Las crisis en las organizaciones de infraestructura crítica pueden tener graves consecuencias para el

funcionamiento de las empresas y las autoridades del gobierno y por lo tanto dar lugar a daños para el público o para la interrupción del sistema político, social o económico.

La ley de Comercio utiliza el término "amenaza a la existencia", lo cual es muy útil para definir la crisis. Las crisis pueden tener su origen dentro de la propia organización, por ejemplo, las crisis financieras como resultado de la mala gestión o el fraude. Los disparadores externos para las crisis incluyen caídas de los mercados de valores, la cobertura negativa de los medios o dificultades de abastecimiento. Otros factores desencadenantes de las crisis en las infraestructuras críticas incluyen desastres naturales, fallos técnicos, errores humanos, actos intencionales de un terrorista o naturaleza criminal, y los conflictos armados.

1.3. CARVER (Criticality, Accessibility, Recoverability, Vulnerability, Effect on Population, Recognizability). Ejército de los EUA

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.

CARVER define seis factores para la evaluación en cada sitio o punto dentro de una instalación, valora estos seis factores en una escala de 1 (bajo) a 10 (más alto) y proporciona una lista ordenada de los puntos fuertes y débiles. Los elementos específicos de análisis CARVER son:

1.3.1. Criticidad

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

1.3.2. Accesibilidad

La accesibilidad es la facilidad con que un objetivo puede ser 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 / atacante no siempre se correlaciona con la accesibilidad de un objetivo.

1.3.3. Recuperación del funcionamiento y la propiedad

La recuperabilidad es una medida del tiempo requerido para reemplazar, reparar o evitar la destrucción o el daño infligido al objetivo, y varía en función de las fuentes y la antigüedad de los componentes seleccionados, y con piezas de repuesto o capacidades redundantes.

1.3.4. Vulnerabilidad

La 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 ataque tenga éxito. La vulnerabilidad depende de:

- I. La naturaleza y construcción del objetivo,
- II. La cantidad de daño necesario / deseado;
- III. Los activos disponibles:
 - a) Mano de Obra, experiencia y mentalidad;

- b) Transporte, armas, explosivos y equipos

1.3.5.Efecto sobre la población

El 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.

1.3.6.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 del ataque terrorista: 5
- Nivel alto de trascendencia del ataque terrorista: 4
- Nivel considerable de trascendencia del ataque terrorista: 3
- Nivel general de trascendencia del ataque terrorista: 2
- Nivel bajo de trascendencia del ataque terrorista: 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 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:

- I. Caracterización del sistema
- II. Identificación y valoración de la amenaza
- III. Identificación y valoración de la vulnerabilidad
- IV. Determinación de los parámetros de control
- V. Establecimiento de probabilidades
- VI. Análisis de impacto
- VII. Determinación de riesgos
- VIII. Recomendaciones para controles de seguridad
- IX. Documentación de los resultados y elevación del pertinente informe a la organización competente.

1.4. CIP/DSS (Critical Infrastructure Protection Decision Support System)

El Programa de Protección de Infraestructuras Críticas (CIP), patrocinado por el Departamento de Seguridad Nacional de los EE.UU (DHS) tiene tres objetivos principales:

1. Desarrollar, implementar y elaborar un enfoque racional para dar prioridad a las estrategias del CIP y para las asignaciones de recursos utilizando el modelado, simulación y análisis para evaluar las vulnerabilidades, las consecuencias y los riesgos.
2. Proponer y evaluar la protección, mitigación, respuesta y estrategias de recuperación y opciones, y
3. Proporcionar apoyo en tiempo real a los tomadores de decisiones en situaciones de crisis y emergencias.

Se emplea un modelo de dinámica de sistemas, simulación y análisis para llevar a cabo evaluaciones de las consecuencias y los análisis de riesgo (basándose en amenazas reales, vulnerabilidades de la infraestructura para las amenazas dadas, resultando así las consecuencias). Estas metodologías permitirán a los tomadores de decisiones priorizar e invertir los escasos recursos y poner en práctica estrategias racionales para la protección de los diversos sistemas e infraestructuras basadas en un modelado, simulación y análisis dinámico y objetivo.

El sistema de protección de infraestructuras críticas (CIP/DSS) ha desarrollado un sistema de soporte de decisiones riesgo conocido que proporciona información para la toma de decisiones en la protección de infraestructuras críticas, considerando diecisiete tipos de infraestructuras críticas y sus interdependencias primarias. El proyecto CIP/DSS completó un modelo prototipo y dos estudios de caso en febrero de 2004.

Las infraestructuras críticas consideradas son:

1. Agricultura y la Alimentación
2. Agua
3. Salud Pública
4. Servicios de Emergencia
5. Gobierno
6. Defensa Base Industrial
7. Información y Telecomunicaciones
8. Energía
9. Transporte
10. Banca y Finanzas
11. Industria Química y Peligrosos Materiales
12. Correos y Envío

Categorías de activos clave

- 13. Monumentos Nacionales e Iconos
- 14. Centrales Nucleares
- 15. Presas
- 16. Instalaciones de Gobierno
- 17. Activos comerciales clave

1.4.1.Arquitectura

El sistema de soporte de decisiones incluye modelos de consecuencia para todas las infraestructuras críticas que están vinculados a través de sus interdependencias fuertes y acoplados entre lo nacional y las escalas metropolitanas (ver Figura 2). La representación exacta de las interdependencias entre infraestructuras comprende la característica más singular de los modelos CIP/DSS: el sistema puede realizar un seguimiento de la propagación de una perturbación en el sector de las telecomunicaciones, por ejemplo, en los sectores de energía, banca y gubernamental. Por otra parte, respetando los aspectos nacionales y urbanos que difieren de la mayoría de las infraestructuras la CIP / DSS permite resolver tanto los efectos inter-regional e inter-urbanos: algunos incidentes, por ejemplo, podría incluir cualquiera de los efectos localizados o grandes impactos nacionales. Las salidas de los modelos de consecuencia son capturadas en una base de datos, consecuencia de la cual se calculan las medidas ajustadas a los perfiles de las personas que toman las decisiones. Las funciones de utilidad multiatributo se determinan a partir de entrevistas con los tomadores de decisiones y se utilizan para comparar estrategias alternativas de protección de la infraestructura y para ayudar a construir un consenso entre las partes interesadas en la decisión.

Figura 2. Arquitectura del CIP/DSS. Fuente: CIP/DSS

Las consecuencias de los modelos nacionales y urbanos se implementan utilizando el programa "Vensim" que lee los parámetros de entrada y escribe series de tiempo de salida a una base de datos relacional Oracle de medidas de la "consecuencia", que están separados en un conjunto mucho más pequeño de medidas de "decisión". El software de soporte de decisiones (en Visual Basic) accede a la base de datos de decisiones para calcular valores de utilidad para varios escenarios y alternativas.

Los modelos de consecuencia simulan la dinámica de infraestructuras individuales y pares de infraestructuras separadas entre sí de acuerdo a sus interdependencias. Por ejemplo, la reparación de daños en la red de energía eléctrica en una ciudad requiere transporte a los sitios de reparación y entrega de piezas, combustible para vehículos de reparación, las telecomunicaciones para el diagnóstico de problemas y la coordinación de las reparaciones, y la disponibilidad de mano de obra. La reparación en sí implica un diagnóstico, un pedido de piezas, envío de equipos humanos, y realizar las reparaciones. La red de energía eléctrica responde al daño inicial y para la realización de las reparaciones con los cambios en su capacidad operativa (el número de megavatios que se puede distribuir a los clientes). Procesos dinámicos como estos están representados en las simulaciones CIP/DSS para cada sector de infraestructura mediante ecuaciones diferenciales, eventos discretos y reglas codificadas de operación.

Cada sector de infraestructura crítica se divide en un número de "subsectores", que tienen un carácter más uniforme y para el que se separan resultados en vistas separadas. Por ejemplo, el sector de los servicios de emergencia se divide en

servicios (i) de fuego, (ii) los servicios médicos de emergencia, (iii) policía y (iv) servicios de apoyo de emergencia. Se utiliza un modelo Vensim "enlazador" hecho a medida para montar un modelo unificado multisectorial a partir de archivos individuales que contienen cada uno un único modelo de sector: el enlazador identifica "variables opuestas" presentes en modelos con dependencias en otros sectores y resuelve las referencias cuando se combinan los modelos. Esto permite el desarrollo y prueba de los modelos a nivel de sector y realiza el análisis a nivel multisectorial.

El modelo actual urbano de CIP/DSS tiene cerca de 4.500 las variables que incluyen un centenar de interdependencias entre subsectores. El modelo nacional tiene un tamaño y complejidad similares.

1.4.2. Soporte de decisión

El equipo CIP/DSS llevó a cabo una serie de entrevistas con los responsables y actores de decisión del CIP con el fin de identificar los requisitos para el sistema de apoyo a la toma de decisiones y cuantificar la priorización de las consecuencias. La clasificación de las medidas de decisión derivada de esta investigación resulta en seis categorías: (i) en sectores específicos, (ii) problemas de salud y seguridad pública y ocupacional, lesiones no mortales, enfermedades, (iii) los costes económicos inmediatos e interdependientes de evento, incluyendo la implementación y coste de operación para las medidas opcionales, (iv) el aire y las emisiones de agua, el suelo no productivo, y la pérdida de valor intrínseco, (v) riesgos socio-políticos, la confianza del público, la confianza en los efectos específicos de cada sector del gobierno, y la confianza del mercado, y (vi) la seguridad nacional de la continuidad de los servicios críticos gubernamentales civiles y militares. Las preferencias de tres tomadores de decisiones representativas fueron codificadas utilizando técnicas de entrevista estructuradas para llegar a funciones de utilidad multi-atributo de consonantes con la salida de los modelos de consecuencia y aplicables a los casos de estudio se describen a continuación.

Figura 3. Matriz de interdependencia de subsectores para modelos urbanos en el prototipo CIP / DSS.

Fuente: CIP/DSS

Los subsectores de infraestructura crítica representadas como columnas tienen una o más dependencias funcionales en el subsector representados como filas. Las abreviaturas del subsector son:

A = Agricultura; Bin = Seguros; Bsp = gasto; Cha = materiales peligrosos; E = Servicios de Emergencia; Efi = Servicios de Bomberos; Eme = Servicios Médicos de Emergencia; Epo = Aplicación de la ley; Servicios Esu = Apoyo de Emergencia; Fpr = Procesamiento de Alimentos; Monitoreo Gmo = Gobierno; Ibc = Broadcast; Llamadas Ica = telefónicas; Ida = Redes de datos; Ire Reparación = Telecomunicaciones; Ite = Telecomunicaciones; MKA = Activos clave; Operaciones = postales; P = Salud Pública; Pcl = Clínicas; Pho = Hospitales; PMO = mortuorios; Pps = Farmacéutica de suministro; S = Escenario; T = Transporte; Cucharadas = autobús; Tro = Camino; Tsw = metro; Ula = Trabajo; Upo = Población; W = agua; Wpo = Agua Potable; Xel = Electricidad; XNG = Gas Natural; Xpo = Petróleo, Petróleo y Lubricantes.

El bloque de construcción principal para el análisis de decisiones en la CIP / DSS se denomina “caso”. Un caso consta de dos o más pares de escenarios; cada par de escenario se compone de un escenario disposición y un escenario incidente:

- Base Escenario Par
 - Escenario base de preparación: Asunto como condiciones habituales; consecuencias en ausencia de eventos terroristas u otras interrupciones.

- Escenario base de Incidentes: los eventos propuestos ocurren sin opcional adicional de medidas implementadas, más allá de lo que existe en el momento.
- Uno o más pares de escenarios alternativos
 - Escenario de preparación alternativo: Un conjunto específico de medidas opcionales adicionales en lugar; evento postulado no se inicia.
 - Escenario de incidentes alternativo: las medidas opcionales están en el lugar; ocurre el evento propuesto.

Comparación de los pares de escenarios alternativos con pares escenario base indica que los efectos de diversas inversiones y estrategias, etiquetados aquí como medidas opcionales (que incluyen hardware, procesos y estrategias relacionadas con la prevención, protección, mitigación, respuesta y recuperación), podrían tener si fueran implementados por los tomadores de decisiones. Cada escenario requiere una simulación por separado durante un período de tiempo (definido por el caso) con los modelos nacionales y urbanos detallados.

1.4.3. Categorías de incidentes estudiadas

Los casos considerados para su estudio son:

- Ataque biológico
- Ataque químico
- Ataque radiológico
- Ataque nuclear
- Ataque con explosivos
- Asalto físico
- Infiltración de personas
- Cyber ataque
- Desastres
- Accidentes

1.5. Cluster of User Networks in Transport and Energy Relating to Anti-terrorist Activities (COUNTERACT)

El proyecto COUNTERACT se desarrolló entre 2006 y 2009 y fue diseñado para proporcionar las herramientas para ayudar a las organizaciones de transporte público

a prepararse ante la amenaza terrorista. Se identificó como una prioridad clave proporcionar pautas para la realización de la evaluación de riesgos. Debido al alcance del proyecto, las directrices se centran en las amenazas terroristas utiliza una determinada intención humana para evaluar los riesgos, basándose en el daño (efecto) y la disponibilidad (vulnerabilidad / amenaza). Sin embargo, se puede adaptar fácilmente a otros delitos (por ejemplo, los asaltos contra conductores o pasajeros) o incluso amenazas proporcionadas por eventos naturales.

Los sistemas de transporte público son objetivos fáciles para el terrorismo y los delitos graves, porque:

- sus sistemas abiertos facilitan fácil acceso y salida rápida;
- el anonimato apoya la preparación desapercibida e impide su descubrimiento; y especialmente,
- el alto número de personas que se reúnen en ambientes cerrados y restringidos los hace particularmente vulnerables y ofrece el máximo potencial de víctimas.

Esta metodología es una herramienta para las operaciones de transporte público para llevar a cabo las evaluaciones de riesgos en relación con las amenazas de seguridad, es decir, el terrorismo y otros delitos graves. Esta ayudará a las personas a cargo de la seguridad: en la sensibilización, así como en el arranque, organización y a llevar a cabo el procedimiento. Finalmente, con los resultados de la evaluación del riesgo a mano, y con el estudio *COUNTERACT PT5 (Public Transport Security Planning-Organisation, Countermeasures & Operations Guidance)* se pueden desarrollar contramedidas eficaces, justificadas e implementadas.

Por razones prácticas, la metodología aquí descrita se basa principalmente en aspectos cualitativos más que en datos cuantitativos. En consecuencia, la evaluación no es un proceso puramente objetivo, así las consideraciones normativas influyen en los resultados. La evaluación se lleva a cabo utilizando un método de índice, es decir, un nivel de probabilidad de ocurrencia y se determina el impacto. La metodología tiene muchas ventajas:

- Se puede aplicar a la mayoría de los tipos de organizaciones;
- No requiere que los usuarios tengan un conocimiento previo de la evaluación de riesgos;
- Facilita y apoya el intercambio de ideas y evaluación de procesos colectivos de expertos de diversos orígenes;
- Permite la inclusión de todos los diferentes tipos de amenazas;
- Permite la inclusión de todas las fases de la gestión de riesgos, es decir, la prevención, mitigación y rehabilitación.

1.5.1. Amenazas potenciales

A continuación se da una lista incompleta de amenazas potenciales:

- Artefactos explosivos improvisados (IED), utilizando materiales como explosivos militares o comerciales, por ejemplo, minas o explosivos improvisados;
- Armas de Asalto, armas a distancia y uso de explosivos estándar (granadas de mano, granadas propulsadas por cohetes, disparo);
- Bombas suicida;
- Vehículos dirigidos IED, vehículos bombas;
- Incendio provocado y artefacto incendiario improvisado (por ejemplo, cócteles molotov);
- Secuestro;
- Sabotaje;
- Armas de destrucción masiva: química / biológica / radiológico / nuclear (CBRN-E).
- Etc.

Dos factores determinan el riesgo de un ataque:

- Probabilidad de ocurrencia;
- Impacto / gravedad del suceso.

La combinación de los dos componentes, probabilidad de ocurrencia y resultados del ataque, permite al usuario identificar riesgos con facilidad y mostrar estos riesgos con mayor claridad.

La probabilidad de ocurrencia es la posibilidad de una amenaza de ser llevada a cabo, y se mide en una escala de categorías. A continuación se muestra un ejemplo válido de escala de categorías, si bien las definiciones siguientes pueden ser modificadas con el fin de adaptar la evaluación de riesgos para una operación específica.

Tabla 6. Escala de medida de la Probabilidad de ocurrencia. COUNTERACT

Probabilidad de ocurrencia	Criterios de definición (derivado de Euro Norm 50126)
Muy alta	La amenaza puede ser ejecutada en cualquier momento y / o se ha ejecutado dentro de la organización repetidamente.
Alta	Se tiene que tener en cuenta la amenaza que se ejecuta repetidamente. La amenaza se ha producido dentro de la propia organización una vez.
Posible	La ejecución de la amenaza se tiene que tener en cuenta. La amenaza ha sido ejecutada repetidamente dentro de otras operaciones d en todo el mundo, o al menos una vez dentro de una operación en el país propio/vecino.
Baja	La amenaza se ejecuta en raras ocasiones, pero se ha ejecutado en casos aislados en otras organizaciones (a nivel mundial).
Muy improbable	Una ejecución de la amenaza es muy poco probable, y la amenaza nunca se ha ejecutado en otras operaciones antes.

Fuente: COUNTERACT

Impacto/gravedad significa el daño a un activo derivado de la ejecución de una amenaza, que se mide en la escala de categorías (que deben definirse).

El Impacto/gravedad de las amenazas está clasificado en cuatro categorías.

Tabla 7. Escala de medida del Impacto/gravedad. COUNTERACT

Impacto/gravedad	Criterios de definición	
	(derivado de Euro Norm 50126)	
	Consecuencias para Personas y/o Propiedades/Medio Ambiente	Consecuencias para el Operador y Servicios
Desastrosas	Varias muertes (a definir por el Operador) y / o numerosas lesiones graves y / o daños más graves a la propiedad y/o el medio ambiente.	Pérdida de las funciones y/u operaciones vitales durante un largo período de tiempo (a definir por el Operador).
Criticas	Bajo número de muertes (a definir por el Operador) y/o lesiones graves y/o graves daños a la propiedad (a definir por el Operador) y/o el medio ambiente	Pérdida de las funciones y/u operaciones vitales durante un corto período de tiempo
Marginales	Pérdidas mínimas y/o daño notable a la propiedad y/o el medio ambiente.	Impacto leve en las funciones y/u operaciones.
No criticas	Posibilidad de pocas bajas y / o pequeños daños a la propiedad y/o el medio ambiente	Sin impacto en las funciones y / u operaciones

Fuente: COUNTERACT

La combinación de la probabilidad de ocurrencia y el impacto/gravedad da como resultado las categorías de "riesgo". Para diferenciar el riesgo con mayor precisión dentro de las cuatro categorías de riesgo, las cinco categorías de "probabilidad de ocurrencia", así como las cuatro categorías para "Impacto/gravedad" pueden ser atribuidas a una escala de números. Las cifras resultantes permiten una clasificación más precisa de los diferentes riesgos, incluso dentro de dichas categorías.

Las categorías "de riesgo" también pueden ser ilustradas por colores. Esto hace que el resultado final sea muy claro:

Tabla 8. Categorías del Riesgo. COUNTERACT

Probabilidad de ocurrencia	Categorías del Riesgo			
Muy alta (5)	Tolerable (5)	Peligroso (10)	Intolerable (15)	Intolerable (20)
Alta (4)	Tolerable (4)	Peligroso (8)	Peligroso (12)	Intolerable (16)
Posible (3)	Insignificante (3)	Tolerable (6)	Peligroso (9)	Peligroso (12)
Baja (2)	Insignificante (2)	Tolerable (4)	Tolerable (6)	Peligroso (8)
Muy improbable(1)	Insignificante (1)	Insignificante (2)	Negligible (3)	Tolerable (4)
	No crítico (1)	Marginal(2)	Crítico (3)	Desastroso (4)
	Impacto / Gravedad			

Fuente: COUNTERACT

Las categorías de riesgo están vinculadas con las contramedidas, como se muestra en la siguiente tabla:

Tabla 9. Acciones requeridas. COUNTERACT

Categoría del riesgo	Puntuación	Acciones Requeridas
Intolerable	15-20	Se debe evitar o el impacto debe ser mitigado en la medida de lo posible
Peligroso	8-12	Sólo se aceptará si los esfuerzos para la prevención y/o mitigación de impacto es irrazonablemente alta
Tolerable	4-6	Aceptable pero la amenaza debe ser evaluada regularmente
Insignificante	1-3	Aceptable

Fuente: COUNTERACT

1.5.2. Evaluación del riesgo

Sería útil comenzar con una sesión de lluvia de ideas para recoger el primer aporte de expertos internos y externos. Este “input” debe ser incorporado en una estructura visualizable que represente todo el sistema. El siguiente gráfico es parte de un ejemplo de sistema ferroviario. Un dibujo similar debería hacerse para todos los subsistemas ferroviarios, es decir, pesado, metro, tren ligero / tranvía, autobús, y otros, por ejemplo ferry.

Figura 4. Ejemplo de gráfico de valoración de amenazas en FFCC. COUNTERACT

Fuente: COUNTERACT

Esta visualización puede apoyar la discusión y evaluación en los talleres posteriores para la evaluación de riesgos cualitativa. En cualquier caso, la estructura completa final debe estar incluida en la matriz siguiente, y que se explica a continuación.

Como primer paso, se recomienda discutir aspectos generales en una sesión de lluvia de ideas con expertos internos y externos (abogados/policía) de diversos campos:

- ¿Cómo son de graves las amenazas para su propia red?
- ¿Cuán atractiva es la ciudad/región para los terroristas en comparación con las demás?
- ¿Cuán atractivo es el sistema de transporte público para los terroristas en comparación con otros objetivos potenciales de la ciudad/región?
- ¿Qué elementos del sistema son los más atractivos para los terroristas?
- ¿Qué partes de la red son más críticas para la operación?

Matrix for qualitative Assessment (Metro)				Treat									
				Atomic Bomb	Dirty Bomb	Biological Weapon	Chemical Weapon	Arson Attack	Bomb Threat	ED	Car Bomb	Rocket-Propelled Grenade	Sniper Attack
Station	Target												
	Location A	Specification	Specification										
	Location B	Specification	Specification										
	Location C	Specification	Specification										
	Location D	Specification	Specification										
	Location E	Specification	Specification										
	Location F	Specification	Specification	Specular									
			Specification	Specular									
	Location G	Specification	Specification	Specular									
	Location H	Specification	Specification	Specular									
		Specification	Specification	Specular									
			Specification	Specular									

Figura 5. Ejemplo de matriz de evaluación. COUNTERACT.

Fuente: COUNTERACT

Aspectos relevantes a investigar que pueden aumentar el "atractivo" de las partes del sistema como un objetivo para ataques

- El número de pasajeros en intercambiadores/estaciones/paradas, vehículos (en horas punta)
- Los nodos e intersecciones/papel y la importancia de la red
- Características distintivas geográficas y geológicas que podrían facilitar ataques o impedir los esfuerzos de respuesta y por lo tanto aumentar el impacto potencial, por ejemplo,
 - Ubicación en punto bajo (por ejemplo, donde los vehículos se pueden observar y atacar con facilidad desde un terreno más elevado)
 - Lugares con zonas profundas / empinadas
 - Túneles profundos
 - Elevaciones
 - Grandes estructuras inferiores
 - Ubicaciones remotas donde sería difícil una respuesta
- Carácter simbólico
 - De una parte del sistema o
 - De los edificios adyacentes

- Vista general de la estación/infraestructura que podría producir imágenes "fuertes" en la cobertura de los medios de comunicación después de un ataque
- Eventos especiales/grandes organizados en las inmediaciones (adyacente o donde el transporte público lleva a los visitantes) que podrían aumentar temporalmente el nivel de riesgo
- Fechas especiales (conmemoraciones)
- Obras de construcción temporales
- Instituciones/Organizaciones cercanas que generan un grupo de pasajeros, lo cual es un riesgo especial (por ejemplo, grupos políticos o religiosos)
- Manejo de efectivo.
- ¿Existe un historial de ataques? ¿Ha habido ataques en el pasado?
- Las áreas con fácil acceso de vehículos a las zonas sensibles a corta distancia, por ejemplo, estaciones y activos críticos

Aspectos clave para estructurar todo el sistema de transporte público en una sistemática operativa:

- ¿Cuáles son las diferentes partes del sistema?
 - Tren
 - Metro
 - Tren ligero / tranvía
 - Autobús
 - Otros, por ejemplo, Ferry
- ¿Qué infraestructura de apoyo y gente hay en el sistema?

A continuación se dan algunos ejemplos, bien no se trata de una lista completa.

Tabla 10. Ejemplos de aspectos clave a considerar. COUNTERACT

Infraestructura operacional con acceso público	
	Intercambiadores <ul style="list-style-type: none"> ▪ Elevados ▪ A nivel ▪ Subterráneos
	Estaciones <ul style="list-style-type: none"> ▪ Elevadas ▪ A nivel ▪ Subterráneas
	Vías/carreteras <ul style="list-style-type: none"> ▪ Elevadas ▪ A nivel ▪ Ubicaciones en puntos bajos ▪ Subterráneas
Infraestructura operacional y equipamiento de acceso restringido	
	Acondicionado y ventilación <ul style="list-style-type: none"> ▪ Estaciones ▪ Vehículos
	Head office Cash centres
	Centro de Control de Tráfico
	Centro de Control de Seguridad (diferente al anterior)
	Salas técnicas y operacionales del sistema
	Salas vacías y sin uso del sistema

Fuente: COUNTERACT

El sistema de transporte público se ha estructurado de manera sistemática en el diagrama de funcionamiento y ahora se debe organizar en las plantillas de la matriz para cada sub-sistema (es decir ferrocarril convencional, metro, tren ligero, autobuses, etc.)

Las columnas de la izquierda muestran las diferentes localizaciones del sistema (de acuerdo con el gráfico de la estructuración del sistema como se muestra antes).

Las filas de la derecha indican todas las amenazas que se consideren posibles.

Se recomienda que los resultados de la evaluación respecto a la probabilidad de ocurrencia e impacto/gravedad se marquen por colores de acuerdo a las categorías de riesgo. Estos colores indican claramente y visualmente donde están los mayores riesgos detectados y se muestran donde se requiere una acción preventiva o mitigación.

Matrix indicating Risks (Metro)			Type of Attack													
			Type of Attack A	Type of Attack B	Type of Attack C	Type of Attack D	Type of Attack E	Type of Attack F	Type of Attack G	Type of Attack H	Type of Attack I	Type of Attack K	Type of Attack L	Type of Attack M	Type of Attack N	
Station	Target															
	Location A	Specification														
	Location B	Specification														
	Location C	Specification														
	Location D	Specification														
	Location E	Specification														
	Location F	Specification														
	Location G	Specification														
	Location H	Specification														

Figura 6. Matriz de indicadores del riesgo. COUNTERACT

Fuente: COUNTERACT

Los resultados del análisis se pueden utilizar para "experimentar": pueden ser clasificados de acuerdo a diferentes consideraciones, por ejemplo, de acuerdo a las ubicaciones, como se demuestra en el siguiente gráfico.

Risks ranked according to Locations							
No	Target					Type of Attack	Risk Category
1	Location / Specification		Location	Specification		Type of Attack A	
2 to 7			Location	Specification		Type of Attack A	
			Location	Specification		Type of Attack B	
			Location	Specification		Type of Attack B	
			Location	Specification		Type of Attack B	
			Location	Specification		Type of Attack B	
	Location / Specification	Specification	Location	Specification	Specification	Type of Attack B	
		Specification	Location	Specification	Specification	Type of Attack B	
8 to 26	Location / Specification	Specification	Location	Specification	Specification	Type of Attack C	
						Type of Attack D	
		Specification	Location	Specification	Specification	Type of Attack B	
		Specification	Location	Specification	Specification	Type of Attack B	
		Specification	Location	Specification	Specification	Type of Attack C	
	Location / Specification		Location	Specification			
			Location	Specification			

Figura 7. Riesgo por niveles en función de la localización. COUNTERACT

Fuente: COUNTERACT

Por otra parte, los resultados del análisis pueden ser clasificados de acuerdo a las amenazas y los tipos de ataque, como se ilustra en el gráfico siguiente.

Esta es una excelente manera de demostrar la necesidad de una acción específica, por ejemplo, para los tomadores de decisiones con poco tiempo.

Risks ranked according to Type of Attack						
Type of Attack	Target					Risk Category
1. Type of Attack A	Specification		Location	Location		
			Location	Location		
			Location	Location		
	Specification	Specification				
	Specification	Specification				
	Specification	Specification				
2. Type of Attack B	Specification	Specification	Location	Location	Location	
		Specification	Location	Location	Location	
	Specification		Location	Location		
			Location	Location		
			Location	Location		
	Specification	Specification	Location	Location	Location	
	Specification					

Figura 8. Riesgo por niveles en función del tipo de ataque. COUNTERACT

Fuente: COUNTERACT

1.5.3. Evaluación de la vulnerabilidad

Ahora que la matriz esté completa, indica claramente dónde están los mayores riesgos que se localizan y eso muestra donde se requiere una acción preventiva o mitigadora. Por lo tanto, este análisis debe ser la base sólida para cualquier acción, debido a que:

- Previene la acción ineficaz;
- Permite a los tomadores de decisiones hacer un uso más eficiente de los escasos recursos mediante la orientación óptima de sus inversiones en seguridad y protección.

El siguiente paso lógico es la evaluación de la vulnerabilidad. Básicamente, la evaluación de la vulnerabilidad consiste en analizar posibles disposiciones adicionales de seguridad y protección contra los riesgos diagnosticados en el paso anterior, es decir, ¿hasta qué punto la existencia de dispositivos de seguridad previstos se corresponde con los riesgos diagnosticados?

Con este enfoque se identifica la acción más urgente. Basándose en la identificación de los puntos débiles, se pueden desarrollar medidas adecuadas de prevención y mitigación.

La evaluación de las posibles medidas y dispositivos de seguridad podría incluir:

- Costes;
- Eficacia;
- Tiempo de ejecución;
- Beneficios adicionales sobre aspectos de seguridad laboral (aumentar el nivel de iluminación para el uso de CCTV facilitará la evacuación) o el servicio/comodidad de los pasajeros, mejorando la percepción de seguridad de los pasajeros/personal, la reducción del vandalismo, etc.
- Impacto de los seguros

1.5.4. Resultado de la evaluación

Se presentan los resultados en una tabla como la que se muestra a continuación.

Tabla 11. Evaluación de la vulnerabilidad. COUNTERACT

Objetivo dentro del Sistema Transporte	Amenaza		Riesgo y ranking ANTES	Categoría del riesgo & ranking DESPUÉS	Enfoque actual con dificultades y deficiencias	Posible Nuevo enfoque Para prevenir y mitigar	Costs	Remarks
Objetivo en el Sistema de Transporte	Tipo de amenaza	Especificación	20	16	ABC...	DEF...	...€	...
Objetivo en el Sistema de Transporte	Tipo de amenaza	Especificación	20	15	GHI...	JKL...	...€	...
Objetivo en el Sistema de Transporte	Tipo de amenaza	Especificación	15	12	MNO...	PQR...	...€	...
Objetivo en el Sistema de Transporte	Tipo de amenaza	Especificación	12	8	STU...	VWX...	...€	...
Objetivo en el Sistema de Transporte	Tipo de amenaza	Especificación	9	6	YZA...	BCD...	...€	...
Objetivo en el Sistema de Transporte	Tipo de amenaza	Especificación	8	4	EFG...	HIJ...	...€	...
Objetivo en el Sistema de Transporte	Tipo de amenaza	Especificación	6	4	KLM...	NOP...	...€	...
Objetivo en el Sistema de Transporte	Tipo de amenaza	Especificación	3	1	QRS...	TUV...	...€	...
Objetivo en el Sistema de Transporte	Tipo de amenaza	Especificación	2	1	WXY...	ZAB...	...€	...

Fuente: COUNTERACT

La tabla anterior permite la experimentación. Las categorías de riesgo y la clasificación (de acuerdo con el producto evaluado de la probabilidad de ocurrencia y el impacto/gravedad) antes y después se han puesto en práctica ciertas medidas de prevención / mitigación, son un trabajo de preparación ideal y una buena base para la toma de decisiones de la dirección.

La amplia lista de medidas y dispositivos de seguridad potenciales se ha ajustado en el proceso descrito, y se ha desarrollado así una lista con prioridades claras. Las prioridades toman en cuenta el nivel de riesgo, la eficacia y la rentabilidad, así como el calendario de ejecución de las garantías posibles.

Por último, la lista de prioridades de los dispositivos de seguridad recomendados para su aplicación se elabora en un informe. El informe debe identificar claramente y hacer comentarios sobre incertidumbres, limitaciones y simplificaciones en la evaluación del riesgo y también puede requerir investigaciones más detalladas en algunos aspectos, si es necesario.

1.6. DECRIS. SINTEF (Noruega)

El análisis probabilístico de seguridad (PSA) y análisis cuantitativo de riesgos (QRA) se han aplicado durante décadas como una parte integral de la gestión de la seguridad en las centrales nucleares y otras industrias de proceso industrial. PSA y QRA comprenden modelos probabilísticos detallados, tales como los árboles de fallos y eventos, y los modelos físicos de, por ejemplo, un el desarrollo de un incendio y una explosión. En Noruega, se reconoció que este tipo de modelos de riesgo requiere más conocimientos y recursos de los que se disponen en las pequeñas y medianas empresas y en el sector público. Por lo tanto, a principios de los años noventa, un enfoque mucho más simple se desarrolló bajo el acrónimo ROS. Se va a utilizar el correspondiente RVA acrónimo Inglés (Análisis de Riesgos y Vulnerabilidad) para describir esta metodología y las extensiones propuestas. La Dirección de Protección Civil y Planificación de Emergencias (OSD) tiene la responsabilidad general en Noruega de coordinar y asegurar que el RVA se utiliza en la gestión de las infraestructuras críticas.

En Noruega, el RVA se ha aplicado y adaptado para cada sector de forma independiente, lo que resulta en diferencias en los enfoques.

El enfoque DECRIS es el resultado de una intensa investigación de SINTEF en el ámbito de la evaluación del peligro / riesgo de las infraestructuras críticas. El proyecto / enfoque DECRIS se basa en las capacidades existentes en las metodologías de evaluación de riesgos sectoriales que ya existían en Noruega. El principal problema de estas metodologías de evaluación de riesgos, que es común a nivel mundial, es exactamente el enfoque sectorial y la evaluación de cada sector de forma independiente. Así el proyecto DECRIS tiene como objetivo reducir la brecha entre las metodologías que existen en diversos sectores y proponer una metodología de evaluación de todo el peligro genérico Riesgo y Vulnerabilidad para el análisis de la infraestructura intersectorial.

1.6.1.Fases

La metodología DECRIS se basa en un procedimiento de cuatro pasos:

1. Establecimiento de la clasificación de eventos y las dimensiones de riesgo.
2. Riesgo simplificado y el análisis de vulnerabilidad para los eventos identificados.
3. Selección de eventos que debe analizarse más.
4. Análisis detallado de los eventos seleccionados.

El proyecto DECRIS utiliza la experiencia del análisis de riesgos dentro de las diferentes infraestructuras críticas, y uno de los objetivos principales es desarrollar una

metodología RVA genérica de todos los peligros adecuado para el análisis de infraestructura intersectorial. Se consideran aspectos tanto de la seguridad laboral (accidentes, fallos tecnológicos, etc.) como de la seguridad de las instalaciones (ataques maliciosos). Además, el proyecto analiza las cuestiones relativas a cómo los medios de comunicación y el público afectan al proceso de decisión, y considera cómo las diferentes opiniones se pueden combinar para conseguir un sistema más adecuado para la toma de decisiones en todos los sectores.

1.6.2. Evaluación del riesgo

DECRIS considera las siguientes infraestructuras críticas; suministro de energía eléctrica, suministro de agua, el transporte y las TIC. A continuación se detalla el sector del transporte por resultar el de interés para esta investigación.

El sistema de transporte consta de varias redes de transporte y modos de transporte para personas y bienes. En Noruega en la actualidad existen cuatro redes principales de transporte: redes de carreteras, ferroviarias, aéreas y de transporte marítimo. Cada una de estas redes comprende elementos como cruces, puentes, túneles, aceras y terminales con una gran cantidad de equipos, tales como iluminación, señalización y sistemas de comunicación. Las autoridades públicas son responsables de la gestión de las redes de transporte de Noruega, sin embargo, la gestión de carreteras, aeropuertos y puertos está parcialmente financiada por su número de usuarios.

Los medios de transporte incluyen vehículos, como automóviles y camiones, trenes, tranvías, ferris, barcos y aviones. Hoy en día, las empresas privadas se encargan de los dos servicios de transporte, programados y no programados. Además, embarcaciones de recreo, vehículos particulares, bicicletas, y el recuento de viajes para un considerable número de trayectos diarios. Por otra parte, existe una considerable industria de servicios para el sector del transporte, incluida la producción y distribución de vehículos, combustible, y así sucesivamente.

Los noruegos hacen una media de 3-4 viajes diarios con una longitud media de 10.5 km, con una duración de 70-80 minutos al día, y se consumen en viajes. Se mueven 240 millones de toneladas de mercancías a unos 90 km cada año, principalmente por camión o barco.

La mayor parte de la actividad de transporte es muy dependiente de la energía y de un suministro constante y suficiente de combustible, en condiciones climáticas razonables. Si no es así, la gente y mercancías no llegan a sus destinos, lo que en consecuencia puede crear graves problemas para el desempeño de las funciones vitales de la sociedad, como la gestión de crisis, el suministro de alimentos, eliminación de desechos, la asistencia sanitaria, etc. Por lo tanto, el transporte es a la vez dependiente de otras infraestructuras críticas y a la vez esencial para que una sociedad funcione bien.

El RVA actual no es capaz de capturar la complejidad de las infraestructuras críticas interdependientes de una manera satisfactoria. El enfoque DECRIS al RVA propone llevar a cabo el análisis en dos niveles o fases.

En la primera fase, la cuestión principal es detectar las situaciones de riesgo más graves. En un estudio realizado en Oslo (Sklet et al., 1997; SAFETEC, 2004), se identificaron casi trescientos eventos no deseados. Por lo tanto, es necesario seleccionar sólo un subconjunto de éstas para el análisis detallado. Este proceso se asemeja al concepto básico de un PHA con algunas extensiones, sin embargo, un reto importante en un PHA es la evaluación de las consecuencias de un evento no deseado. Se podría especificar la consecuencia "promedio", o con el fin de poner de relieve las graves consecuencias, se podría más bien especificar una "peor consecuencia".

La elección de la evaluación de las consecuencias influirá en la forma en que se evalúan las frecuencias del evento no deseado. Si se elige la consecuencia "promedio" hay que evaluar la frecuencia del evento no deseado, independientemente de lo que sería el efecto después del evento. Sin embargo, si se opta por evaluar una consecuencia del "peor caso", la frecuencia del evento no deseado sólo debe cubrir las situaciones en que el evento no deseado se desarrollará de una manera muy grave, es decir, una frecuencia mucho menor. Dado que los resultados de los análisis de RVA a menudo se utilizan para la planificación de la preparación para emergencias, resulta más relevante para utilizar un enfoque de "peor caso".

En DECRIS, se evalúan varias dimensiones, por ejemplo, la seguridad, el impacto económico y la pérdida de servicios, en la misma hoja de trabajo, lo que hace difícil la evaluación de la frecuencia en un escenario de "peor caso". Una manera propuesta para superar este problema es llevar a cabo la evaluación de la frecuencia en dos pasos: en primer lugar, se evalúa la frecuencia "normal" del evento no deseado, y luego por separado evaluar la probabilidad condicionada de que los resultados de los eventos no deseados resulten en el "peor de los casos".

Un PHA suele centrarse en los "eventos no deseados". Con el fin de determinar las medidas de reducción del riesgo hay que vincular el evento no deseado a la infraestructura o los servicios. Por ello, se ha especificado un procedimiento para vincular funciones críticas llamada de seguridad laboral (SCF2) para los eventos no deseados, lo que en la metodología DECRIS se denomina "principales eventos".

Está claro que esta es una metodología en la que no hay una gran diferencia con respecto a una típica evaluación de riesgos. Sin embargo, un mecanismo de perfeccionamiento se ha incorporado con el fin de reducir la lista de eventos que deben evaluarse. Este proceso de selección es tal vez el punto culminante de esta metodología. El proceso de selección se lleva a cabo sobre la base de la importancia

del riesgo, de la cantidad de infraestructuras impactados y también en las dificultades de comunicación de este evento para el público.

1.7. Directrices para terminales de transporte combinado. Union of Combined Road-rail transport companies (UIRR)

La Unión Internacional de Transporte Combinado Ferrocarril-Carretera (UIRR) consideró de importancia participar activamente en la elaboración de medidas de seguridad para el transporte intermodal con el fin de garantizar que estas medidas fueran eficaces y viables, y por tanto aumentar así el nivel de seguridad evitando por tanto poner en peligro la eficiencia económica del transporte combinado. Así pues, en el año 2004 publicó las "Propuestas de la UIRR destinadas a aumentar la seguridad en el transporte combinado".

La UIRR elaboró entonces su metodología para análisis de riesgos: "Directrices para terminales de transporte combinado" a disposición de los expertos del sector del transporte con el fin de contribuir a la discusión sobre medidas eficaces relativas a la seguridad en el transporte de mercancías sector.

A continuación se resume la metodología de análisis desarrollada por la UIRR.

1.7.1. Evaluación de la vulnerabilidad de las terminales

Los factores de la vulnerabilidad

Se definen dos factores principales respecto de la vulnerabilidad:

- **La sensibilidad** del lugar, que se mide en función de la presencia de sustancias peligrosas, este último hecho, representa el factor clave de interés para los terroristas con respecto a una terminal de transporte combinado. De hecho, se podría concebir que una organización terrorista puede atacar a un terminal para otros fines.
- **La ubicación** de la terminal, y sobre todo su proximidad posible a las zonas densamente pobladas, a los centros de recogida para los miembros de la población (escuelas, hospitales, residencias...), o a las infraestructuras críticas (aeropuertos, estaciones de ferrocarril, los corredores de transporte, plantas químicas, etc.).

Además se tienen en cuenta otros dos elementos para evaluar la verdadera vulnerabilidad del sitio. Por un lado, las precauciones ya tomadas para garantizar la seguridad de este último. Por otro lado, el estado de alerta, es decir, la constante evolución de la amenaza y como se analiza por la administración, regional o nacional.

Estos dos tipos de parámetros, estrechamente vinculados con el contexto espacio-temporal, no entran en el marco de un estudio general. Sin embargo, no pueden faltar en un análisis de riesgos aplicado a un sitio en particular.

1. Presencia de sustancias sensibles

Variabilidad de la sensibilidad de las sustancias

En cuanto a las sustancias sensibles se refiere, deben tenerse en cuenta tres variables:

- su naturaleza
- la cantidad
- la posible combinación

Respecto de estos tres elementos, el primero es fundamental: es tanto que determina la cantidad de daño probable que puede causar directa o indirectamente por los productos de que se trate. La cantidad es un factor que puede empeorar el problema potencial. Esencialmente, al igual que un elemento combinatorio, crea el problema de un "efecto dominó".

Tipos de riesgo causado por la presencia de sustancias sensibles

La magnitud de las consecuencias dependerá de la naturaleza de los productos transportados, su cantidad, las circunstancias del ataque y la distancia a la que se produce el impacto. Dejando a un lado los riesgos específicos vinculados a la irradiación de sustancias bacteriológicas y sustancias que constituyen una amenaza de infección, estas consecuencias pueden dividirse en tres tipos dependiendo de si son el resultado de:

- una explosión
- un fuego
- una nube tóxica

Intento de clasificación de la sensibilidad en materia de seguridad y salud y seguridad física

Por ello se propone poner las sustancias de alto riesgo presentes en un momento dado en un terminal y ordenarlas en una clasificación correspondiente a tres niveles:

- Muy sensibles
- Sensibles
- Menos sensibles

La evaluación de la sensibilidad que aquí se basa en tres fuentes principales:

- la literatura en general y, más concretamente, en el trabajo del CIFMD (Comité para el Desarrollo de la Formación en el Transporte de Mercancías Peligrosas) sobre la Seguridad de Transportes Terrestres de mercancías peligrosas.
- la experiencia de INERIS (Instituto Nacional Francés para el Medio Ambiente Industrial y Riesgos).
- documentación finalizado por el Departamento de Bomberos de Ginebra para cada sustancia peligrosa sobre la base de hechos reales (informes de experiencias) y el análisis científico; estos datos, recogidos en la Guía Naranja del Departamento de Bomberos de Ginebra (GOR SAP), proporcionan información sobre las distancias mínimas de aproximación a un desastre para las partes intervinientes sin protección respiratoria, las distancias máxima difusión de la toxicidad de un producto, las distancias de seguridad en caso de una explosión, etc.

Variaciones en la clasificación de la sensibilidad en función de los riesgos adicionales

La clasificación así establecida introduce un factor de diferenciación que se refleja en un promedio, sin tener en cuenta, en esta etapa, el potencial efecto dominó. Por lo tanto, debe interpretarse en función de la situación exacta. Teniendo en cuenta los riesgos realmente encontrados, ciertas clasificaciones podrían ser revisadas y equilibradas de una manera diferente.

Así, por ejemplo, si la terminal está situada en una zona densamente poblada o en las inmediaciones de una infraestructura crítica de gran importancia, ciertas sustancias sensibles se pueden subir a la categoría inmediatamente superior. Este podría ser el caso, por ejemplo, del nitrato de amonio y fertilizantes a partir de nitrato de amonio o líquidos y sustancias explosivos que, de acuerdo a la realidad sobre el terreno, posiblemente parecen ser muy sensibles. Las dos siguientes tablas ilustran la variabilidad de estas situaciones.

Tabla 12. Clasificación de sensibilidad en caso de que el riesgo adicional consiste en un ataque a la Terminal se considere como un objetivo en sí mismo. UIRR

Class	Division	Material	Quantity		
			Tank (l)	Bulk (kg)	Package
1	1.1	Explosive substances and objects	-	-	0
	1.2	Explosive substances and objects	-	-	0
	1.3	Explosive substances and objects in compatibility group C	-	-	0
	1.5	Explosive substances and objects	0	-	0
2	2.1	Inflammable gases	3000	-	b
	2.3	Toxic gases (excluding aerosols)	0	-	0
3		Inflammable liquids in packing groups I and II	3000	-	b
		Desensitised explosive liquids	-	-	0
4	4.1	Desensitised explosive substances	-	-	0
	4.2	Substances in packing group I	3000	-	b
	4.3	Substances in packing group I	3000	-	b
5		Combustible liquids in packing group I	3000	-	b
		Perchlorates, ammonium nitrate and fertilizers made fr. ammonium nitrate	3000	3000	b
6	6.1	Toxic substances in packing group I	0	-	0
	6.2	Infectious substances in category A	-	-	0
7		Radioactive substances	3000 A1 or 3000 A2; in a package of type B(U) or of type B(M)		
8		Corrosive substances in packing group I	3000	-	b

Fuente: UIRR

Tabla 13. Clasificación de sensibilidad caso de que el riesgo adicional consiste en el robo de sustancias peligrosas. UIRR

Class	Division	Material	Quantity		
			Tank (l)	Bulk (kg)	Package
1	1.1	Explosive substances and objects	-	-	0
	1.2	Explosive substances and objects	-	-	0
	1.3	Explosive substances and objects in compatibility group C	-	-	0
	1.5	Explosive substances and objects	0	-	0
2	2.1	Inflammable gases	3000	-	b
	2.3	Toxic gases (excluding aerosols)	0	-	0
3		Inflammable liquids in packing groups I and II	3000	-	b
		Desensitised explosive liquids	-	-	0
4	4.1	Desensitised explosive substances	-	-	0
	4.2	Substances in packing group I	3000	-	b
	4.3	Substances in packing group I	3000	-	b
5		Combustible liquids in packing group I	3000	-	b
		Perchlorates, ammonium nitrate and fertilizers made fr. ammonium nitrate	3000	3000	b
6	6.1	Toxic substances in packing group I	0	-	0
	6.2	Infectious substances in category A	-	-	0
7		Radioactive substances	3000 A1 or 3000 A2; in a package of type B(U) or of type B(M)		
8		Corrosive substances in packing group I	3000	-	b

Fuente: UIRR

2. Localización de las terminales

Definición de la vulnerabilidad de las zonas

El factor estructural que determina la vulnerabilidad de una terminal es su ubicación. Entre los elementos que permiten evaluar el riesgo potencial están los siguientes:

- la proximidad a una o más áreas de estancia o la construcción de la terminal,
- la proximidad de las instalaciones a otras consideradas vulnerables: escuelas, hospitales, etc.,
- la presencia de infraestructuras críticas o sensibles: aeropuertos, estaciones ferroviarias, centros de transporte (carretera, ferrocarril u otros) que si quedaron inoperativas supondrían graves problemas: arsenales, fábricas de productos químicos, etc.,
- las características ambientales del sitio en el que la terminal se encuentra: existe el riesgo de una fuerte contaminación debido, por ejemplo, a la

presencia de un río, las aguas subterráneas, o un punto de captación de agua, etc.

Estimación de las áreas involucradas

La determinación habitual de las zonas de vulnerabilidad no sólo es una tarea difícil sino también muy delicada. La construcción arbitraria podría suponer una discriminación indebida de ciertas terminales cuya ubicación específica en el espacio no haya sido tenida en consideración suficientemente.

La única manera de establecer un sistema de nomenclatura es mediante el empleo de un método deductivo: de acuerdo con un estudio de amplio alcance aplicado a un número importante de terminales, sería posible realizar promedios estadísticos

Sin embargo es posible, en base a la bibliografía existente, definir los valores indicativos que se podrían utilizar de una manera formal en el marco de dicho estudio.

En el caso de un sitio que contenga sustancias peligrosas muy sensibles, las zonas se pueden definir de la siguiente manera:

Tabla 14. Definición de zonas (UIRR)

NATURALEZA DE LA ZONA	DISTANCIAS
Zona de impacto inmediata	200 a 600 m
Zona de expansión de toxicidad	2.500 a 4.000 m

Fuente: UIRR

Sensibilidad cruzada y localización de las terminales

Con el fin de correlacionar la sensibilidad y la vulnerabilidad, es decir, los riesgos derivados de los productos peligrosos presentes en el lugar y los relacionados con la ubicación de este último, se propone considerar dos series de indicadores en el análisis local del riesgo. Gracias a estos indicadores, que incorporan las características del producto peligroso, es posible medir, producto a producto, las zonas de vulnerabilidad

Se definen a continuación el peligro y los indicadores de riesgo:

1. Escala de peligrosidad

En cada hoja de cada producto figurará una escala de peligro como la siguiente:

Tabla 15. Escala de peligrosidad (UIRR)

Incremento del riesgo	Escala de peligrosidad					Efectos inmediatos	Denominación UN
	Salud	Fuego	Inestable al calor	Reactivo al agua	Compuestos explosivos		

Fuente: UIRR

Una escala de 0 a 4 indica el nivel de peligrosidad:

Tabla 16. Nivel de peligrosidad (UIRR)

0	Riesgo cero o bajo
1	Riesgo bajo
2	Peligroso
3	Muy peligroso
4	Excesivamente peligroso

Fuente: UIRR

2. Escala de riesgo

La segunda serie de indicadores implica a los elementos relacionados con el potencial de riesgo en el caso de un evento negativo que afecta a un terminal. Se consideran los siguientes:

- La densidad de la población residente [D];
- Público y/o instalaciones estratégicas (escuelas, estaciones de ferrocarril, aeropuertos, hospitales, cárceles ...) [E];
- Las instalaciones de las infraestructuras de transporte [I];
- Efecto dominó potencial en otras instalaciones sensibles (empresas de riesgo, los depósitos de mercancías peligrosas...) [D].
- Medio ambiente [M]

Para cada una de estas categorías, se define un criterio que permite el establecimiento de una escala de riesgo.

Así para la **densidad de población** se definen cinco niveles (nivel 1 a nivel 5) en función de la cantidad de habitantes de la zona.

El **público** se calcula en base al número de personas que puede contener, por una parte y la naturaleza sensible, estratégica o simbólica de las instalaciones por otra, asignándole valores comprendidos entre 1N para pequeñas estructuras y 5N para áreas con más de 1.500 personas. El carácter simbólico o estratégico de las instalaciones se evalúa desde categoría 1S para prisiones y hospitales a 5S para estaciones de ferrocarril o aeropuertos de tamaño significativo, etc. Por definición, la determinación de los objetivos estratégicos y del valor simbólico de una instalación se basa en una evaluación que, por una parte, nunca puede ser totalmente objetiva y, por otra parte, dependerá del contexto y los factores de otras variables (como la estrategia utilizada por los terroristas, el nivel de protección de los sitios, etc.). En consecuencia, y como producto de los anteriores, resultarán cinco niveles de riesgo, N1 a N5.

Las **infraestructuras de transporte** se dividen también en cinco categorías, en función de su nivel de impacto en la cadena del transporte si son destruidas o si quedaran fuera de servicio. La categoría 1 para pasajeros o mercancía de segundo orden, hasta la categoría 5 para dos o más infraestructuras afectadas del tipo; intersecciones varias autopistas en áreas urbanas que puedan afectar gravemente a la cadena de transporte, puertos, aeropuerto, etc. Consecuentemente el nivel de riesgo asociado a la infraestructura será de N1 a N5.

El **efecto dominó** se considera asimismo con niveles N1 a N5 que consideran la posibilidad de la presencia de sustancias peligrosas en un radio de 4 kilómetros hasta el nivel 5 que considera lugares tipo “Seveso”, de gran riesgo por tanto.

El riesgo **medio ambiental** más inmediato en caso de destrucción de un terminal en la que intervengan sustancias peligrosas, es la proximidad de éstas a los acuíferos, los cuales pueden causar la rápida propagación de un producto químico y por lo tanto dañar el medio ambiente y crear una amenaza para la salud humana. El examen de la ubicación de terminales de transporte combinado por lo tanto se basará en este factor valorándose con un N1 para ausencia de acuíferos y canales de agua en un radio de 600 m cursos de agua pequeña en un área de 4 kilómetros, hasta el N5 para la presencia de un gran río, planta de purificación, aguas subterráneas o áreas de captación de agua en un radio de seiscientos metros.

Tabla 17. Ejemplo de escala de riesgos obtenida. UIRR

	Density of resident population [P]	Public and/or strategic facilities [I]	Transport infrastructure facilities [T]	Potential domino effect [D]	Environment [E]
Level 5					
Level 4					
Level 3					
Level 2					
Level 1					

Fuente: UIRR

1.7.1.1. Ejecución de la evaluación en siete etapas

El análisis de riesgos aplicado a un terminal intermodal requiere un enfoque detallado y metódico de un especialista con experiencia de trabajo con operadores de terminales, usuarios, autoridades, etc. Sin embargo, es posible realizar un análisis preliminar del riesgo global con bastante rapidez a través de un enfoque sistemático basándose la metodología de análisis de riesgos descrita anteriormente.

Las etapas a seguir para la evaluación de los riesgos de una terminal serán las siguientes:

1. Determinación de la vulnerabilidad de una terminal en función de su localización (elaboración de la escala de riesgo).
2. Determinación de la vulnerabilidad de la terminal en función de su contenido (desarrollo de la escala de riesgo).
3. Determinación de los factores contextuales susceptibles de afectar a la vulnerabilidad de un lugar.

Cuando los dos factores principales que determinan la vulnerabilidad de una terminal, ubicación geográfica y contenido, son identificados, es importante tener en cuenta los otros parámetros que pueden influir en la evaluación de la vulnerabilidad del lugar.

En particular, será necesario tener en cuenta, por una parte, el plan de seguridad existente, es decir, las medidas y dispositivos que refuerzan de hecho la seguridad

de un sitio, o que no fueron concebidos para este fin, y por otra parte, la falta de alarma.

4. Elaboración de la evaluación de la vulnerabilidad de la terminal.

Una vez identificados, todos los parámetros (localización [L], dispositivos reales existentes [D], nivel existente de alarma [A]) asociados en una matriz común que hará posible el equilibrio de acuerdo a la importancia relativa de los demás, tal y como se refleja en la siguiente figura:

Figura 9. Matriz de evaluación de la vulnerabilidad. UIRR

Fuente: UIRR

5. Identificación de la naturaleza de la amenaza potencial

En base a la vulnerabilidad específica de las instalaciones, obtenida en apartados anteriores, es recomendable tener una idea clara de las amenazas a las que la terminal está potencialmente expuesta. En general, es probable que una terminal se sitúe alejada de centros urbanos, donde podría servir como sitio para la transferencia de materiales peligrosos, o como soporte de un ataque terrorista directo.

Por otra parte, no se descarta que pudiera constituir un punto de partida para sirviendo a los cometidos terroristas como un “Caballo de Troya”. Tal vez no sea una terminal muy importante, si esta se dispone cerca de viviendas, podría presentar un riesgo. En definitiva existen muchas amenazas fundamentadas en una terminal intermodal.

6. Identificar las consecuencias de un ataque terrorista

De acuerdo con los parámetros establecidos por la escala de riesgo, se tienen en cuenta las posibles consecuencias para la terminal y su entorno.

Anexo | **2**

Encuesta al Sistema Portuario
Español

POLITÉCNICA

ENCUESTA SOBRE LA EVALUACIÓN DE RIESGOS PARA LA SEGURIDAD EN TERMINALES PORTUARIAS EN ESPAÑA

OBJETO

El objeto de la presente encuesta es contribuir a la mejora en la evaluación de riesgos potenciales para la seguridad en instalaciones portuarias a través de la opinión y el análisis de los explotadores de terminales.

Para ello se pretende conocer de primera mano la opinión del operador respecto de la evaluación de riesgos actual en terminales portuarias, basándose en su experiencia y en las eventualidades sufridas para la seguridad desde la puesta en marcha de ésta. Se trata, por tanto, de generar **nuevos parámetros** a considerar para obtener una fórmula ajustada a la realidad de la seguridad en los puertos de interés general.

La información obtenida se utilizará para la elaboración de una Tesis Doctoral de la Universidad Politécnica de Madrid. Dicho trabajo está dirigido por el Profesor D. Alberto Camarero Orive, Director del Departamento de Ingeniería Civil. Transportes de la Escuela de Ingenieros de Caminos, Canales y Puertos de la Universidad Politécnica de Madrid.

Agradecerle de antemano el tiempo dedicado para completar esta encuesta necesaria para la elaboración del estudio. Su opinión es de gran importancia para intentar mejorar la evaluación de riesgos, objetivo del estudio.

Asimismo, el resultado de estas encuestas será totalmente confidencial, no haciéndose públicas las respuestas en ningún caso.

Si tiene alguna duda acerca de la confidencialidad de la encuesta, o considera de importancia aportar algún otro tipo de información, comuníquese con nosotros enviándonos un correo electrónico a david.romero@upm.es

Como se indicaba anteriormente, el ámbito de la encuesta se ciñe única y exclusivamente al ámbito de las terminales operadas en su puerto.

Le rogamos que **responda a todas las cuestiones planteadas** ajustándose **al formato de respuesta dado**.

CUESTIONARIO

1. ¿Conoce la Metodología de Evaluación del Riesgo que se aplica para los puertos de interés general españoles a través de la plataforma SECUREPORT?

Sí

No, pero si conozco SECUREPORT

2. ¿Considera que existen riesgos frecuentes para las personas en su terminal que no estén recogidos en SECUREPORT?

No, todos los riesgos están debidamente considerados

SI. ¿Cuáles?

3. ¿Y para las mercancías?

No, todos los riesgos están debidamente considerados

SI. ¿Cuáles?

4. Según usted, ¿Cuáles son los escenarios de amenaza a la seguridad más factibles que se pueden dar en su terminal?

5. ¿Cuáles han sido los escenarios de amenaza más frecuentes?

6. A su juicio, ¿son más frecuentes los riesgos asociados a la seguridad de la mercancía (robo, destrucción, etc.) o a la seguridad de las personas?

A la seguridad de la mercancía

A la seguridad de las personas

7. Valore la seguridad de la accesibilidad de su terminal:

Alta seguridad (difícil accesibilidad a la instalación)

Regular seguridad (accesibilidad relativamente sencilla a la instalación)

Baja seguridad (fácil accesibilidad a la instalación)

8. Defina el sistema de accesibilidad existente en su terminal y de que se compone; tipo de vallado, características, sistema de barreras, si existe control de tarjetas, de personas, etc.

9. ¿Existen elementos vulnerables en la terminal (edificios, zonas de tránsito, aparcamientos...) de fácil alcance/acceso a través de terminales contiguas?

No

Sí. ¿Cuáles?

10. A su juicio, ¿la disposición de las instalaciones dentro de la terminal influye en la posibilidad de recibir algún tipo de ataque o por el contrario no influye?

Sí

No

11. Ordene las principales instalaciones de su terminal, en función de la relevancia que a su juicio tienen para la seguridad, de mayor a menor (mayor relevancia equivale a más susceptibilidad a ataques o amenazas a la seguridad).

12. ¿Considera que los problemas de conflictividad laboral inciden en la seguridad de sus instalaciones?

Bastante

Algo

Nada

13. ¿La formación del equipo de control y vigilancia de la terminal es la adecuada?

Sí

No

14. ¿Cuántos años de experiencia media tiene dicho equipo? _____

15. En caso de amenaza a la seguridad, ¿cuál es su tiempo medio de respuesta?

Menos de 5 minutos

Aproximadamente 5 minutos

Más de 5 minutos

16. ¿Se han efectuado inspecciones de las instalaciones portuarias por parte de la Comisión Europea con el fin de controlar la aplicación efectiva del Reglamento (CE) Nº 725/2004?

Sí

No

17. ¿Cuál ha sido el grado de satisfacción de dicha inspección?

Satisfactorio

Aceptable

Deficiente

18. ¿Considera suficientes las medidas implantadas para la mejora de la seguridad en función del riesgo real de su instalación?

Sí

No

Parcialmente

Si considera necesario hacer alguna observación, por favor indíquela a continuación:

IMPORTANTE: No olvide enviar la encuesta al correo electrónico: david.romero@upm.es o bien por correo ordinario a la dirección:

Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos, Avda. Profesor Aranguren s/n. 28040 Madrid, a la atención del Profesor D. Alberto Camarero Orive.

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** (columnas A y B). 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).

Amenaza (columna C). 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 (columna D). 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 (columna E). 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 (columna F). 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.

La puntuación más elevada para una determinada situación será:

Amenaza – Alta.....	3
Vulnerabilidad – No se han contemplado contramedidas.....	4
Impacto – Muertes o lesiones posibles.....	5
Puntuación del riesgo.....	60

El resultado más bajo será:

Amenaza – Baja.....	1
Vulnerabilidad – Plena.....	1
Impacto – Pequeño.....	1
Puntuación del riesgo.....	1

Prioridad de actuación (Columna G). Tabular y listar las puntuaciones de cada amenaza contra cada uno de los objetivos potenciales facilitarán la fijación del orden de prioridades para hacer frente a cada incidente potencial. El proceso debería dar lugar a indicaciones acerca de las medidas necesarias para evitar, detectar y atenuar

las consecuencias de posibles incidentes, de los recursos disponibles o necesarios, y sobre las medidas de protección adecuadas.

Cuando se identifique el objetivo potencial y se determinen y evalúen las medidas de protección más apropiadas se debería considerar el historial y el modus operandi de grupos ilegales que pudieran operar en la zona al evaluar las situaciones probables.

Esto es una reducción evaluada del resultado para cada situación, basada en la eficacia percibida de las medidas de protección cuando se lleven a la práctica. El resultado debería servir para orientar acerca de las iniciativas y recursos que mejor podrían contribuir a disuadir los ataques contra el objetivo potencial. También puede dar indicaciones acerca de los objetivos o amenazas que no haga falta tomar en consideración, o que la medida de protección de que se trate no sea viable por falta de recursos u otras limitaciones.

La TRAM de cada objetivo potencial debería cotejarse con una matriz general en la que figuren las situaciones de amenaza similares y las medidas de protección normales y reconocidas para obtener la máxima eficacia. Será igualmente posible agrupar varios objetivos potenciales bajo una misma medida de protección.

La TRAM debidamente completada, acompañada de un resumen consolidado de todas las medidas de protección analizadas y que puedan ponerse en práctica, debería servir de base para la formulación del plan de protección del puerto.

Anexo 3

Criterio Experto

POLITÉCNICA

ENCUESTA SOBRE EVALUACIÓN DE NUEVOS PARÁMETROS PARA LA EVALUACIÓN DE LA SEGURIDAD EN PUERTOS RONDA 1

OBJETO

El objeto de la presente encuesta es contribuir a la mejora en la evaluación de riesgos potenciales para la seguridad en instalaciones portuarias a través de la opinión de expertos.

Durante esta investigación se proponen 5 nuevos parámetros para la evaluación del riesgo en instalaciones portuarias. Se pretende ahora validar los mismos en base al resultado de encuestas realizadas al sistema portuario español y al análisis de boletines de seguridad de la Guardia Civil.

Para ello se describen a continuación los parámetros propuestos preliminarmente y se facilita debajo de cada uno de ellos un espacio para que pueda elaborar su opinión al respecto de cada uno de ellos.

La información obtenida se utilizará para la elaboración de una Tesis Doctoral de la Universidad Politécnica de Madrid. Dicho trabajo está dirigido por el Profesor D. Alberto Camarero Orive, de la Escuela de Ingenieros de Caminos, Canales y Puertos de la Universidad Politécnica de Madrid.

Su opinión es de gran importancia para intentar mejorar la evaluación de riesgos, objetivo del estudio.

Asimismo, el resultado de este cuestionario será totalmente confidencial, no haciéndose público sus datos personales en ningún caso.

Si tiene alguna duda acerca de la confidencialidad de la encuesta, o considera de importancia aportar algún otro tipo de información, comuníquese con nosotros enviándonos un correo electrónico a david.romero@upm.es

Le rogamos que **responda a las cuestiones planteadas** ajustándose **al formato de respuesta dado**.

IMPORTANTE: No olvide enviar la encuesta al correo electrónico: david.romero@upm.es o bien por correo ordinario a la dirección:

Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos, Avda. Profesor Aranguren s/n. 28040 Madrid, a la atención del Profesor D. Alberto Camarero Orive.

Gracias por su participación

Una vez realizado el análisis de las encuestas al Sistema Portuario Español y de los Boletines de Seguridad, se desprenden las siguientes cuestiones de interés que dan lugar a la definición de varios parámetros que se integrarán formando la propuesta metodológica:

1. Puerto/Fachada marítima. Se constata mediante las encuestas y el análisis de las estadísticas que el riesgo que genera una amenaza dada en el puerto depende en gran medida de la localización del puerto en una u otra fachada marítima.

2. Mercancía. El riesgo de que se produzca una amenaza dada (probabilidad de suceso) se ve afectado asimismo por el tipo de mercancía objeto de la amenaza, y por tanto del tipo de terminal de que se trate, habiéndose comprobado mediante los resultados de las encuestas que los riesgos son mayores en unos tipos que en otros en opinión de los responsables de seguridad de los puertos.

3. Accesibilidad. Respecto de la vulnerabilidad existente en los accesos a los puertos, tal y como se refleja en las estadísticas y se desprende asimismo del análisis de las metodologías seleccionadas, se considera importante evaluar mejor aquellos aspectos relativos a la accesibilidad a la instalación.

4. Localización. Del análisis se desprende también la importancia que tiene la localización de la terminal a evaluar en el conjunto del puerto, o en su caso la localización del activo dentro de una terminal concreta pues esto influye en su “factibilidad de ataque”.

5. Elementos clave. Algunos elementos de la terminal resultan clave para el funcionamiento de ésta y su daño o paralización supondría una merma de la operatividad de la terminal.

6. Probabilidad de la amenaza. Se evalúa la probabilidad de suceso de cada amenaza a considerar en base a la estadística de sucesos.

POLITÉCNICA

ENCUESTA SOBRE EVALUACIÓN DE NUEVOS PARÁMETROS PARA LA EVALUACIÓN DE LA SEGURIDAD EN PUERTOS RONDA 2

OBJETO

El objeto de la presente encuesta es realizar la segunda ronda de consultas sobre los nuevos parámetros a proponer en la evaluación de riesgos en puertos.

Para ello se describen a continuación los parámetros propuestos tras la primera ronda para su validación, facilitándose debajo de cada uno de ellos un espacio para que pueda elaborar su opinión al respecto de cada uno de ellos.

La información obtenida se utilizará para la elaboración de una Tesis Doctoral de la Universidad Politécnica de Madrid. Dicho trabajo está dirigido por el Profesor D. Alberto Camarero Orive, de la Escuela de Ingenieros de Caminos, Canales y Puertos de la Universidad Politécnica de Madrid.

Su opinión es de gran importancia para intentar mejorar la evaluación de riesgos, objetivo del estudio.

Asimismo, el resultado de este cuestionario será totalmente confidencial, no haciéndose público sus datos personales en ningún caso.

Si tiene alguna duda acerca de la confidencialidad de la encuesta, o considera de importancia aportar algún otro tipo de información, comuníquese con nosotros enviándonos un correo electrónico a david.romero@upm.es

Le rogamos que **responda a las cuestiones planteadas** ajustándose al **formato de respuesta dado**.

IMPORTANTE: No olvide enviar la encuesta al correo electrónico: david.romero@upm.es o bien por correo ordinario a la dirección:

Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos, Avda. Profesor Aranguren s/n. 28040 Madrid, a la atención del Profesor D. Alberto Camarero Orive.

Gracias por su participación

Tras la primera ronda de consultas se muestran a continuación los parámetros a proponer mejor definidos en su alcance para su valoración.

- Riesgo intrínseco de la fachada Marítima (PT). Se recoge la influencia de la fachada marítima mediante un índice denominado “riesgo intrínseco de la fachada marítima”, y que se deberá considerar como parte de la valoración que se realice de la “amenaza” a la instalación, valorándose la probabilidad de suceso para cada fachada en función de las estadísticas disponibles de seguridad. De esta manera, por ejemplo, un puerto ubicado en la costa cantábrica tendrá una probabilidad de amenaza de intrusión inferior a cualquier puerto dispuesto en la zona del Atlántico Sur o incluso del Mediterráneo Sur. Las fachadas marítimas a considerar para su valoración serán; Atlántica Norte, Atlántica Sur, Mediterránea o Cantábrica.

- Riesgo intrínseco de la terminal (T). Es evidente que la peligrosidad se puede asociar, desde un punto de vista de la probabilidad de suceso de una amenaza, a cada tipo de terminal en virtud del tipo de instalaciones que esta posee y del tipo de actividad que en ella se desarrolla. Se define un parámetro que considera este aspecto, denominado “riesgo intrínseco de la terminal”, y que se deberá considerar como parte de la valoración que se realice de la “amenaza” a la instalación, definiéndose de esta forma diferentes niveles de amenaza para cada tipo de terminal; contenedores, pasajeros, graneles líquidos, graneles sólidos, etc. basándose en las características particulares de cada tipo de mercancía.

- Accesibilidad (Iac). Este factor se redefine, pues ya existía, si bien ahora trata de evaluar la vulnerabilidad de las instalaciones en base a diferentes aspectos físicos. Se evalúan las características del cerramiento, sistemas de vigilancia, etc., variando estas en función del tipo de terminal. Por ello se propone la definición del parámetro de accesibilidad con modificaciones en su valoración, de forma que esta se ajuste a situaciones específicas que garanticen la seguridad, valorándose para ello en este parámetro el tipo de vallado y la existencia de iluminación perimetral adecuada, los sistemas de control de accesos (lectores de matrículas, tarjetas de identificación personal, CCTV, arcos detectores, scanner para mercancías, sensores de movimiento, etc).

- Layout (ILo). Se valora la disposición de la terminal respecto de los accesos al puerto pues ello implica una mayor vulnerabilidad. Además se considera la disposición de la instalación respecto de las terminales de graneles líquidos, debido a su peligrosidad ante un ataque con explosivos o disparos, cuyos efectos podrían alcanzar a otras instalaciones próximas.

- Relevancia operativa de elementos (Ro). Hay elementos particulares de la terminal que no pueden dañarse dada su importancia para un adecuado funcionamiento de esta, por ejemplo; las estructuras de acceso rodado ferroviario, así como los equipos de manipulación, centros de transformación y las instalaciones de almacenamiento (silos, tinglados, etc.) y que pueden sufrir los

efectos de un ataque terrorista, dejando inutilizada una parte importante de la terminal, con las consiguientes consecuencias. Así, se realiza una lista de elementos con una relevancia operativa a considerar la cual será evaluada en función del tipo de amenaza a evaluar.

A large, empty rectangular box with a black border, intended for a list of elements with operational relevance for evaluation.

- Riesgo particularizado (I_s). Este índice considera la probabilidad que se asocia para cada tipo de amenaza evaluada en base a las estadísticas de seguridad del puerto en estudio.

A large, empty rectangular box with a black border, intended for the evaluation of the particularized risk index (I_s).

POLITÉCNICA

OBJETO

El objeto de la presente encuesta es contribuir a la mejora en la evaluación de riesgos potenciales para la seguridad en instalaciones portuarias a través de la opinión de expertos.

Durante esta investigación se han propuesto diferentes parámetros para la evaluación del riesgo en instalaciones portuarias y asociados a cada uno de ellos diferentes sub-parámetros. Se trata ahora de valorar si resulta de interés, por las mejoras que puede introducir en el resultado final, la introducción de coeficientes a los parámetros ya definidos.

La presente encuesta es muy breve y sencilla de responder, y se realiza con el fin de obtener una opinión experta que permita valorar diferentes opciones que se plantean mediante un breve cuestionario.

La información obtenida se utilizará para la elaboración de una Tesis Doctoral de la Universidad Politécnica de Madrid. Dicho trabajo está dirigido por el Profesor D. Alberto Camarero Orive, de la Escuela de Ingenieros de Caminos, Canales y Puertos de la Universidad Politécnica de Madrid.

Su opinión es de gran importancia para intentar mejorar la evaluación de riesgos, objetivo del estudio.

Asimismo, el resultado de estas encuestas será totalmente confidencial, no haciéndose público sus datos personales en ningún caso.

Si tiene alguna duda acerca de la confidencialidad de la encuesta, o considera de importancia aportar algún otro tipo de información, comuníquese con nosotros enviándonos un correo electrónico a david.romero@upm.es

Le rogamos que **responda a las cuestiones planteadas** ajustándose **al formato de respuesta dado**.

IMPORTANTE: No olvide enviar la encuesta al correo electrónico: david.romero@upm.es o bien por correo ordinario a la dirección:

Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos, Avda. Profesor Aranguren s/n. 28040 Madrid, a la atención del Profesor D. Alberto Camarero Orive.

Gracias por su participación.

EXPLICACIÓN PREVIA

El objetivo de la investigación es la obtención de una nueva propuesta metodológica para la evaluación del riesgo en instalaciones portuarias que permita evaluar el riesgo por separado asociado a diferentes amenazas, y simultáneamente evaluar la potencialidad del riesgo global en una instalación mediante el empleo de un método semi-cuantitativo, Para ello se han realizado encuestas al sector portuario, se han evaluado las estadísticas de seguridad en puertos españoles y se han considerado las metodologías actualmente en uso.

El indicador representa el riesgo simplificado de la instalación o terminal del puerto (m) asociado a una amenaza dada (i),

$$r_i^m = A_i \cdot V_i \cdot G_i$$

Siendo los **parámetros**:

A= amenaza

V= vulnerabilidad

G= gravedad (consecuencias)

Y el riesgo potencial de la instalación, que servirá para poder comparar la peligrosidad o el grado global de seguridad de una instalación, se expresa mediante la siguiente formulación:

$$R_T^K = \frac{\sum_{i=1}^n r_i^m}{n}$$

Donde n es el número de amenazas descritas para cada puerto (K), siendo su desarrollo:

$$r_1 = (P_T + T + I_s) \cdot (I_{ac} + I_{Lo} + I_{Ro}) \cdot (I_{RE} + I_{RH} + I_{RA} + I_{PS})$$

Dónde r_1 representa el riesgo derivado de una amenaza, que se descompone en los **índices siguientes**:

P_T=Riesgo intrínseco de la fachada. Se trata de valorar el riesgo general contra la seguridad, denominado "*riesgo intrínseco de la fachada*", es decir la probabilidad de amenaza para cada puerto, valorado en base a la disposición física del mismo en la costa española y al riesgo general que se comprueba que tiene cada instalación del Sistema Portuario en las estadísticas. La disposición del puerto en una fachada o en otra incide sensiblemente en los niveles generales de seguridad general ante posibles amenazas a la instalación.

T= Riesgo intrínseco de la terminal/instalación portuaria. Se trata de considerar el "*riesgo intrínseco del tipo de terminal o instalación*", es decir la probabilidad de amenaza que se asocia o define para cada tipo de terminal en función del tipo de mercancía que ésta mueve. Es evidente que la peligrosidad se

puede asociar, desde un punto de vista de la probabilidad de suceso, a cada tipo de terminal en virtud del tipo de instalaciones que esta posee y del tipo de actividad que en ella se desarrolla. Así pues, se definen diferentes niveles de amenaza para cada tipo de terminal; contenedores, pasajeros, graneles líquidos, graneles sólidos, etc. basándose en las características particulares de cada tipo de mercancía, zonas de servicios, accesos, edificios, etc.

I_s= Riesgo particularizado. Este índice considera el “*riesgo particular*” de ataque, es decir la probabilidad que se asocia o define para cada tipo de amenaza evaluada en base a las estadísticas de seguridad del puerto. Para ello se consideran las siguientes amenazas:

- Inmigración ilegal (polizones y tráfico ilegal de personas)
- Robo
- Sabotaje
- Ataque con explosivos/armas de fuego
- Ataque con armas químicas (bio-terrorismo)
- Conflictos laborales

I_{ac}= Índice de accesibilidad. Este índice se redefine, pues ya existía, si bien ahora trata de evaluar la vulnerabilidad de las instalaciones en base a la valoración de diferentes aspectos físicos y operativos, evaluándose para ello los siguientes aspectos:

- Características del cerramiento; altura y facilidad de acceso
- Sistema de control de accesos adecuados:
 - Lector de matrículas
 - Tarjetas de identificación personal
 - Sistema CCTV
 - Alarmas de intrusión,
 - Sensores de movimiento
 - Arcos detectores y scanner
- Experiencia del equipo de seguridad

I_{ro}= Índice de Relevancia Operativa. Este índice evalúa la importancia que tienen para la operación portuaria determinadas instalaciones o elementos cuya

paralización, en base a una amenaza dada, resultaría relevante para la misma. Un índice no exhaustivo de elementos podría ser el siguiente:

- Infraestructuras de comunicación interna; estructuras, túneles, vías férreas, etc.
- Sistemas de comunicación; telecomunicaciones, fibra óptica, etc.
- Redes de distribución: energía, electricidad, agua, etc.
- Equipos de manipulación de mercancías; grúas portuarias, grúas pórtico, maquinaria auxiliar, etc.
- Instalaciones de almacenamiento; terminales marítimas, tinglados, almacenes, silos, etc.

El parámetro G, Gravedad, se calcula considerando los denominados “Índices de Repercusión”, definidos en la *ROM 0.0: Procedimiento general y bases de cálculo, Criterios Generales*:

IRE= Repercusión económica. Valora la magnitud de las pérdidas económicas y el deterioro de los productos y servicios.

IRH= Repercusión a la vida humana. Se valora en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.

IRA= Repercusión ambiental. Se valora la degradación en el lugar o sus alrededores. En este caso se considerará el daño al sistema marino y a la calidad de las aguas por vertidos incontrolados o accidentales, o contaminación aérea debida a hidrocarburos

IPS= Repercusión pública y social. Valora la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

CUESTIONARIO. RONDA 1

1. ¿Añadiría usted coeficientes para mejorar la valoración de los parámetros propuestos?:

- ☐ a) Si, los añadiría, pues mejorarían el resultado de la evaluación.
- ☐ b) No, no son necesarios, los parámetros actuales (A, V y G) representan suficientemente bien cada elemento de la evaluación del riesgo.

2. En caso de disponer de coeficientes, ¿Cuántos consideraría y cuál sería, a su juicio, la función más adecuada para estos?:

- ☐ a) Consideraría 3 coeficientes, (p.e.: α , β , y γ). Su función sería la valoración de la influencia de los tres parámetros de forma conjunta.
- ☐ b) Consideraría 4 coeficientes (p.e.: α , β , γ y θ , número máximo de sub-parámetros definidos). Su función debería ser la valoración de la influencia de los tres parámetros en el conjunto de la evaluación de forma desagregada, asignando un coeficiente a cada sub-parámetro; α_1 , β_1 , γ_1 , α_2 , β_2 , γ_2 y α_3 , β_3 , γ_3 , θ .

ENCUESTA SOBRE VALORACIÓN DE COEFICIENTES EN LA EVALUACIÓN DEL RIESGO RONDA 2

Estimado colaborador,

Una vez obtenidas las respuestas de los expertos consultados les planteamos una segunda ronda de preguntas para completar la investigación.

Su opinión es de gran importancia para intentar mejorar la evaluación de riesgos, objetivo del estudio.

Asimismo, el resultado de estas encuestas será totalmente confidencial, no haciéndose público sus datos personales en ningún caso.

Si tiene alguna duda acerca de la confidencialidad de la encuesta, o considera de importancia aportar algún otro tipo de información, comuníquese con nosotros enviándonos un correo electrónico a david.romero@upm.es

Le rogamos que **responda a las cuestiones planteadas** ajustándose **al formato de respuesta dado**.

IMPORTANTE: No olvide enviar la encuesta al correo electrónico: david.romero@upm.es o bien por correo ordinario a la dirección:

Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos, Avda. Profesor Aranguren s/n. 28040 Madrid, a la atención del Profesor D. Alberto Camarero Orive.

Gracias por su participación.

CUESTIONARIO. RONDA 2

1. En base a los resultados de la ronda 1, y partiendo de la necesidad de los coeficientes y la función asignada a los coeficientes, ¿cómo los analizaría?

- ☐ a) Como elementos independientes entre si y del tipo de amenaza.
- ☐ b) En el contexto de cada parámetro, como elementos dependientes entre si y asignándoles un peso a cada uno en función de la influencia que el sub-parámetro al que afectan tiene para la amenaza que se evalúa.

2. Para finalizar, ¿cómo los valoraría?

- ☐ a) Asignándoles valores comprendidos entre 0-1, de forma que la suma de los mismos sea de valor 1.
- ☐ b) Asignándoles valores enteros comprendidos entre 1-10 para darle mayor incidencia a aquellos que resultan de mayor peso en la evaluación.

POLITÉCNICA

OBJETO

El objeto de la presente encuesta es contribuir a la mejora en la evaluación de riesgos potenciales para la seguridad en instalaciones portuarias a través de la opinión de expertos.

Durante esta investigación se han propuesto diferentes parámetros para la evaluación del riesgo en instalaciones portuarias y asociados a cada uno de ellos diferentes índices, así como la adopción de una serie de coeficientes que ponderan dichos índices. Estos índices se adoptaron como resultado de un primer análisis Delphi. Se trata ahora de definir la valoración de dichos coeficientes en función de su definición inicial.

La presente encuesta se realiza con el fin de obtener una opinión experta que permita valorar diferentes opciones que se plantean mediante un breve cuestionario.

La información obtenida se utilizará para la elaboración de una Tesis Doctoral de la Universidad Politécnica de Madrid. Dicho trabajo está dirigido por el Profesor D. Alberto Camarero Orive, de la Escuela de Ingenieros de Caminos, Canales y Puertos de la Universidad Politécnica de Madrid.

Agradecerle de antemano el tiempo dedicado para completar esta encuesta necesaria para la elaboración del estudio. Su opinión es de gran importancia para intentar mejorar la evaluación de riesgos, objetivo del estudio.

Asimismo, el resultado de estas encuestas será totalmente confidencial, no haciéndose público sus datos personales en ningún caso.

Si tiene alguna duda acerca de la confidencialidad de la encuesta, o considera de importancia aportar algún otro tipo de información, comuníquese con nosotros enviándonos un correo electrónico a david.romero@upm.es

Le rogamos que **responda a las cuestiones planteadas** ajustándose **al formato de respuesta dado**.

IMPORTANTE: No olvide enviar la encuesta al correo electrónico: david.romero@upm.es o bien por correo ordinario a la dirección:

Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos, Avda. Profesor Aranguren s/n. 28040 Madrid, a la atención del Profesor D. Alberto Camarero Orive.

Gracias por su participación

EXPLICACIÓN PREVIA

El objetivo de la investigación es la obtención de una **nueva propuesta metodológica para la evaluación del riesgo** (security) **en instalaciones portuarias** que permita evaluar este asociado a diferentes amenazas, y simultáneamente evaluar la potencialidad del riesgo global en una instalación mediante el empleo de un método semi-cuantitativo, Para ello se han realizado encuestas al sector portuario, se han evaluado las estadísticas de seguridad en puertos españoles y se han considerado las metodologías actualmente en uso. A continuación se resumen la propuesta metodológica para la evaluación del riesgo.

El indicador representa el riesgo simplificado de la instalación o terminal del puerto (m) asociado a una amenaza dada (i),

$$r_i^m = A_i \cdot V_i \cdot G_i \quad (1)$$

Siendo los **parámetros**:

A_i = amenaza

V_i = vulnerabilidad

G_i = gravedad (consecuencias)

Y el riesgo potencial de la instalación, que servirá para poder comparar la peligrosidad o el grado global de seguridad de una instalación, se expresa mediante la siguiente formulación:

$$R_T^K = \frac{\sum_{i=1}^n r_i^m}{n} \quad (2)$$

Donde **n es el número de amenazas descritas** en el puerto (K) siendo su desarrollo:

$$r_1 = (P_T + T + I_s) \cdot (I_{ac} + I_{Lo} + I_{Ro}) \cdot (I_{RE} + I_{RH} + I_{RA} + I_{PS}) \quad (3)$$

A estos índices se les afecta de unos **coeficientes α , β , γ , θ** (objeto de esta encuesta), resultando:

$$r_1 = (\alpha_1 \cdot P_T + \beta_1 \cdot T + \gamma_1 \cdot I_s) \cdot (\alpha_2 \cdot I_{ac} + \beta_2 \cdot I_{Lo} + \gamma_2 \cdot I_{Ro}) \cdot (\alpha_3 \cdot I_{RE} + \beta_3 \cdot I_{RH} + \gamma_3 \cdot I_{RA} + \theta \cdot I_{PS}) \quad (4)$$

Dónde r_1 representa el riesgo asociado a una amenaza, que se descompone en los **índices siguientes** según el parámetro evaluado:

Amenaza

P_T =Riesgo intrínseco de la fachada. Se trata de valorar el riesgo general contra la seguridad, denominado “*riesgo intrínseco de la fachada*”, es decir la probabilidad de

amenaza para cada puerto, valorado en base a la disposición física del mismo en la costa española y al riesgo general que tiene cada instalación del Sistema Portuario en las estadísticas.

T= Riesgo intrínseco de la terminal/instalación portuaria. Se trata de considerar el “*riesgo intrínseco del tipo de terminal o instalación*”, es decir la probabilidad de amenaza que se asocia o define para cada tipo de terminal en función del tipo de mercancía que ésta mueve.

I_S = Riesgo particularizado. Este índice considera el “*riesgo particular*” de ataque, es decir la probabilidad que se define para cada tipo de amenaza, evaluada en base a las estadísticas de seguridad del puerto. Para ello se consideran las siguientes amenazas:

- Inmigración ilegal (polizones y tráfico ilegal de personas)
- Robo
- Sabotaje
- Ataque con explosivos/armas de fuego
- Ataque con armas químicas (bio-terrorismo)
- Conflictos laborales

Vulnerabilidad

I_{ac} = Índice de accesibilidad. Este índice se redefine, pues ya existía, si bien ahora trata de evaluar la vulnerabilidad de las instalaciones en base a la valoración de diferentes aspectos físicos y operativos, evaluándose para ello los siguientes aspectos:

- Características del cerramiento; altura y facilidad de acceso
- Sistema de control de accesos adecuados:
- Experiencia del equipo de seguridad

I_{Lo} = Índice layout. Este índice evalúa la influencia que tiene en la seguridad de un elemento o instalación su disposición próxima a los accesos al puerto (próximo al exterior), así como la proximidad a otras instalaciones de alto riesgo de ataque.

I_{Ro} = Índice de Relevancia Operativa. Este índice evalúa la importancia que tienen para la operación portuaria determinadas instalaciones o elementos cuya paralización, en base a una amenaza dada, resultaría relevante para la misma. Un índice no exhaustivo de elementos podría ser el siguiente:

- Infraestructuras de comunicación interna; estructuras, túneles, vías férreas, etc.
- Sistemas de comunicación; telecomunicaciones, fibra óptica, etc.
- Redes de distribución: energía, electricidad, agua, etc.

- Equipos de manipulación de mercancías; grúas portuarias, grúas pórtico, maquinaria auxiliar, etc.
- Instalaciones de almacenamiento; terminales marítimas, tinglados, almacenes, silos, etc.

Gravedad

IRE= Repercusión económica. Valora la magnitud de las pérdidas económicas y el deterioro de los productos y servicios.

IRH= Repercusión a la vida humana. Se valora en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.

IRA= Repercusión ambiental. Se valora la degradación en el lugar o sus alrededores. En este caso se considerará el daño al sistema marino y a la calidad de las aguas por vertidos incontrolados o accidentales, o contaminación aérea debida a hidrocarburos

IPS= Repercusión pública y social. Valora la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

Los coeficientes propuestos, α , β , γ , θ , **objeto de esta encuesta**, se analizan valorándose **en función exclusiva del tipo de amenaza evaluada**; sabotaje, robo, ataque con armas, etc., **y por tanto no se ven condicionados por el tipo de instalación (terminal) o el puerto del que se trate.**

Asimismo **se analizan en el contexto de cada parámetro** (bien sea amenaza, vulnerabilidad o gravedad), **como elementos dependientes entre si y asignándoles un peso o valor a cada uno en función de la influencia que el índice al que afectan tiene para la amenaza que se evalúa** (p.e. en la escenario de amenaza: *Sabotaje de las grúas portacontenedores*, el índice de relevancia operativa, I_{Ro} , puede tener un peso mayor que el de Layout, I_{Lo} , o que la accesibilidad, I_{ac} , en el análisis de la vulnerabilidad).

Los coeficientes se valoran asignándoles valores comprendidos entre 0-1, siendo la suma de los mismos sea de valor 1 en cada parámetro, de forma que;

$$\alpha_1 + \beta_1 + \gamma_1 = 1 \qquad \alpha_2 + \beta_2 + \gamma_2 = 1 \qquad \alpha_3 + \beta_3 + \gamma_3 + \theta = 1 \qquad (5)$$

CUESTIONARIO

En función de las amenazas consideradas definidas en la página 3, y de los índices propuestos, ¿qué valores daría a cada uno de los coeficientes descritos en la ecuación (5) y asignados a dichos índices (ver ecuación 4), teniendo en cuenta que la valoración se realiza exclusivamente en función del peso que, a su juicio, debe tener cada uno de los índices (PT, T, I_S..., etc.) en cada tipo de amenaza planteada?

Inmigración ilegal

 $\alpha_1 =$ $\alpha_2 =$ $\alpha_3 =$ $\theta =$ $\beta_1 =$ $\beta_2 =$ $\beta_3 =$ $\gamma_1 =$ $\gamma_2 =$ $\gamma_3 =$

Observaciones:

Robo

 $\alpha_1 =$ $\alpha_2 =$ $\alpha_3 =$ $\theta =$ $\beta_1 =$ $\beta_2 =$ $\beta_3 =$ $\gamma_1 =$ $\gamma_2 =$ $\gamma_3 =$

Observaciones:

Sabotaje

 $\alpha_1 =$ $\alpha_2 =$ $\alpha_3 =$ $\theta =$ $\beta_1 =$ $\beta_2 =$ $\beta_3 =$ $\gamma_1 =$ $\gamma_2 =$ $\gamma_3 =$

Observaciones:

Ataque con explosivos/armas de fuego

$\alpha_1 =$

$\alpha_2 =$

$\alpha_3 =$

$\theta =$

$\beta_1 =$

$\beta_2 =$

$\beta_3 =$

$\gamma_1 =$

$\gamma_2 =$

$\gamma_3 =$

Observaciones:

Ataque con armas químicas (bio-terrorismo)

$\alpha_1 =$

$\alpha_2 =$

$\alpha_3 =$

$\theta =$

$\beta_1 =$

$\beta_2 =$

$\beta_3 =$

$\gamma_1 =$

$\gamma_2 =$

$\gamma_3 =$

Observaciones:

Conflictos laborales

$\alpha_1 =$

$\alpha_2 =$

$\alpha_3 =$

$\theta =$

$\beta_1 =$

$\beta_2 =$

$\beta_3 =$

$\gamma_1 =$

$\gamma_2 =$

$\gamma_3 =$

Observaciones:

POLITÉCNICA

UNIVERSIDAD POLITÉCNICA DE MADRID
E.T.S DE INGENIEROS DE CAMINOS CANALES Y PUERTOS
DEPARTAMENTO DE INGENIERÍA CIVIL. TRANSPORTE Y TERRITORIO

POLITÉCNICA

OBJETO

Como continuación a la primera ronda de encuestas realizada, le envío adjunto los valores medios obtenidos para cada uno de los coeficientes descritos.

Asimismo le ruego revise dichos resultados y si lo estima oportuno modifique sus valoraciones en base a las propuestas en la primera ronda de encuestas en las hojas siguientes.

Agradecerle de antemano el tiempo dedicado para completar esta encuesta necesaria para la elaboración del estudio. Su opinión es de gran importancia para intentar mejorar la evaluación de riesgos, objetivo del estudio.

Asimismo, el resultado de estas encuestas será totalmente confidencial, no haciéndose público sus datos personales en ningún caso.

Si tiene alguna duda acerca de la confidencialidad de la encuesta, o considera de importancia aportar algún otro tipo de información, comuníquese con nosotros enviándonos un correo electrónico a david.romero@upm.es

Le rogamos que **responda a las cuestiones planteadas** ajustándose **al formato de respuesta dado**.

IMPORTANTE: No olvide enviar la encuesta al correo electrónico: david.romero@upm.es o bien por correo ordinario a la dirección:

Escuela Técnica Superior de Ingenieros de Caminos, Canales y Puertos, Avda. Profesor Aranguren s/n. 28040 Madrid, a la atención del Profesor D. Alberto Camarero Orive.

Gracias por su participación

RESULTADOS

Inmigr. Ilegal		VALOR MEDIO
PT	$\alpha 1$	0,44
T	$\beta 1$	0,23
IS	$\gamma 1$	0,34
Iac	$\alpha 2$	0,60
Ilo	$\beta 2$	0,27
Iro	$\gamma 2$	0,13
IRE	$\alpha 3$	0,18
IRH	$\beta 3$	0,32
IRA	$\gamma 3$	0,01
IPS	θ	0,49

Ataque explo/armas		VALOR MEDIO
PT	$\alpha 1$	0,29
T	$\beta 1$	0,41
IS	$\gamma 1$	0,30
Iac	$\alpha 2$	0,44
Ilo	$\beta 2$	0,26
Iro	$\gamma 2$	0,31
IRE	$\alpha 3$	0,24
IRH	$\beta 3$	0,34
IRA	$\gamma 3$	0,12
IPS	θ	0,30

Robo		VALOR MEDIO
PT	$\alpha 1$	0,21
T	$\beta 1$	0,43
IS	$\gamma 1$	0,35
Iac	$\alpha 2$	0,58
Ilo	$\beta 2$	0,25
Iro	$\gamma 2$	0,16
IRE	$\alpha 3$	0,53
IRH	$\beta 3$	0,10
IRA	$\gamma 3$	0,06
IPS	θ	0,32

Ataque armas quimicas		VALOR MEDIO
PT	$\alpha 1$	0,32
T	$\beta 1$	0,39
IS	$\gamma 1$	0,28
Iac	$\alpha 2$	0,45
Ilo	$\beta 2$	0,25
Iro	$\gamma 2$	0,29
IRE	$\alpha 3$	0,18
IRH	$\beta 3$	0,31
IRA	$\gamma 3$	0,19
IPS	θ	0,32

Sabotaje		VALOR MEDIO
PT	$\alpha 1$	0,26
T	$\beta 1$	0,41
IS	$\gamma 1$	0,33
Iac	$\alpha 2$	0,38
Ilo	$\beta 2$	0,21
Iro	$\gamma 2$	0,42
IRE	$\alpha 3$	0,38
IRH	$\beta 3$	0,21
IRA	$\gamma 3$	0,15
IPS	θ	0,28

Conflic. Laborales		VALOR MEDIO
PT	$\alpha 1$	0,27
T	$\beta 1$	0,30
IS	$\gamma 1$	0,42
Iac	$\alpha 2$	0,24
Ilo	$\beta 2$	0,19
Iro	$\gamma 2$	0,57
IRE	$\alpha 3$	0,45
IRH	$\beta 3$	0,10
IRA	$\gamma 3$	0,08
IPS	θ	0,38

CUESTIONARIO

Inmigración ilegal

$\alpha_1 =$

$\alpha_2 =$

$\alpha_3 =$

$\theta =$

$\beta_1 =$

$\beta_2 =$

$\beta_3 =$

$\gamma_1 =$

$\gamma_2 =$

$\gamma_3 =$

Observaciones:

Robo

$\alpha_1 =$

$\alpha_2 =$

$\alpha_3 =$

$\theta =$

$\beta_1 =$

$\beta_2 =$

$\beta_3 =$

$\gamma_1 =$

$\gamma_2 =$

$\gamma_3 =$

Observaciones:

Sabotaje

$\alpha_1 =$

$\alpha_2 =$

$\alpha_3 =$

$\theta =$

$\beta_1 =$

$\beta_2 =$

$\beta_3 =$

$\gamma_1 =$

$\gamma_2 =$

$\gamma_3 =$

Observaciones:

Ataque con explosivos/armas de fuego

$\alpha_1 =$

$\alpha_2 =$

$\alpha_3 =$

$\theta =$

$\beta_1 =$

$\beta_2 =$

$\beta_3 =$

$\gamma_1 =$

$\gamma_2 =$

$\gamma_3 =$

Observaciones:

Ataque con armas químicas (bio-terrorismo)

$\alpha_1 =$

$\alpha_2 =$

$\alpha_3 =$

$\theta =$

$\beta_1 =$

$\beta_2 =$

$\beta_3 =$

$\gamma_1 =$

$\gamma_2 =$

$\gamma_3 =$

Observaciones:

Conflictos laborales

$\alpha_1 =$

$\alpha_2 =$

$\alpha_3 =$

$\theta =$

$\beta_1 =$

$\beta_2 =$

$\beta_3 =$

$\gamma_1 =$

$\gamma_2 =$

$\gamma_3 =$

Observaciones: