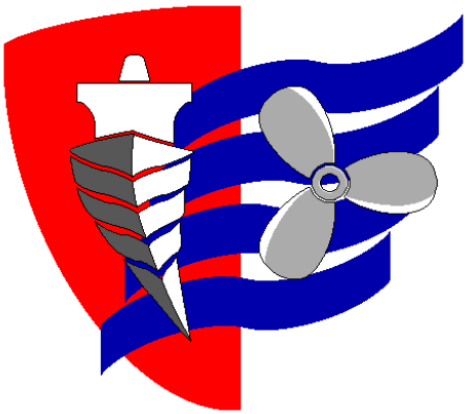
ESCUELA TÉCNICA SUPERIOR DE NÁUTICA

UNIVERSIDAD DE CANTABRIA



Trabajo Fin de Grado

PROPUESTA PARA LA PROTECCIÓN DE LA NUEVA TERMINAL DE PASAJEROS DEL PUERTO DE SANTANDER

(Proposal for the security of the new passenger terminal building of the Port of Santander)

Para acceder al Título de Grado en

INGENIERÍA NÁUTICA Y TRANSPORTE MARÍTIMO

Autor: Goio Atxirika

Director: Andrés R. Ortega Piris

Marzo-2015

ÍNDICE:

ESCUELA TÉCNICA SUPERIOR DE NÁUTICA
UNIVERSIDAD DE CANTABRIA

Trabajo Fin de Grado

PROPUESTA PARA LA PROTECCIÓN DE LA NUEVA TERMINAL DE PASAJEROS DEL PUERTO DE SANTANDER

(Proposal for the security of the new passenger terminal building of the Port of Santander)

Para acceder al Título de Grado en

INGENIERÍA NÁUTICA Y TRANSPORTE MARÍTIMO

Marzo - 2015

RESUMEN:

La finalidad de este documento es la de realizar una propuesta que desarrolle la protección de una hipotética nueva Estación Marítima que nacería como consecuencia de las obras de remodelación de la actual, y que se destinaría igualmente al transporte de pasajeros y carga acompañada, dando servicio a buques de crucero y transbordadores tal como se recoge en el Plan Director del Puerto de Santander 2012-2022. En él, se tratan los siguientes contenidos:

1) ***Introducción:***

i) Se contextualiza la situación presente de la seguridad marítima y se plantean los principales riesgos que a nivel general amenazan el negocio marítimo, poniendo de manifiesto la falta de control que ha caracterizado históricamente al dominio marítimo:

- La piratería.
- El robo armado y el terrorismo.
- La proliferación de armas.
- El tráfico de personas y drogas.
- La diseminación de enfermedades infecciosas.
- La degradación ambiental.

Tras los atentados terroristas del 11-S se establecen políticas concretas sobre protección marítima y se aprueban enmiendas al convenio SOLAS, creándose el capítulo XI-2 (medidas especiales para la mejora de la seguridad marítima), y el código PBIP, que proporciona un marco estandarizado consistente, al objeto de evaluar el riesgo, a la vez que facilita la modificación de las medidas de protección de buques e instalaciones, para hacer frente a niveles mayores de amenaza.

La implantación de las medidas de protección conlleva una serie de pasos y esfuerzos, tales como la realización de evaluaciones de riesgos, desarrollo de planes de protección y la programación de ejercicios, a la vez que involucra a todos los actores que intervienen en el tráfico marítimo internacional.

La Comunidad Europea, como compromisaria del convenio SOLAS, adopta una Estrategia de Seguridad Marítima al objeto de proporcionar un marco común que asegure el desarrollo coherente de las políticas nacionales y europeas, y una respuesta conjunta a las amenazas en el ámbito marítimo; así, desarrolla el

reglamento CE 725/2004 que sienta las bases para la interpretación y aplicación armonizadas de las enmiendas al convenio SOLAS por los países integrantes, y aprueba la directiva 2005/65/CE sobre mejora de la protección portuaria.

La trasposición de esas normas al ordenamiento jurídico español se refleja en el Real Decreto 1617/2007 en el que se marcan pautas concretas para el desarrollo de la seguridad en buques e instalaciones marítimas.

ii) Se trata la complejidad de las instalaciones portuarias previstas para dar servicio a pasajeros, sus características principales y las bases para su protección:

- Designación de responsables.
- Confección de Planes de Protección.
- Realización de evaluaciones de seguridad.
- Propuesta de medidas correctoras a las no conformidades observadas.
- Implantación de medidas correctoras.
- Verificación de la efectividad de las medidas correctoras.
- Formación del personal.
- Labores de inteligencia en el ámbito portuario.
- Auditorías de seguridad.
- Coordinación de todas las organizaciones públicas y privadas que intervienen en el negocio marítimo.

iii) Se recogen los principales actos de interferencia ilícita realizados en buques de crucero y transbordadores, y se citan algunas vulnerabilidades propias de la industria marítima que podrían ser explotadas por grupos criminales para materializar sus ataques.

2) Objeto del estudio:

Partiendo del esquema de una Estación Marítima ficticia que sustituya a la actual, se dotará a la instalación portuaria de todos los medios de seguridad necesarios para dar cumplimiento a la normativa aplicable en materia de protección marítima y se desarrollará el Plan de Protección de la Estación Marítima.

3) Descripción de las instalaciones:

- Edificio terminal de pasajeros:

Se propone un edificio terminal de pasajeros de dos plantas, destinándose la superior a facilitar las salidas de pasajeros (facturación de equipajes, control de seguridad y acceso a salas de embarque, a pasarelas de embarque o vías peatonales, y al buque) y la inferior a dar servicio durante las llegadas (salas de recogida de equipajes, control de documentación y aduana).

A la entrada del edificio terminal, en la planta superior, se accede al vestíbulo de salidas en el que se realiza la facturación de equipajes de cabina, de modo que los pasajeros únicamente portan sus equipajes de mano en el momento de acceder a la zona de embarques.

Tras atravesar el control de seguridad, dispuesto con todos los medios necesarios para asegurar que ninguna persona porta armas o artículos prohibidos, se accede a la zona restringida de seguridad.

El equipaje facturado (equipaje de cabina) es sometido a una inspección de seguridad por niveles, antes de ser embarcado. Esta modalidad de inspección garantiza razonablemente que no se introducen armas no autorizadas, ni sustancias explosivas o incendiarias destinadas a ser embarcadas.

- Perímetro de seguridad en la zona de tierra:

Las instalaciones de la Estación Marítima están delimitadas por un perímetro exterior que aísla la zona de operaciones y la interfaz buque/puerto, de la zona pública.

La zona de atraque de los buques y las superficies adyacentes se encuentran confinadas tras un cerramiento perimetral que, al igual que las zonas restringidas del edificio terminal, forman parte de un área estéril; por lo cual todas las personas, vehículos, carga, correo y suministros que accedan a ella deben ser objeto de medidas de control.

Las casetas de acceso y de salida disponen de medios para realizar el control de documentación, las inspecciones de seguridad y los controles fiscales.

- Perímetro de seguridad en la zona marítima:

Mediante la colocación de barreras flotantes, capaces de detener embarcaciones pequeñas, se delimita un perímetro de seguridad en el que se controla a todas las embarcaciones que pretenden acceder, a la vez que sirve de elemento disuasorio, facilitando la labor del servicio de seguridad.

4) Medios técnicos de protección:

- Cerramiento perimetral: establece una frontera que sirve como elemento disuasorio al objeto de evitar la intrusión y la introducción de artículos u objetos en las zonas restringidas.
- Puertas: una serie de puertas de interés se conectarán al sistema de seguridad para que puedan realizarse operaciones remotas sobre las mismas (apertura, cierre, bloqueo, desbloqueo) desde los puestos de mando del sistema de seguridad.
- Barreras flotantes: delimitan la zona marítima a proteger y sirven de elemento disuasorio ante ataques con embarcaciones pequeñas.
- Alumbrado de seguridad: cuando se emplea adecuadamente, la iluminación desalienta la actividad criminal, potencia las labores de vigilancia y reduce el temor en los usuarios legítimos de las instalaciones.
- Sistema de gestión de la seguridad: en una solución escalable, y gestionada mediante módulos específicos de software, permite controlar los siguientes subsistemas:
    - Sistema de gestión y control.
    - Sistema de CCTV.
    - Sistema de almacenamiento de datos.
    - Sistema de control de accesos.
    - Sistema de iluminación.

  Tareas de funcionamiento básicas:
    - Visualización de cámaras en tiempo real.
    - Gestión de alarmas y eventos.
    - Gestión de grabaciones.
    - Gestión de control de accesos.
    - Atención a interfonos.

- Administración (configuración de zonas, permisos, privilegios, eventos, preposicionamiento de cámaras, etc.).
- Gestión de iluminación de seguridad.

- Señalización: Sirve de elemento disuasorio e informativo, en prevención de la intrusión.

5) Medios técnicos de inspección:

- Arcos detectores de metales: son capaces de detectar e indicar mediante señales de alarma la presencia de todo tipo masas metálicas.
- Detectores de metales portátiles: sensibles a los metales, permite al personal de seguridad ayudar a resolver las alarmas metálicas generadas en los arcos detectores de metales.
- Detectores de metales en calzado: son un medio de inspección adicional que permiten detectar la presencia de objetos metálicos en el calzado.
- Equipos de RX: permiten inspeccionar equipajes proporcionando imágenes de alta resolución y calidad de su interior.
- Equipos de detección de explosivos: son equipos capaces de detectar de manera automática, y así indicarlo por medio de una alarma, sustancias explosivas contenidas en los bultos, independientemente del material del que estén fabricados.
- Sistemas de tomografía computerizada: realizan un barrido completo de Rayos X, desde diferentes ángulos, proporcionando una visión excelente del interior de los bultos inspeccionados, en tres dimensiones.
- Equipos de inspección de líquidos explosivos: sirven para inspeccionar líquidos, aerosoles y geles permitiendo la detección de explosivos.
- Equipos de detección de trazas de drogas y explosivos: permiten detectar restos de explosivos y/o drogas presentes en las superficies de los objetos.

6) Perros:

Los perros se han mostrado un apoyo con capacidades extraordinarias en la detección de todo tipo de artículos y su eficacia es comparable a la de los equipos de inspección más desarrollados, también pueden realizar labores de guarda.

7) Plan de Protección de la Estación Marítima:

Se trata de un documento confidencial realizado a instancias de la entidad gestora de la Estación Marítima al objeto de proporcionar a la instalación portuaria los estándares de calidad apropiados para garantizar la seguridad de todos los usuarios y trabajadores, permitir la continuidad de las operaciones y minimizar la posibilidad de que se cometan actos ilícitos.

Su alcance lo hace efectivo en el interior del edificio terminal de pasajeros, la zona delimitada por el cerramiento perimetral terrestre y la zona marítima controlada. Este Plan de Protección deberá integrarse en el Plan de Protección del Puerto de Santander.

En él se determina la estructura del Sistema de Protección de la Estación Marítima y se relacionan los recursos humanos, organizativos y materiales disponibles:

- Se asignan cargos, funciones y responsabilidades a las personas encargadas de la protección; se indican las cualificaciones requeridas para ocupar dichos puestos.
- Se describen detalladamente los recursos organizativos (creación de zonas de seguridad, puntos de acceso, recorridos, definición de zonas de acopio y almacenamiento de artículos, procedimientos, auditoría) que garanticen la correcta aplicación de las medidas de protección.
- Se relacionan y denominan los medios técnicos de protección e inspección, y se indica su ubicación en la infraestructura.

El Plan de Protección se complementa con una Evaluación de Riesgos de Seguridad, que trata de en la que se tratan obtener valoraciones de los impactos que produciría la hipotética materialización de ciertos supuestos concretos de amenazas a la seguridad. Este proceso sirve para detectar vulnerabilidades, no conformidades y oportunidades de mejora, plantear medidas correctoras, implantarlas y evaluar su efectividad.

ABSTRACT:

The aim of this document is to propose the development of the security measures at an hypothetical new Sea Terminal which would be set up as a consequence of the renewal of the present one, also intended to serve to the transport of passengers and accompanying cargo, providing services to cruise vessels and ferries, as stated in the Director Plan of the Port of Santander 2012-2022. In order to achieve this, the following issues are addressed:

1) Introduction:

i) The present situation regarding the maritime security is contextualized and the main global risks threatening the maritime business posed, highlighting the lack of control which has historically characterized the maritime domain:

- Piracy.
- Armed robbery and terrorism.
- Proliferation of weapons.
- Smuggling of persons and drugs.
- Dissemination of infectious diseases.
- Environmental degradation.

In the aftermath of the 11 – S attacks, specific policies on maritime security were introduced and amends to the SOLAS conventions are approved, developing the Chapter XI-2 (special measures for the enhancement of the maritime security and the ISPS Code, providing a consistent standardized frame with a view to assess the risk, facilitating the change of the security measures in vessels and infrastructures, in order to address higher levels of threat).

The implementation of the security measures involves several stages and efforts such as undertaking security assessments, developing security plans and establishing training and drill programs, involving every agent in the international maritime trafficking.

The European Community, as a stakeholder in the SOLAS Convention, adopted a Maritime Security Strategy to provide a common framework in order to ensure the coherent development of national and European policies and a common response to the maritime threats; thus, the Regulation EC 725/2004, that states the basis for harmonized interpretation and application of amendments to the SOLAS Convention

by the stakeholders, is developed and the Directive 2005/65/CE, on maritime security enhancement, approved.

The transposition of these regulations to the Spanish legal system takes place in the Royal Decree 1617/2007, in which, particular guidelines are established in the development of the security of ships and maritime facilities.

ii) The complexity of port facilities provided to serve passengers, their main features and the basis for their security is treated.

- Appointment of persons with responsibilities.
- Development of security plans.
- Security assessments.
- Proposal of corrective measures to the findings of non-compliance.
- Implementation of corrective measures.
- Verification of the effectiveness of corrective action.
- Personal training.
- Intelligence gathering operations in the port environment.
- Security audits.
- Coordination with every public and private organization taking part in the maritime business.

iii) The main actions of unlawful interference against cruise ships and ferries are issued and some vulnerabilities of the maritime industry, which could be exploited by terrorist groups to make their attacks, are listed.

2) Object of the study:

Starting with the draft of a fictitious Sea Terminal which will replace the present one, the infrastructure will be provided with all the necessary means to comply to maritime security regulations, and the Sea Terminal Security Plan will be developed.

3) Description of facilities:

- Passenger terminal building:

A two storey passenger terminal building is proposed, the upper one intended to allow the departure of passengers (baggage check-in, security control and access to boarding lounges, fingers or walkways, and to the vessel), and the lower one to provide services to the arriving vessels.

At the entrance of the terminal building, access is provided to the departure hall, where cabin baggage is checked in; thus, the passengers only hold their hand baggage upon entry into the embarkation areas.

After passing through the security control, which is provided with all the necessary means to guarantee that no person smuggles weapons or forbidden articles, access to the restricted area is granted.

The checked in baggage (cabin baggage) is screened through several levels, prior to being loaded on board. This screening method reasonably guarantees that no unauthorized weapons, explosive or incendiary substances are introduced to be boarded.

- Security perimeter on the land area:

The facilities of the Maritime Station are limited by a perimeter that aisles the operations areas and the vessel/port interface, from de public area. The berthing area and the adjacent surfaces are confined behind a perimeter fencing which forms part of a sterile area, just the same as the restricted areas inside the terminal building; because of this, every person, vehicle, cargo, mail and supplies entering must be subject to control measures.

- Security perimeter on the maritime area:

By means of the installation of floating barriers, able to stop small crafts, a security perimeter is established where every vessel intending to enter is subject to security controls; simultaneously serving as a deterrent, reinforcing the work of the security service.

4) Technical security means:

- Perimeter fencing: establishes a boundary that serves as a element in order to avoid the intrusion and the introduction of articles to the restricted areas.
- Doors and gates: several doors and gates will be connected to the security system so as to enable remote operations (opening, closure, locking, unlocking) from the operating positions.
- Floating barriers: establish the limit of the maritime area to protect and serve as a deterrent element to attacks by small crafts.
- Security lighting: when adequately employed, the lighting discourages criminal activity, enhances the monitoring tasks and reduces the fear of legitimate facilities users.
- Security management system: in a scalable solution, and managed under specific software modules, allows the control of the following subsystems:
    - Management and control system.
    - TVCC system.
    - Data store system.
    - Access control system.
    - Lighting system.

  Basic operations:
    - Real time TVCC visualization.
    - Alarms and events management.
    - Video recording management.
    - Access control management.
    - Attention to interphones.
    - Administration (zone configuration, allowances, privileges, events, camera prepositioning …)
    - Security lighting management.

5) Technical screening means:

- Walk through metal detectors: they are able to detect metallic bodies, and indicate their positions, activating alarm signals.
- Hand held metal detectors: they are sensitive to metals; they allow the security staff to help solving metallic alarms generated in the metal detector arches.
- Shoe analyzers: provide supplementary screening, allowing the detection of metallic bodies in footwear.
- X-ray equipment: allows baggage screening providing high resolution and quality images of their interior.
- Explosive detection systems (EDS): these systems are able to automatically detect, and thus indicate by activating an alarm signal, explosive substances contained within cases, independently of the material with which they are built.
- Computerized tomography systems (CTX): these make a full X-ray scan of the objects, from different angles, offering an excellent three dimensional vision of their interior.
- Liquid explosive detection devices: they are used to inspect liquids, sprays and gels allowing the detection of explosives.
- Drug and explosive trace detection equipment: these apparatuses are able to detect traces of explosives and/or drugs on the surface of objects.

6) Dogs:

Dogs are proved means of security support with extraordinary skills in the detection of all kinds of articles; their effectiveness is comparable to that of most modern equipment; they can also carry out guard duties.

7) Sea Terminal Security Plan:

This is a restricted document developed on behalf of the managing body of the Sea Terminal, in order to provide the port facility with the appropriate quality security standards to guarantee the security of every user and worker, allowing continuity of operations and minimizing the possibility of illicit acts.

Its scope makes it effective in the interior of the passenger terminal building, the area limited by the terrestrial perimeter fencing and the maritime controlled area.

This Security Plan must get integrated in the Santander Port Security Plan.

It states the structure of the Security System of the Sea Terminal and lists the human, organizational and material resources available:

- Positions, functions and responsibilities of the security staff are assigned; the qualifications required to occupy those positions are indicated.
- Detailed description of the organizational resources (creation of security areas, access points, routes, designation of areas for stores, procedures, internal audits), to guarantee the proper application of the protective measures, is given.
- Technical security and screening means are related and named, indicating their position within the infrastructure.

The Security Plan is complemented by a Security Assessment that attempts to obtain values for the impacts that the hypothetical materialization of some particular security threat scenarios would cause. This process serves to detect vulnerabilities, findings of non-compliance, and improvement opportunities, pose corrective measures, implement them and assess their effectiveness.

PALABRAS CLAVE / KEY WORDS:

- Estrategia de Seguridad Marítima / *Maritime Security Strategy*
- Acto Ilícito Deliberado / *Deliberate Unlawful Act*
- Plan de Protección de Instalación Portuaria / *Port Facility Security Plan*
- Declaración de Protección Marítima / *Declaration of Security (DOS)*
- Evaluación de la Protección / *Security Assessment*
- Procedimientos de Seguridad / *SecurityProcedures*

1. PRIMERA PARTE: PLANTEAMIENTO Y OBJETIVO DEL TRABAJO

1.1- INTRODUCCIÓN

La globalización es un fenómeno que se caracteriza por tener múltiples dimensiones, facilitando el libre movimiento de las personas, el desarrollo y la expansión de la tecnología, el conocimiento, el comercio, la inversión y los flujos de capital privado y, con todo ello, la interdependencia. Al tiempo que se crean posibilidades reales de lograr la prosperidad económica, la paz y la libertad, surgen fuerzas de fragmentación social que derivan en brotes de violencia y conflicto, resultando en amenazas dirigidas hacia sistemas críticos, como son los de comunicaciones, transportes, energéticos y bancarios.

El transporte marítimo, como pilar fundamental del comercio mundial, constituye un evidente objetivo potencial ante amenazas tales como la piratería, el robo armado y el terrorismo, a la vez que sirve a fines como la proliferación de armas, el tráfico de personas y drogas, la diseminación de enfermedades infecciosas y la degradación ambiental. La falta de control que ha caracterizado históricamente al dominio marítimo, la mayor parte del cual está formado por aguas internacionales, ha favorecido la comisión de dichos actos ilícitos (1).

Los atentados del 11-S marcaron un hito en la seguridad del transporte mundial, poniendo de manifiesto su vulnerabilidad, y los actores nacionales e internacionales con competencias reguladoras y de control establecieron políticas concretas sobre protección, que en el ámbito marítimo internacional se formalizaron, en primera instancia, mediante la aprobación de diversas enmiendas al Convenio para la Seguridad de la Vida en la Mar (SOLAS) dirigidas a intensificar la seguridad física a bordo de los buques y en las interfaces buque-puerto, al objeto de prevenir los actos ilícitos que amenazan la seguridad de los buques, así como sus pasajes, cargamentos y tripulaciones: entre otras medidas, la Conferencia Diplomática de la Organización Marítima Internacional creó y aprobó el capítulo XI-2 (medidas especiales para la mejora de la seguridad marítima), con el requerimiento, a los Estados miembros, de adoptar el Código Internacional para la Protección de los Buques e Instalaciones Portuarias (Código PBIP).

El código PBIP proporciona un marco estandarizado y consistente, al objeto de evaluar el riesgo, a la vez que permite a los gobiernos contrarrestar los cambios ante

diferentes niveles de amenaza o alerta, mediante alteraciones en las medidas de protección de buques e instalaciones.

1.1-1. IMPLANTACIÓN DEL CÓDIGO PBIP

La implantación del código PBIP conlleva una serie de pasos y esfuerzos, tales como la realización de evaluaciones de riesgos derivados de la seguridad física, el desarrollo de planes de seguridad, la designación de oficiales de seguridad y la programación de ejercicios y actividades formativas, en materia de seguridad física; involucra a gobiernos, administraciones locales, autoridades portuarias, compañías marítimas y, en general, a todos los actores del tráfico marítimo internacional (1).

Entre otras medidas, se requiere que los puertos y los buques tengan personal adecuadamente entrenado para desempeñar funciones de seguridad, recopilar y evaluar información, mantener protocolos de comunicación, restringir accesos, prevenir la introducción de armas no autorizadas y artículos de contrabando, establecer los medios para activar alarmas, asegurar la realización periódica de ejercicios y simulacros de seguridad, y establecer niveles de seguridad.

A fin de acreditar el cumplimiento con el programa, los operadores de seguridad marítima deben implantar procedimientos para: monitorizar los accesos, las actividades del personal y las operaciones de carga, realizar con regularidad inspecciones de los buques e instalaciones portuarias, coordinar la aplicación de las medidas correspondientes a cada nivel de seguridad, proporcionar formación adecuada en materia de seguridad, informar a las autoridades competentes y asegurarse de que los equipos de seguridad y de comunicaciones se operan, se prueban y se mantienen adecuadamente.

1.1-2. LA SEGURIDAD MARÍTIMA EN LA UNIÓN EUROPEA

En junio de 2014, el Consejo Europeo adoptó una Estrategia de Seguridad Marítima a fin de proporcionar un marco común que asegure el desarrollo coherente de las políticas nacionales y europeas, y una respuesta conjunta a las amenazas en el ámbito marítimo (2).

Los propósitos principales que plantea la Estrategia de Seguridad Marítima Europea son:

1) Identificar y articular los principales intereses estratégicos de la UE.
2) Identificar y articular las principales amenazas, retos y riesgos que afrontan dichos intereses estratégicos.
3) Organizar la respuesta conjunta para atajarlos.

Esta Estrategia se basa en los siguientes principios:

1) Aproximación intersectorial: todas las autoridades civiles y militares, así como las agencias de la UE y la industria, deben cooperar en mayor medida.
2) Integridad funcional: la estrategia no interferirá con las respectivas competencias de la UE y sus Estados Miembros.
3) Respeto a las normas y principios: al derecho internacional, los derechos humanos, la democracia y los tratados bilaterales.
4) Multilateralismo marítimo: se cooperará con todos los miembros y foros internacionales de relevancia, en particular con la ONU y la OTAN.

Los intereses marítimos estratégicos de la UE y sus Estados Miembros son:

1) La seguridad de la UE, sus Estados Miembros y sus ciudadanos.
2) La preservación de la paz, en línea con la Carta de las Naciones Unidas, la resolución pacífica de las disputas relativas al dominio marítimo, de acuerdo con el derecho internacional, la prevención de conflictos y el fortalecimiento de la seguridad internacional.
3) La protección contra los riesgos y amenazas a la seguridad marítima, incluyendo la protección de infraestructuras críticas marítimas como áreas específicas de puertos e instalaciones portuarias, instalaciones off-shore, el suministro de energía por la mar, tuberías submarinas, cables submarinos y la promoción de investigaciones científicas y proyectos de innovación.
4) La preservación de la libertad de la navegación, la protección de la cadena de suministro el comercio marítimo, el derecho de tránsito inocente y el pasaje de buques, así como la seguridad de sus tripulantes y pasajeros.
5) La protección de los intereses económicos, incluyendo la salvaguarda de los recursos energéticos marítimos, la explotación sostenible de los recursos

naturales y marítimos en las diferentes zonas marítimas y en alta mar, el control de la pesca ilegal, la seguridad de las flotas pesqueras de los Estados Miembros y la delimitación de las zonas marítimas.

6) La promoción y el desarrollo común y validado de situaciones de alerta marítima.
7) La gestión efectiva de las fronteras externas de la UE y las áreas de interés al objeto de prevenir y contrarrestar las actividades transfronterizas ilegales.
8) La protección del medio ambiente y la gestión del impacto del cambio climático en las áreas marítimas y las regiones costeras, así como la conservación y el uso sostenible de la biodiversidad para evitar futuros riesgos.

Los principales riesgos y amenazas a la seguridad marítima que afronta la UE son:

1) La amenaza o el uso de la fuerza contra los derechos de los Estados Miembros y su jurisdicción en sus zonas marítimas.
2) Amenazas a la seguridad de los ciudadanos europeos y a sus intereses económicos mediante actos de agresión externa.
3) El crimen internacional y organizado, incluyendo la piratería y el robo armado en la mar, el tráfico de seres humanos y el tráfico de emigrantes, drogas y bienes.
4) El terrorismo y otros actos ilegales en los puertos, contra los buques, la carga, las tripulaciones y los pasajeros; contra los puertos, instalaciones marítimas e instalaciones críticas marítimas y energéticas.
5) La proliferación de armas de destrucción masiva, incluyendo amenazas químicas, biológicas, radiológicas y nucleares.
6) Amenazas a la libertad de la navegación, como la negación al acceso a la mar y los estrechos, y la obstrucción de vías marítimas.
7) Riesgos medioambientales, incluyendo la explotación no sostenible y no autorizada de los recursos marítimos y naturales, y las amenazas a la biodiversidad.
8) El potencial impacto a la seguridad de los desastres naturales o provocados por el hombre, eventos extremos y el cambio climático sobre el sistema de transporte, y en particular, sobre las infraestructuras marítimas.

9) La investigación arqueológica ilegal y no regulada, y el pillaje de objetos arqueológicos.

La Comunidad Europea adoptó el reglamento CE 725/2004 al objeto de instaurar y aplicar medidas comunitarias que mejoren la protección de los buques e instalaciones portuarias frente a las amenazas de actos ilícitos deliberados, sentando las bases para la interpretación y aplicación armonizadas de las enmiendas al convenio SOLAS en materia de protección marítima.

Este reglamento articula, además, los principios del control de la Comisión Europea sobre la aplicación de la legislación de seguridad marítima por parte de los Estados Miembros, y de la verificación de la efectividad de las medidas, procedimientos y estructuras desarrolladas en este ámbito.

Si bien los requisitos establecidos en el Reglamento CE 725/2004 han sido aplicados a los buques autorizados a enarbolar el pabellón español y a las instalaciones portuarias a las que aplica, se considera que es un conjunto parcial de todas 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, y se aprueba la Directiva 2005/65/CE sobre mejora de la protección portuaria, en la que se establece la obligatoriedad de desarrollar un Plan de Protección Portuaria basado en una evaluación de riesgos de amenazas y un análisis de riesgos de las instalaciones portuarias.

1.1-3. LA SEGURIDAD MARÍTIMA EN ESPAÑA

1.1-3.1. La dimensión marítima de la nación española:

Las consideraciones precedentes relativas al ámbito marítimo aplican íntegramente en una nación de carácter marítimo como la española: este carácter viene determinado por su posición geográfica, su dependencia de las comunicaciones marítimas y la importancia del sector marítimo en la economía nacional; por otra parte, es destacable el nexo que el medio marítimo ha supuesto tradicionalmente para conectar la península con los archipiélagos y las Ciudades Autónomas de Ceuta y Melilla.

Como consecuencia de esta realidad, España está expuesta de forma singular a riesgos y amenazas de carácter marítimo (3).

Los principales intereses nacionales, en su dimensión de seguridad marítima, que deben tenerse en cuenta son los siguientes:

1) El cumplimiento de la legislación nacional e internacional en los espacios marítimos bajo nuestra soberanía y jurisdicción, así como el respeto a las normas internacionales en alta mar.
2) La protección de la vida en la mar.
3) La libertad y seguridad en la navegación.
4) El comercio y el transporte marítimos.
5) La industria naviera y otras industrias marítimas.
6) La seguridad de los buques bajo pabellón español.
7) Los puertos e infraestructuras marítimas, incluyendo las instalaciones off-shore, oleoductos, tuberías y cables submarinos e infraestructuras críticas situadas en las costas.
8) Los recursos, vivos y no vivos, del medio marino.
9) El medio ambiente marino.
10) El patrimonio arqueológico subacuático.

1.1-3.2. Riesgos y amenazas para la seguridad marítima nacional:

En la mar se distinguen dos grandes grupos de riesgos y amenazas, según su origen: El primero es el derivado de los actos deliberados de naturaleza delictiva, que es el objeto de este estudio, y el segundo es el derivado de las circunstancias de naturaleza accidental o fortuita. Esta clasificación lleva a distinguir entre los actos ilícitos contra la seguridad marítima, y los accidentes marítimos o catástrofes naturales (3).

Además de los riesgos referidos, se pueden identificar factores que pueden contribuir a su aparición, como pueden ser la pobreza, la desigualdad, los extremismos ideológicos, los desequilibrios demográficos y el empleo nocivo de las nuevas tecnologías.

1.1-3.3. Actos ilícitos contra la seguridad marítima:

1) Tráficos ilícitos: tráfico de estupefacientes, contrabando, etc.; es importante destacar en este contexto el que se realiza por medio de contenedores de carga: esto es así debido a la dificultad de controlar el gran volumen de mercancía que se mueve de ese modo.
2) Piratería y robo a mano armada: son un tremendo problema en las zonas de especial riesgo y conforme a las prácticas que actualmente se utilizan; pese a que los puertos y las costas españolas no son una zona de especial riesgo, la introducción de armas en buques de crucero o transbordadores podría dar lugar a un acto de este tipo.
3) Terrorismo: es una amenaza que afecta directamente a la vida y seguridad de las personas y el medio marino puede ser la vía de infiltración de recursos humanos y materiales con fines terroristas. Como potenciador de la peligrosidad del terrorismo, señalar que determinados grupos no descartan el recurso al suicidio para conseguir sus objetivos.
4) Proliferación: la proliferación de armas de destrucción masiva constituye una de las preocupaciones más importantes para la comunidad internacional y tiene en el medio marino un elemento facilitador, debido a sus características.
5) Inmigración irregular por vía marítima y tráfico ilícito de migrantes: los flujos migratorios irregulares llevados a cabo por individuos, grupos u organizaciones criminales suponen un riesgo para la seguridad marítima y, en términos más amplios, para la Seguridad Nacional.

1.1-3.4. Estrategia de Seguridad Nacional:

La visión española de la seguridad marítima consiste en la acción concertada que involucre de forma eficiente todos los recursos públicos y privados dirigidos a anticiparse, prevenir y, en su caso, responder con eficacia a los riesgos y amenazas (3).

En este sentido, la Estrategia de Seguridad Nacional se marca como objetivo el de impulsar una política de seguridad amplia para proteger los intereses marítimos nacionales.

Son cuatro los principios informadores de dicha estrategia:

1) Unidad de acción de las organizaciones públicas y privadas.
2) Anticipación y prevención en la detección de situaciones de riesgo o amenaza potencial.
3) Eficiencia y sostenibilidad de recursos.
4) Capacidad de resistencia y recuperación, o aptitud de los recursos humanos y materiales para afrontar con flexibilidad y fortaleza las situaciones de crisis, sobreponiéndose a ellas.

1.1-4. PROTECCIÓN DE PUERTOS Y BUQUES DE PASAJE

Los puertos son infraestructuras de gran extensión en las que se desarrollan multitud de actividades acuáticas y terrestres que pueden llegar a emplear una ingente cantidad de medios materiales y humanos. Los movimientos simultáneos de embarcaciones y vehículos, además de los numerosos medios materiales que requiere la actividad portuaria: grúas, traspaletas, elevadoras, etc., complican enormemente la gestión de su seguridad, que puede verse asimismo comprometida en beneficio de la puntualidad de las operaciones, en aquellos casos en que se hace dejación en el cumplimiento de los procedimientos de seguridad con el fin de agilizar la operativa (4). Con todo, la seguridad de un puerto siempre se puede ver afectada por la seguridad de otro puerto, o la falta de ella, dado que la calidad de la seguridad no mantiene el mismo nivel en todas las naciones del globo.

Las terminales de buques de pasaje son las más estéticas, limpias y acogedoras, dado que se destinan al transporte de personas; en ocasiones tienen gran similitud con algunas terminales de aeropuertos, por el modo en que están estructuradas. Lo más usual es que se ubiquen en centros urbanos para que resulten fácilmente accesibles. Deben disponer de accesos para vehículos particulares, al objeto de que los pasajeros realicen el cambio de modo de transporte, y de que los vehículos de empresas accedan a las instalaciones para proporcionar suministros y servicios a las embarcaciones (5).

El objeto de la seguridad portuaria es el de establecer un entorno en el cual el comercio (en caso de los terminales de pasajeros, el transporte intermodal) se desarrolle con un grado razonable de seguridad frente a actividades criminales,

mediante el esfuerzo constante para reducir al mínimo las posibilidades de que se emplee el sistema de transporte marítimo en aras de la comisión de actos ilícitos. Con ello, las operaciones de seguridad portuaria han de ser proactivas (y no únicamente reactivas), anticipándose a la comisión de los hechos delictivos mediante la inteligencia, la investigación y la coordinación de todas las organizaciones públicas y privadas que prestan sus servicios en beneficio de la seguridad portuaria y marítima.

El diseño de la seguridad en los puertos pasa por la realización regular programada, y extraordinaria (en función de los acontecimientos), de evaluaciones de seguridad en las que se ponen de manifiesto las amenazas al entorno portuario y las vulnerabilidades del sistema de protección, y se plantean medidas correctoras para hacer frente a los riesgos, a la vez que los medios de protección se adaptan a la evolución normativa, a la de los propios medios de transporte y a la evolución de los medios que las organizaciones criminales emplean en la comisión de actos ilícitos (6).

Los servicios de inteligencia (recogida, análisis, diseminación y evaluación de datos tácticos y estratégicos) que se desarrollan en el entorno portuario y marítimo pueden proporcionar indicaciones e información del desarrollo y evolución de las actividades criminales y las amenazas que pueden tener que afrontarse: en ocasiones, el éxito de los planteamientos de seguridad depende de la habilidad de los servicios de seguridad para tratar la información recogida y neutralizar de manera proactiva las amenazas (5).

El sistema más común para controlar de manera efectiva los movimientos en el interior de las instalaciones portuarias es el de crear zonas de seguridad y emitir tarjetas de acreditación personal asociadas a la permanencia selectiva de sus portadores en ellas. De este modo, el portador de una tarjeta de acreditación personal podrá acceder a mayor o menor número de zonas, en función de sus necesidades (4). La emisión de estas tarjetas requiere una solicitud previa realizada en nombre de una organización que justifique su necesidad de acceder, y un estudio personalizado de los privilegios de acceso que se le asignan a cada una de ellas. La pérdida o el olvido de las tarjetas de acreditación personal se deben comunicar al servicio de seguridad de la instalación portuaria, a la mayor brevedad, para que los encargados de la gestión de acreditaciones tramiten las correspondientes bajas temporales o

definitivas y bloqueen su uso para que no se puedan realizar accesos sirviéndose de ellas. Este aspecto también se puede lograr incorporando al sistema de control de accesos datos biométricos, como lectores de huellas digitales o de retina (no obstante, en la actualidad los sistemas más extendidos son los de tarjetas de proximidad o de banda magnética, cuya eficiencia está ampliamente demostrada, y que resultan más económicos que los primeros).

Al objeto de lograr un ámbito portuario seguro, resulta imprescindible la implicación de todas las organizaciones y del propio personal que desarrolla sus funciones en los puertos, que deberá permanecer plenamente concienciado y adecuadamente formado en materia de seguridad, con conceptos y conocimientos claros y bien definidos. En este sentido, es importante señalar que ningún componente de la seguridad puede llevar a cabo sus cometidos sin el apoyo y el compromiso del resto: por ejemplo, se puede afirmar que un Vigilante de Seguridad que se ocupe del control de accesos a la zona restringida no podría realizarlo con efectividad si no se hubiesen desarrollado con anterioridad procedimientos adecuados en los que apareciesen perfectamente definidos los criterios que se han de seguir, o si no se hubiese puesto en producción un sistema de acreditaciones personales que permitiese conocer a qué áreas se autoriza el acceso de cada persona (5).

1.1-4.1. Actos ilícitos deliberados en buques de crucero:

Puesto que los buques de crucero se muestran, en la mayoría de las ocasiones, como iconos del lujo y del esplendor en los que viajan confinadas multitud de personas, se considera que pueden representar objetivos terroristas altamente atractivos; la repercusión mediática y el alcance de las consecuencias económicas que podrían resultar de un ataque de ese tipo, en el que se pretendiera maximizar el número de víctimas civiles, serían de una magnitud enorme (7).

Los siguientes son algunos de los posibles escenarios que podrían resultar de este tipo de ataques:

1) Secuestro de un buque de crucero con sus pasajeros, similar al del Achille Lauro, en que un grupo de personas aborda un crucero amenazando al pasaje y a la tripulación si no se atiende a sus demandas.

2) Hundimiento de un buque empleando un artefacto explosivo improvisado, similar a los ataques al USS Cole y al M/V Limburg, en los que se cargaron pequeñas embarcaciones con material explosivo, se lanzaron contra los buques y se detonaron.
3) Hundimiento de un buque mediante la fijación y detonación de material altamente explosivo a su casco, por debajo de la línea de flotación.
4) Introducción de material explosivo abordo, con la finalidad de detonarlo in situ.
5) Empleo de artillería pesada contra un buque, desde tierra o desde otra embarcación más pequeña.
6) Ataque biológico mediante la contaminación del agua o la comida del buque.

Además de resultar objetivos atractivos, hay algunas vulnerabilidades propias de la industria marítima que podrían ser explotadas por grupos terroristas para materializar sus ataques:

1) Los controles de seguridad no son tan estrictos como en la aviación comercial (8).
2) Mientras que la mayoría de los operadores verifican los antecedentes de sus propias tripulaciones y personal de mantenimiento, no se sigue el mismo procedimiento respecto de otro personal de servicio que accede a bordo durante las escalas.
3) Algunas prácticas operativas, como el hecho de fondear por períodos prolongados para permitir a los pasajeros desembarcar y visitar algunas ciudades, podrían perfilar/dibujar el escenario propicio para llevar a cabo un asalto o un ataque con una embarcación rápida cargada de explosivos.
4) La práctica habitual de congregarse el pasaje en las cubiertas del buque en las maniobras de atraque y desatraque, facilitaría la maximización de víctimas ante un ataque con armas de fuego o granadas tipo RPG desde tierra.
5) Prácticamente todos los buques de crucero navegan conforme a itinerarios planificados y accesibles al público, que normalmente están disponibles en internet, en los folletos publicitarios y en las agencias de viajes. Esta información podría permitir a un grupo armado diseñar ataques en los lugares y tiempos/momentos que favoreciesen su éxito en mayor medida (8).

Si bien las vulnerabilidades descritas hacen que los buques de crucero sean susceptibles de ser objeto de muchos tipos de ataques, se considera que son extremadamente difíciles de hundir, dado que la seguridad es prioritaria en su diseño y construcción: en este sentido, se puede destacar que son habituales los dobles cascos y los numerosos compartimentos estancos, de los cuales se les dota.

Las consecuencias de los ataques terroristas a buques de crucero son, hasta cierto punto, impredecibles y dependen de las dimensiones del buque, del daño causado al mismo y de la respuesta que reciban de los actores públicos y privados involucrados. Atendiendo a ataques de este tipo llevados a cabo con anterioridad se observa que, en el peor de los escenarios, podría verse afectada la integridad física de miles de personas.

El coste humano causado por un ataque biológico sofisticado, en el que se emplease ántrax o patógenos, podría ser la muerte de miles de personas, si bien la obtención del material y la infección exitosa de un número suficiente de pasajeros resulta compleja. En contraposición, la infección con bacterias, como la salmonella, resulta relativamente sencilla y podría dar lugar a tratar a cientos o miles de personas, pudiendo causar la muerte a decenas de ellas.

El coste económico directo asociado a la reparación de daños significativos o pérdidas de buques e instalaciones, puede ser de cientos de millones de Euros; las compensaciones por los daños causados a las personas y las pérdidas de vidas humanas, los costes asociados a la movilización de los medios de emergencia, sanidad y descontaminación, en su caso; si el ataque se dirigiese contra instalaciones portuarias o se llevase a cabo en aguas interiores, habría que considerar la paralización de las operaciones en puerto; además, los costes asociados al incremento de la seguridad, el decremento de la demanda de viajes de crucero, etc.

1.1-4.2. Actos ilícitos deliberados en transbordadores:

Los transbordadores resultan un medio de transporte accesible y generalizado, utilizado por multitud de personas para realizar trayectos marítimos que vienen a durar entre los 10 minutos y las 24 horas; muchos de estos buques pueden acomodar a miles de personas y a sus vehículos, para lo cual están diseñados con bodegas corridas y cubiertas amplias. Grandes portones hidráulicos en proa o en popa

facilitan la carga y descarga de personas y vehículos, que se realiza normalmente en cuestión de minutos (7).

A continuación se plantean algunos de los posibles escenarios que podrían resultar de este tipo de ataques:

1) Hundimiento de un buque empleando un artefacto explosivo improvisado, similar a los ataques al USS Cole y al M/V Limburg, en los que se cargaron pequeñas embarcaciones con material explosivo, se lanzaron contra los buques y se detonaron.
2) Hundimiento de un buque mediante la detonación de un explosivo adosado a su casco.
3) Detonación de un artefacto explosivo en el interior de una embarcación, tras haber sido introducido desde el exterior.
4) Ataque a la embarcación con artillería (metralletas, RPG…), desde la costa o desde otra embarcación.

Vulnerabilidades de los transbordadores.

1) Los controles de seguridad son superficiales, en la mayoría de los casos, incluso en las naciones más desarrolladas y concienciadas en materia de seguridad física. A ello contribuye, en gran medida, la necesidad de facilitar los flujos de embarque y desembarque de una manera eficiente, lo cual no hace viable la opción de inspeccionar a las personas, sus equipajes y sus vehículos (muchos, camiones cargados con mercancía).
2) Las verificaciones de antecedentes que se efectúan al personal empleado en este tipo de buques son prácticamente inexistentes: los países menos desarrollados ni siquiera tienen los medios, mientras que en los más desarrollados no se comprueban los historiales delictivos (antecedentes penales y policiales). Todos los expertos coinciden en que el acceso a las instalaciones y a los buques, por parte de personal adoctrinado y dispuesto a participar en la comisión de actos de interferencia ilícita constituye una vulnerabilidad importante.
3) Al igual que ocurre con los buques de crucero, prácticamente todos los transbordadores navegan conforme a itinerarios planificados y accesibles al público, que normalmente están disponibles en internet, en los folletos

publicitarios y en las agencias de viajes. Esta información propicia la planificación de ataques efectivos.

4) Algunas características del diseño de los buques tipo transbordador contribuyen a debilitar su integridad estructural y su seguridad: las largas bodegas corridas, aptas para propiciar el embarque y desembarque de vehículos, no son efectivas para contener las inundaciones y permiten desplazamientos de la carga que afectan al centro de gravedad del buque.

El coste humano asociado a un ataque dirigido a un transbordador dependería del daño causado al mismo: este tipo de embarcaciones acomodan a gran cantidad de pasajeros, mientras que las tripulaciones se reducen al mínimo; a mayor daño causado al buque, mayor probabilidad de que se hunda y mayor número heridos y fallecidos.

Los costes económicos, si bien no igualan por lo general a los de los buques de crucero, podrían también situarse en unas cifras enormes, considerando las indemnizaciones, la paralización de la actividad portuaria, los costes asociados a las operaciones de rescate, sanidad, incremento de la seguridad, caída de la demanda (esta caída podría originarse, en gran medida, como consecuencia de los cambios de hábitos y rutinas diarias de particulares, empresas de transportes, empresas de mensajería…), etc.

1.2- OBJETO DEL TRABAJO

El Puerto de Santander es un elemento clave en el transporte intermodal, con un considerable impacto en la economía regional; el Gobierno de Cantabria está planificando y ordenando áreas en el arco de la Bahía de Santander, que pueden convertirse en centros de actividades económicas capaces de aprovechar las ventajas competitivas que ofrece la proximidad del puerto (9).

El Plan Estratégico del Puerto de Santander propone una serie de actuaciones encaminadas a fortalecer su competitividad, explotando sus puntos fuertes, como la oferta logística de alta calidad, potenciando el tráfico de carga rodada, la captación de tráficos de mercancía general containerizada a través de líneas regulares, e incrementando el volumen de cargas sólidas y líquidas a granel: las líneas de actuación que se han valorado para conseguir tales objetivos contemplan tanto la

creación de un puerto exterior en la costa de Cantabria, como la ampliación del puerto en la Bahía de Santander.

El modelo actual de gestión portuaria tiende hacia el Modelo de Puertos en Red, intentando que el sector público impulse la actividad privada en los puertos, no solo en la prestación de servicios, sino también favoreciendo las inversiones necesarias para la modernización de sus instalaciones (financiación, construcción y explotación de las instalaciones portuarias especializadas), coordinando entre ambos estrategia e inversión. De este modo, se requerirá un esfuerzo importante en el desarrollo de infraestructuras portuarias, fundamentalmente en lo referente a los accesos marítimos y espacios terrestres, al objeto de crear las condiciones necesarias para que la iniciativa privada pueda consolidar la viabilidad financiera de sus inversiones en instalaciones portuarias concesionadas, y utilice el puerto como lanzadera hacia la conquista de mayores cuotas de mercado exterior.

En esta línea, se ha desarrollado un Plan Director del Puerto de Santander 2012-2022 en el que se contemplan tres fases que permitirán poner en servicio una infraestructura construida con inversión pública, para la maduración posterior de los proyectos de inversión privada:

- 1ª fase (2012-2015): inicio de las obras de ampliación con la construcción del muelle Raos 9, y generación de ingresos extraordinarios con la puesta en valor del frente marítimo-portuario.
- 2ª fase (2015-2020): aumento del calado del canal de navegación y generación de espacios en Raos Sur con el vertido del material dragado. Esta fase contempla el desarrollo de inversiones de integración puerto-ciudad en el frente urbano, con prioridad de la infraestructura portuaria de uso crucerístico y la consolidación del tráfico regular de pasajeros con el Reino Unido, creciendo el número de escalas de cruceros y carga acompañada. Las mejoras propuestas se basan en una mejora sustancial de las condiciones de atraque, dotando a la terminal de un mínimo de dos puestos para evitar los problemas operativos que actualmente se generan cuando coinciden las escalas de dos buques (habitualmente un transbordador y un crucero).
- 3ª fase (2020-2022): inversión privada en equipos y medios mecánicos en las nuevas terminales.

Atendiendo al contexto descrito en la introducción del documento, se observa que la seguridad marítima, en general, y la dirigida al transporte de personas, en particular, se pueden ver gravemente comprometidas. Con ello, y conocidas las propuestas de crecimiento y desarrollo del Puerto de Santander, se parte del esquema de una Estación Marítima ficticia que sustituya a la actual y se pretende contribuir localmente a garantizar su protección mediante la creación de una estructura orgánica local que planifique y coordine el diseño y la aplicación de las medidas seguridad con el resto de entidades implicadas, en los niveles transversal y vertical, dotando a la instalación portuaria de todos los medios de seguridad necesarios para dar cumplimiento a la normativa aplicable en materia de protección marítima: todo ello se plasma en el Plan de Protección de la Estación Marítima, como instrumento básico, fundamento de la protección .

Tal como se recoge en el Plan Director del Puerto de Santander 2012-2022, por considerarse que la Estación Marítima atraerá a tráficos limpios que generan un alto valor añadido a la ciudad, este edificio estará ubicado en su emplazamiento actual, en conexión con el centro urbano. El proyecto de reordenación urbanística del Frente Marítimo Portuario de Santander contempla la rectificación de la geometría de los muelles de Maliaño y la creación de tres puestos de atraque para buques de pasajeros, con una dotación de superficie terrestre superior a 80.000 m2.

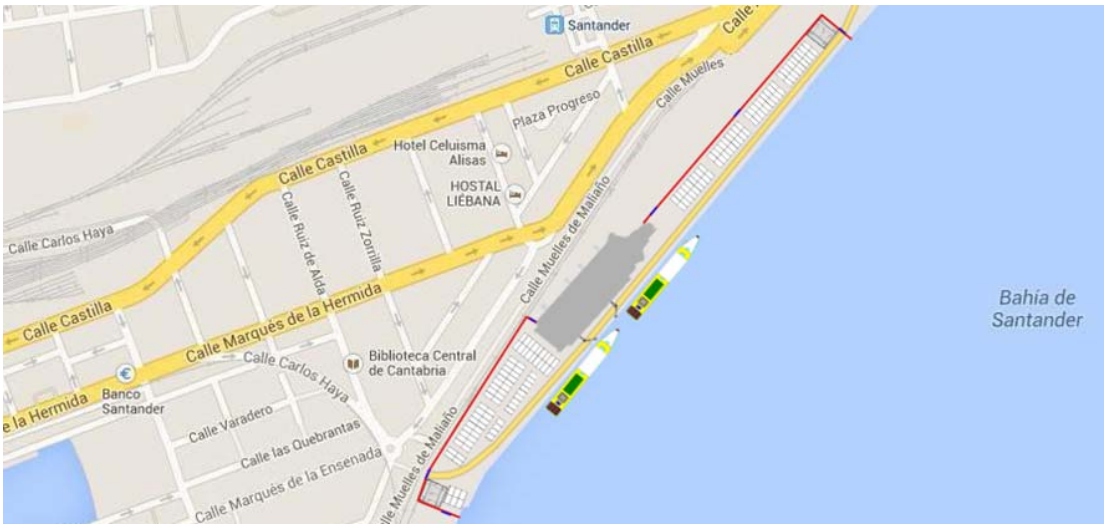


Figura 1: Plano de ubicación de la Estación Marítima
Fuente: el autor sobre fondo de Google Maps

2. SEGUNDA PARTE: METODOLOGÍA

2.1- CONSULTA DE PUBLICACIONES

Existe un enorme número de publicaciones (artículos, estudios, libros y páginas web) relacionadas con asuntos referentes a seguridad y una amplia variedad de puntos de vista desde los que abordar la problemática de la seguridad marítima, que se ve en este estudio acotada a la seguridad de una instalación portuaria: la Estación Marítima del Puerto de Santander.

La realización de este trabajo se fundamenta y se inspira en la consulta de algunos libros, documentos y páginas web, con varios objetivos:

1) Ofrecer una visión previa acerca del marco actual que engloba a la seguridad portuaria.
2) Diseñar una estructura de seguridad para la Estación Marítima.
3) Proponer unos medios de seguridad modernos con los que equipar la instalación para garantizar un nivel elevado de protección.

Por otra parte, se ha pretendido cumplir con la normativa nacional vigente en materia de protección marítima, que es absolutamente consecuente con las recomendaciones y normas internacionales que la regulan.

2.2- REALIZACIÓN DEL ESTUDIO

Conocidos los contextos internacional y nacional en materia de seguridad marítima y los medios humanos, organizativos y materiales que pueden aplicar a una instalación de este tipo, se diseña un boceto válido para albergar una Estación Marítima y se siguen los siguientes pasos:

1) Elaboración de una memoria descriptiva:

En ella, se muestra la disposición de las instalaciones y la facilitación (distribución de los espacios y medios disponibles al objeto de facilitar el paso de los usuarios a través del edificio terminal).

2) Elaboración de una memoria técnica:

Se explican los principales medios organizativos y técnicos propuestos para garantizar un nivel elevado de seguridad.

3) Confección del Plan de Protección de la Estación Marítima:

Este documento constituye el alma de la planificación de la protección y en él se detallan todos los aspectos relevantes en materia de seguridad, se relacionan los medios humanos, organizativos y materiales dispuestos y se detallan las funciones del personal de seguridad y las ubicaciones de los medios de protección de la Estación Marítima. El Plan se complementa con una Evaluación de Seguridad de la instalación en la que se tratan obtener valoraciones de los impactos que produciría la hipotética materialización de ciertos supuestos concretos de amenazas a la seguridad.

El Plan de Protección es un documento vivo que se debe ir adaptando a la evolución normativa y actualizando a la vez que se modifican los medios de seguridad. Con carácter regular, se programan auditorías y verificaciones de seguridad en las que se detectan puntos de mejora o vulnerabilidades y se plantean medidas correctoras a implantar, que provocan modificaciones en el Plan de Protección.

Dado que este estudio solo pretende ser un ejemplo y en la realidad este tipo de documentos son confidenciales, siendo su difusión restringida a aquellas personas con necesidad de conocerlos, únicamente se ha utilizado material de carácter público, como guía para su realización: por lo tanto, no procede desarrollar procedimientos de seguridad.

3. TERCERA PARTE: DESARROLLO

3.1- MEMORIA DESCRIPTIVA

3.1-1. EDIFICIO TERMINAL DE PASAJEROS

Se propone un edificio terminal de pasajeros de dos plantas, destinadas la superior a facilitar las salidas de pasajeros (facturación de equipajes, control de seguridad y acceso a salas de embarque, a pasarelas de embarque o vías peatonales, y al buque), y la inferior a dar servicio durante las llegadas (desembarco, recogida de equipajes, control de documentación y control fiscal).

A la entrada en el edificio terminal, en la planta superior, se accede al vestíbulo de salidas en el que se realiza la facturación de equipajes de cabina, de modo que los pasajeros únicamente portan sus equipajes de mano en el momento de acceder a la zona de embarques.

Tras atravesar el control de seguridad, dispuesto con todos los medios para asegurar que ninguna persona porta armas o artículos prohibidos, se accede a la zona restringida de seguridad, que se considera estéril, ya que tanto los trabajadores y las tripulaciones como los vehículos y los artículos que se introducen en ella han sido sometidos a controles de seguridad.

El equipaje facturado (equipaje de cabina) es sometido a una inspección de seguridad por niveles, antes de ser embarcado. Esta modalidad de inspección garantiza razonablemente que no se portan armas no autorizadas ni sustancias explosivas o incendiarias con la intención de embarcarlas.

El bloque técnico, en zona de acceso controlado, se destina a albergar las oficinas del gestor de la instalación portuaria; también puede dar cabida a personal perteneciente a otras organizaciones. El acceso a dicha zona no interfiere con otros pasos por el terminal y únicamente se autoriza por motivos justificados. Todas las personas que entren deben ir convenientemente acreditadas.

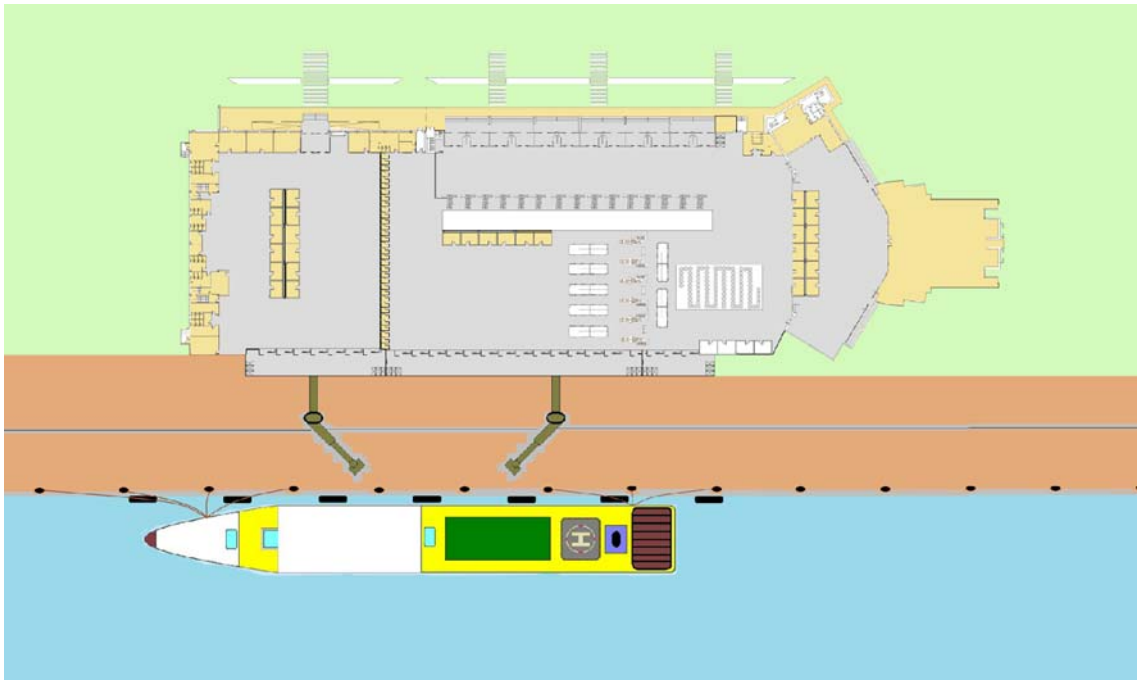


Figura 2: Planta de salidas del edificio terminal de pasajeros
Fuente: el autor

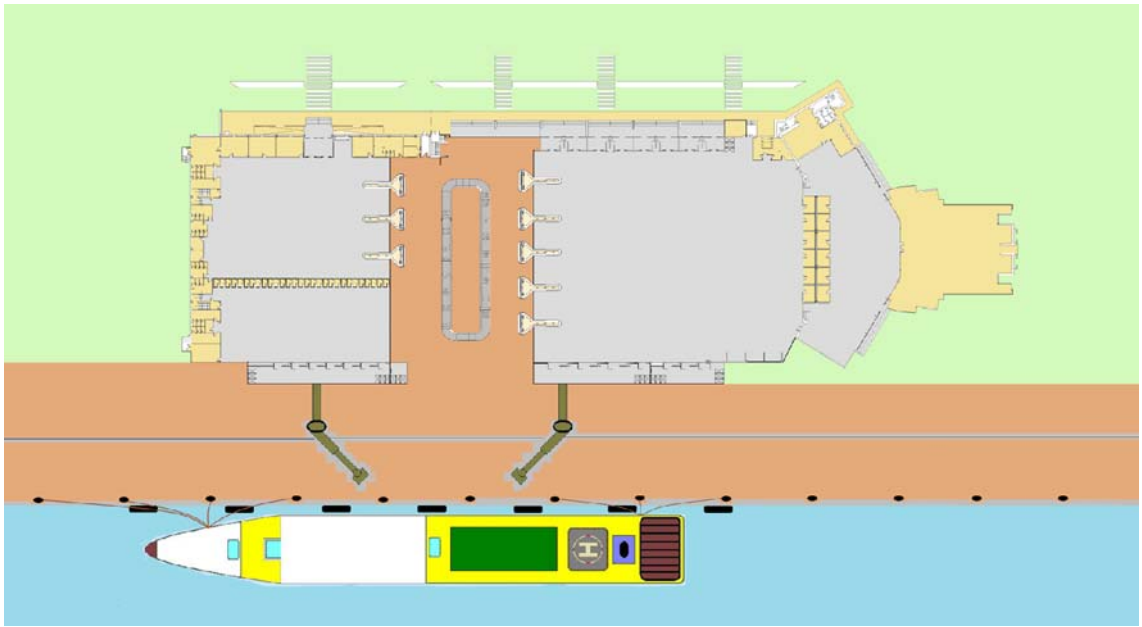


Figura 3: Planta de llegadas del edificio terminal de pasajeros
Fuente: el autor

Facilitación:

La planta de salidas alberga el vestíbulo de facturación, el control de seguridad y las salas de embarque nacional e internacional (ésta última dotada con las correspondientes instalaciones dependientes del puesto fronterizo, para efectuar el control de documentación).

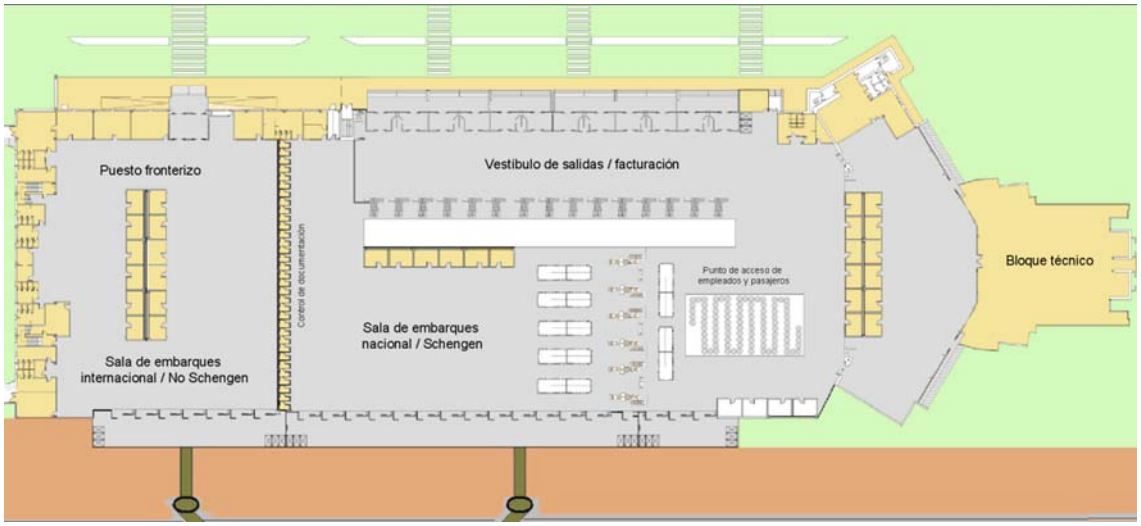


Figura 4: Disposición de espacios en planta de salidas
Fuente: el autor

Planta de llegadas: el edificio cuenta con una sala de llegadas nacionales y otra de llegadas internacionales, esta última equipada con cabinas para la realización del control de documentación e instalaciones dedicadas a realizar el control fiscal de los pasajeros procedentes de países no adscritos al convenio Schengen.

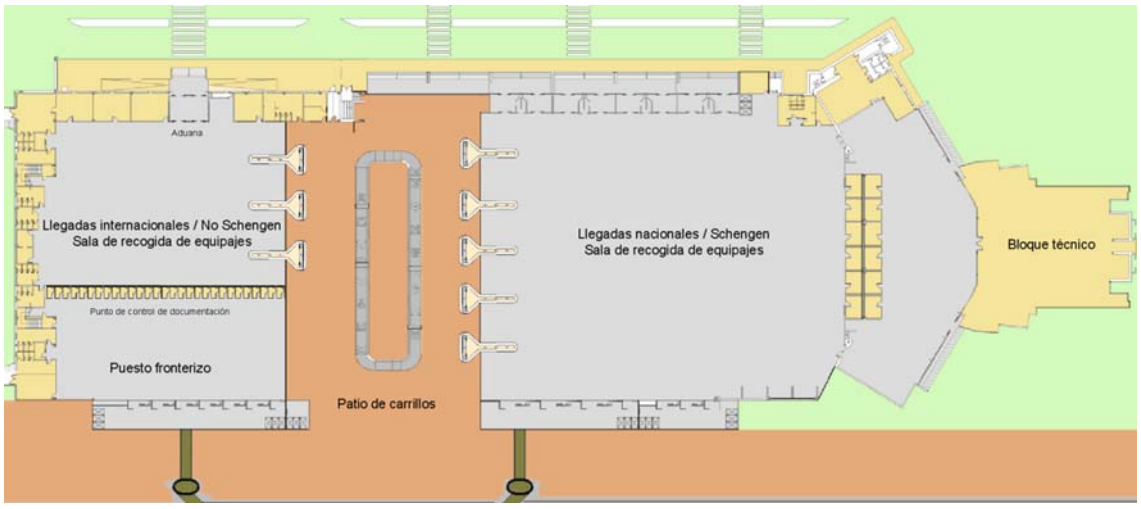


Figura 5: Disposición de espacios en planta de llegadas
Fuente: el autor

Nota: Schengenland es la denominación dada al territorio que comprende a aquellos Estados de la Unión Europea que han acordado la creación de un espacio común cuyos objetivos fundamentales son la supresión de fronteras entre estos países, la seguridad, la inmigración y la libre circulación de personas.

En la actualidad forman parte del territorio de Schengen los siguientes países: Alemania, Austria, Bélgica, Dinamarca, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Holanda, Hungría, Islandia, Italia, Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Noruega, Polonia, Portugal, República Checa, República Eslovaca, Suecia y Suiza (10)**.**

Un sistema de cintas permite realizar la facturación de los equipajes en la planta superior y transportarlos de manera automática a la planta inferior para su posterior embarque; del mismo modo, los servicios de asistencia en tierra pueden recoger los equipajes abordo para trasladarlos al patio de carrillos y distribuirlos posteriormente en las cintas de recogida de equipajes asignadas desde el centro de coordinación de operaciones y facilitación.

El patio de carrillos es el lugar desde el que los equipajes, convenientemente inspeccionados e identificados, se distribuyen para su embarque en las salidas, y desde el que los equipajes desembarcados se colocan en las cintas de las salas de recogida de equipajes, a las llegadas.

3.1-2. PERÍMETRO DE SEGURIDAD EN LA ZONA DE TIERRA

El perímetro de seguridad es la primera línea de defensa de la Estación Marítima y permite manejar una situación de riesgo o crisis facilitando el libre movimiento de los recursos propios en el interior de la zona protegida y favoreciendo a los tiempos de respuesta de los servicios de seguridad; su objetivo es prevenir, disuadir, frenar o retardar a los posibles intrusos, y alertar al grupo de seguridad sobre su presencia antes de que penetren en las instalaciones (también sirven al objeto de alertar sobre la presencia de personas que pretendan abandonar, o llegar al exterior, sin hacerlo por los puntos de acceso designados) (11).

Las instalaciones exteriores pertenecientes a la Estación Marítima están delimitadas por un cerramiento perimetral que aísla la zona de operaciones y la interfaz buque/puerto de las zonas aptas para la libre circulación del público: los muelles de atraque, las áreas de estacionamiento para vehículos destinados a ser transportados y para los que abandonan tras ser desembarcados, las áreas de depósito de suministros, provisiones, correo y carga, las zonas de inspección de vehículos y personas, y el

patio de carrillos, en el que se manipulan los equipajes de salida y de llegada permanecen estériles en la parte interior del perímetro delimitado para las operaciones, por lo cual todas las personas, vehículos, carga, correo y suministros que accedan a ella deben ser objeto de medidas de control. Los puntos de acceso y de salida están equipados con los medios necesarios para realizar los controles de documentación, de seguridad y fiscales.

Las puertas perimetrales, que permanecen cerradas habitualmente, si bien no son puntos de acceso a la zona restringida, pueden emplearse para el acceso extraordinario de medios de emergencia o para otras necesidades puntuales.

3.1-3. PERÍMETRO DE SEGURIDAD EN LA ZONA MARÍTIMA

El ataque a buques de crucero o transbordadores mediante el empleo de embarcaciones rápidas, de pequeñas dimensiones, cargadas de explosivo, es una de las acciones hipotéticas que más preocupación suscitan a las compañías marítimas dedicadas a este tipo de tráfico y a las autoridades de países costeros (12).

Al objeto de prevenir este y otros tipos de ataques mientras los buques se encuentren en la estación marítima (como la aproximación de embarcaciones para soltar artefactos explosivos improvisados o transportar buzos con el fin de adosar explosivos al costado del buque) (12), y mostrar unos límites claramente identificables (13), se pueden colocar barreras flotantes a lo largo del perímetro marítimo controlado.

Estas barreras, capaces de detener embarcaciones pequeñas, son de fácil apertura y cierre y constituyen un elemento disuasorio muy eficiente; facilitan, asimismo, la labor de vigilancia y control del tráfico en el área delimitada (14).

3.2- MEMORIA TÉCNICA

3.2-1. PERÍMETRO TERRESTRE

El cerramiento perimetral se establece para proteger a las personas (usuarios y trabajadores), así como a las operaciones de interfaz y a la propiedad, ante actos ilícitos deliberados; también para que los medios empleados en el negocio marítimo no se utilicen en la comisión de delitos. La porción de terreno que está destinado a guardar es una franja lineal, sin accidentes geográficos, de poca extensión y despejada: no se acumulan materiales ni bultos que dificulten excesivamente la vigilancia de las patrullas y la del centro de control de la Estación mediante CCTV.

No existen conductos subterráneos, tubos de desagüe, huecos bajo las puertas, pasajes ni pasadizos de dimensiones suficientes para permitir la entrada de personas. Deben realizarse, no obstante, revisiones frecuentes de las zonas adyacentes interiores y exteriores al objeto de garantizar que se encuentran libre de escombros, chatarras, basuras, vehículos, etc., que permitan un apoyo para franquear el vallado perimetral, y para comprobar su integridad.

Elementos que conforman el cerramiento perimetral

1) Base: murete o muro de hormigón, de sección rectangular, dotado de armadura, que sirva de soporte a los postes y a la sujeción de la parte inferior de la malla, con aperturas inferiores que permitan el drenaje del agua de lluvia. Se dotan de dos tubos empotrados, que alojarán la red eléctrica y la red de datos del sistema de detección perimetral, y de cajas de registro dispuestas a intervalos regulares, que facilitan su mantenimiento.
2) Postes: se instalan empotrados en el muro o murete de hormigón, unen los paneles longitudinales y conectan con las bayonetas que soportan el alambre de espino.
3) Paneles de malla: paneles de malla cubriendo la altura de los postes desde su base hasta el inicio de la bayoneta, fijados en su parte inferior al hormigón.
4) Bayonetas: se colocan en los extremos superiores de los postes, al objeto de dificultar la intrusión; pueden ser sencillas o dobles, preferentemente orientadas al exterior en el caso de que sean simples.

5) Puertas de emergencia: se instalan puertas motorizadas automáticas, con apertura remota o manual (desembragando el motor, en caso de fallo del sistema), para ser empleadas en casos extraordinarios o en emergencia.
6) Barreras: se instalan barreras motorizadas automáticas, con apertura remota o manual (mediante pulsador, in situ) al objeto de organizar el tráfico de vehículos desde y hacia el exterior, en los puntos de control de acceso y de salida (16).

El vallado perimetral puede incorporar medios de seguridad activos como cable microfónico (sensible a las vibraciones producidas por la agresión, corte, manipulación o arrancado) o una banda sensora antiasalto que permita detectar una fuerza de apoyo en la parte superior (15).

La instalación de medios de detección perimetral ofrece ventajas, tales como (11):

- Detectar intrusos antes de que hayan accedido al interior de las instalaciones.
- Informar de la posición en que los intrusos pretenden violar la seguridad.
- Discriminar las alarmas reales de las falsas alarmas.

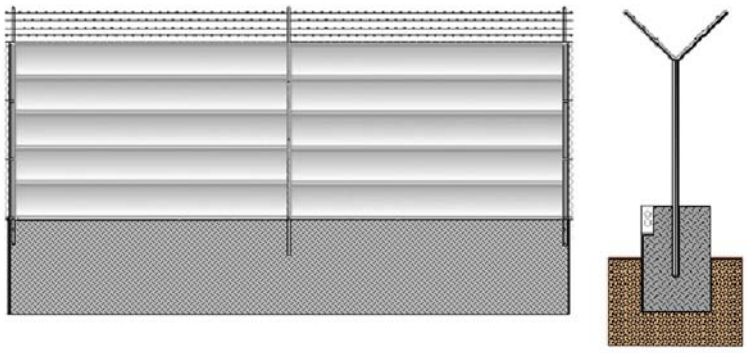


Figura 6: Detalle del vallado dispuesto de doble bayoneta (vistas frontal y lateral)
Fuente: el autor

3.2-2. PUERTAS

Una serie de puertas de interés, pertenecientes al edificio terminal y al cerramiento perimetral, se conectarán al sistema de seguridad para que puedan realizarse operaciones remotas sobre las mismas (apertura, cierre, bloqueo, desbloqueo) desde los puestos de mando del sistema de seguridad de la estación marítima, independientemente de que estén dispuestas de lectoras de tarjetas de acreditación personal, o no.

3.2-3. ZONA MARÍTIMA CONTROLADA

Al igual que en la zona de tierra, la zona marítima se puede confinar mediante barreras flotantes formadas por flotadores de espuma insumergible de alta visibilidad conectados entre sí mediante elementos resistentes a cargas pesadas, que montan vallados dispuestos con dos líneas de cable de acero de alta resistencia. Se pueden complementar con balizas luminosas alimentadas mediante paneles solares (14).

Al margen de la existencia de barreras físicas, la zona se debe controlar con la presencia de una patrulla marítima durante las 24 horas del día. Su función será la de abrir y cerrar el acceso a la instalación portuaria y el de controlar a todas las embarcaciones que entren, así como las operaciones marítimas buque a buque.

La zona se vigilará también mediante las cámaras móviles de la Estación Marítima, que están dotadas de potentes zooms que permiten enfocar perfectamente todo el perímetro delimitado.

Si bien una de las modalidades de ataque que más preocupan es la del ataque con proyectiles RPG (Rocket Propelled Granades) (1), se estima que la vigilancia de las zonas portuarias o exteriores que quedan fuera del perímetro de seguridad de la Estación Marítima, no siendo las zonas inmediatas al vallado perimetral, no es competencia del gestor de la Estación Marítima.

También cabe la posibilidad del ataque con embarcaciones ligeras cargadas de explosivo: si bien se estima que las barreras flotantes son suficientes para detener este tipo de embarcaciones, la Autoridad Portuaria debería considerar proporcionar escolta a los buques de crucero y transbordadores en sus tránsitos de entrada y salida y hasta que se encuentren en mar abierta (12).

Otro aspecto que no se debe desestimar es el acceso de buzos para adosar artefactos explosivos a los cascos de las embarcaciones: se trata de una empresa complicada que requiere un alto grado de especialización, pero que ha dado resultados en anteriores ocasiones. Del mismo modo que es complicado llevar a cabo una acción de este tipo, es complicada su detección una vez realizada, salvo que buzos profesionales revisen los cascos de los buques, antes de su partida (5).

Figura 7: Barreras flotantes Worthington SCB-32; detalle de la unión entre los flotadores y las balizas
Fuente: http://www.tuffboom.com/docs/2009%20SCB-32%20Flyer.pdf

3.2-4. ALUMBRADO DE SEGURIDAD

Puesto que una buena iluminación es uno de los elementos disuasorios más eficaces, es importante que el perímetro y zonas exteriores de la instalación permanezcan adecuadamente alumbrados durante las 24 horas del día, en previsión de impedir el acceso autorizado a las instalaciones, así como de la introducción de productos de contrabando, armas u otros objetos prohibidos que se puedan emplear abordo para la comisión de actos ilícitos. Cuando se emplea adecuadamente, la iluminación desalienta la actividad criminal, potencia las labores de vigilancia y reduce el temor en los usuarios legítimos de las instalaciones (17).

El objetivo es el de mantener, en la medida de lo posible, un nivel constante de iluminación que proporcione una buena visibilidad: cuando no se disponga de luz natural, debe proporcionarse un buen alumbrado artificial, tanto en el plano horizontal como en el vertical (en aquellas áreas en que se considere oportuno), para el desarrollo seguro de las operaciones; debe evitarse que los focos de luz intensos incidan sobre las personas, y las áreas sombrías; aquellas zonas más vulnerables o más indicadas para favorecer la comisión de actos ilícitos deben iluminarse mejor; cuando no se estén llevando a cabo operaciones se deberá disponer de un umbral de alumbrado que permita la vigilancia desde los puestos de patrulla y desde el puesto del Centro de Control; una de las medidas a aplicar ante niveles elevados de amenaza consiste en mantener plenamente iluminada la zona de operaciones durante las 24 horas.

El nivel de alumbrado interior y exterior de las instalaciones es susceptible de ser modificado en función del nivel de seguridad imperante en cada momento.

Se debe prever el fallo de alimentación eléctrica mediante la conexión del alumbrado de seguridad a grupos autónomos de emergencia.

Las características de construcción de los equipos deben ser adecuadas para soportar condiciones climáticas extremas, dada la exposición que sufren a los agentes meteorológicos y a la corrosión.

Figura 8: Focos LED de exteriores All-pro (activables mediante detección de movimiento)
Fuente:http://www.homedepot.com/b/Lighting-Ceiling-Fans-Outdoor-Lighting-Outdoor-Security-Lighting/All-Pro/N-5yc1vZc7qfZ383

Condiciones básicas que debe cumplir el alumbrado (5):

1) Todas las puertas exteriores se iluminarán durante las horas de oscuridad; las fuentes de luz se controlarán mediante células fotoeléctricas, programadores, o manualmente.
2) Se proporcionará un alumbrado adecuado, a lo largo de todo el cerramiento perimetral terrestre y marítimo.
3) Se iluminarán los viales y caminos exteriores, corredores, aparcamientos, escaleras y rampas; los pasillos, ascensores, accesos de vehículos y zonas de operaciones; se dispondrán detectores de movimiento que activen una iluminación complementaria de emergencia en aquellas zonas exteriores en las que no se lleven a cabo operaciones.
4) Se iluminarán todas las zonas interiores que permanezcan abiertas al público; aquellas que permanezcan cerradas dispondrán de iluminación activada mediante detección de movimiento.

3.2-5. SISTEMA DE GESTIÓN DE LA SEGURIDAD

La propuesta integra los siguientes sistemas:

1) **Sistema de gestión y control**: formado por los servidores de datos, los servidores de vídeo y los puestos cliente, es gestionado mediante los módulos de software específico.
2) **Sistema de circuito cerrado de televisión**: lo componen los diferentes elementos de CCTV instalados (cámaras fijas y móviles) y se conectan mediante una red específica para vídeo, al objeto de que el gran volumen de datos que se intercambian por la misma no condicione la operatividad del resto de sistemas.

Figura 9: Domos Autodome IP Dynamic 7000 HD y cámaras fijas DINION IP 7100 HD, de Bosch, para interior o exterior (según carcasa)
Fuente: http://www.boschsecurity.com

3) **Sistema de almacenamiento de datos**: formado por la cabina de grabadores, se gestiona de manera automática, previa configuración, por los servidores de vídeo y cada elemento periférico del sistema de CCTV.

Figura 10: Cabina de discos iSCSI DSA E-Series, de Bosch (solución escalable de almacenamiento en red)
Fuente: http://resource.boschsecurity.com/documents/DSA_E_Series_Data_sheet_esES_9511772939.pdf

4) **Sistema de control de accesos**: las lectoras de tarjetas de acreditación personal se conectan a sus respectivas controladoras (algunas controladoras gestionan una sola cabeza lectora mientras que otras gestionan dos, en función de que los accesos se realicen en uno o en dos sentidos a través de los pasos que protegen) y estas, a través de la red de datos, a los servidores.

Figura 11: Lectoras Bosch para control de accesos ARD FPBEPxx OC Plus (admiten tarjetas de proximidad y/o huella dactilar o clave numérica)
Fuente: http://us.boschsecurity.com

Apertura o desbloqueo de puertas en situaciones de emergencia: al objeto de evitar la improvisación, la interpretación personal de cada circunstancia y el error debido al factor humano, el sistema es configurable para que se programe una serie de eventos correspondientes a situaciones de emergencia

(amenaza de bomba en el terminal, amenaza de bomba en un buque, secuestro de buque, ataque en el interior del terminal, ataque en zona perimetral, etc.) y se realice la apertura remota de grupos de puertas, de manera automática. Desde el centro de control de la Estación Marítima se puede gestionar el desbloqueo y/o apertura de puertas del edificio terminal y de puertas motorizadas automáticas perimetrales.

Alarma e intrusión: este tipo de alarmas, incluidas dentro del grupo de eventos, alertan a todos los puestos cliente que disponen del correspondiente módulo de gestión, si bien han de ser siempre verificadas por el centro de control, que debe rearmarlas una vez resueltas.

Interfonos: integrados en las cabezas lectoras de tarjetas de acreditación personal, los interfonos comunican con el puesto de control a través de la red de datos.

5) **Sistema de iluminación**: la iluminación de seguridad se gestiona desde la unidad de control y se incluye dentro del grupo de eventos.

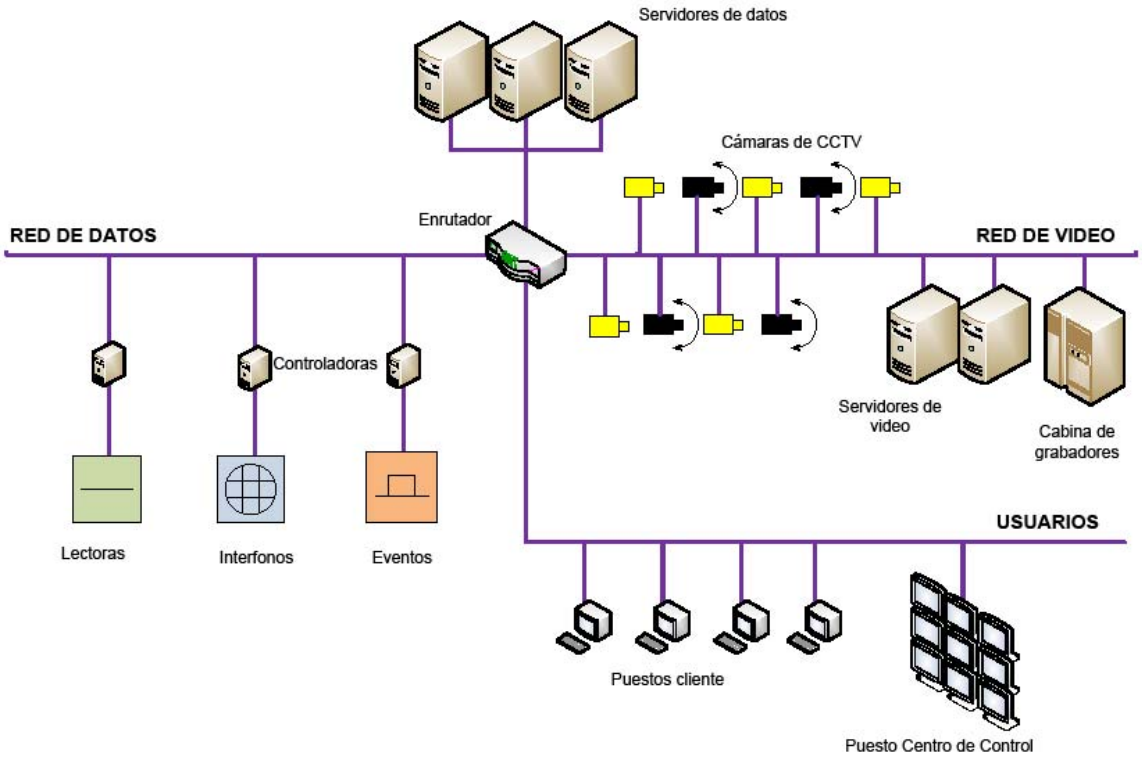


Figura 12: Diagrama de bloques del Sistema Integrado de Seguridad
Fuente: el autor

3.2-5.1. Software de gestión y control:

Un software de gestión integral de la seguridad proporciona una plataforma con acceso a los diferentes módulos de administración, gestión o control en la que se insertan los gráficos de la Estación Marítima y se ubican los diferentes elementos que componen la instalación; el operador dispone de múltiples posibilidades para seleccionar cámaras, domos, lectoras, puertas, luminarias, interfonos o alarmas y actuar sobre ellas.

A su vez, los servidores de vídeo administran el espacio disponible para grabación de imágenes en las cabinas, de manera que se graban constantemente todas las imágenes de cámaras y domos; a medida que se llenan los discos duros y se necesita espacio libre, el sistema automáticamente borra las imágenes más antiguas y retiene las más nuevas. Se debe configurar el sistema para que se cumpla convenientemente la Ley Orgánica de Protección de Datos.

Normalmente, este tipo de software es escalable: es decir, la plataforma tiene la capacidad de incorporar unos u otros módulos, más o menos módulos para la realización del control de los diferentes subsistemas, en función de las necesidades de la organización. De este modo, se podría operar con los módulos básicos (CCTV, CCAA…) o ir incorporando más módulos si se dispone de los medios precisos (detección perimetral, gestión de interfonos, gestión de alarmas…) (18).

Tareas de funcionamiento básicas:

1) Visualización de cámaras en tiempo real.
2) Gestión de alarmas y eventos.
3) Gestión de grabaciones.
4) Gestión de control de accesos.
5) Atención a interfonos.
6) Administración (configuración de zonas, permisos, privilegios, eventos, preposicionamiento de cámaras, etc.).
7) Gestión de iluminación de seguridad.

Figura 13: Presentación de software Bosch Building Integration System, escalable, con capacidad para albergar los diferentes módulos de gestión y control
Fuente:https://st-tpp.resource.bosch.com/media/technology_partner_programm/10_public/bvip_fw_to_sw/BIS_25.pdf

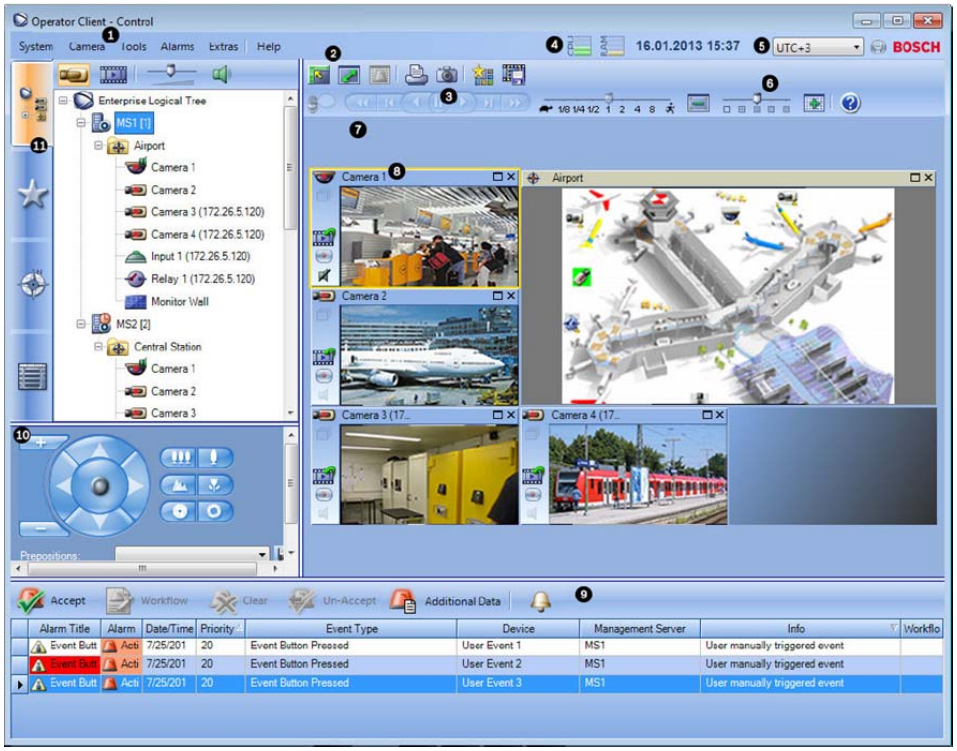


Figura 14: Presentación de software Bosch Video Management System v.5.0, integrable, para gestión de video y alarmas
Fuente:
http://us.boschsecurity.com/us_product/02_products_3/st_bu_f_277305_tams_catalog_prod_us/st_section_f_277673_tams_catalog_prod_us/st_prodfam_p_277673_tams_catalog_prod_us_357532

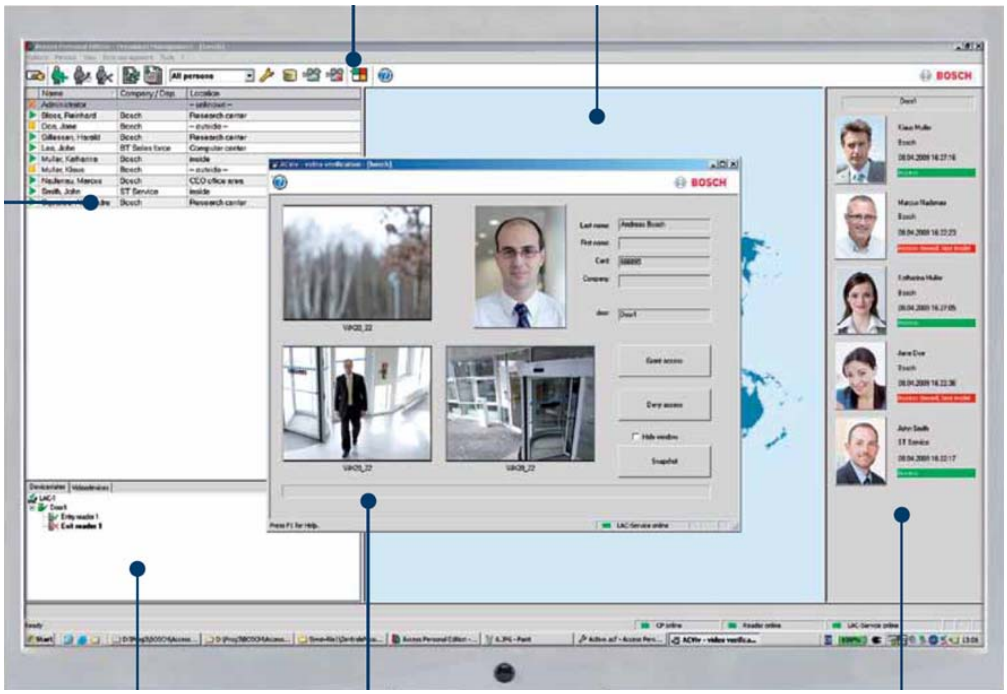


Figura 15: Presentación de software Bosch Access Professional Edition 3.0, integrable, para administración y gestión de control de accesos
Fuente: ***http://resource.boschsecurity.com/documents/Access_PE_3.0_Data_sheet_enUS_16373537675.pdf***

3.2-6. INSPECCIÓN DE PERSONAS, VEHÍCULOS, EQUIPAJES, CARGA, CORREO Y PROVISIONES/SUMINISTROS

Dado que la zona restringida de seguridad se considera una zona estéril, todas las personas, vehículos, artículos y materiales que se introduzcan en ella deben ser sometidos a controles de seguridad: estos controles serán más intensos cuanto más elevado sea el nivel de alarma imperante en cada momento; los controles de seguridad deberán estar perfectamente determinados en los procedimientos de seguridad y deberán conocerse en profundidad por el personal encargado de realizarlos.

El elevado número de personas que pueden hacer uso de la Estación Portuaria, sumado a la enorme cantidad de vehículos y pertenencias personales que pueden intentar acceder no se podría inspeccionar adecuadamente si el complejo no estuviese dotado de los equipos adecuados de inspección de personas, vehículos, equipajes, carga y correo (8).

Con todo, únicamente el personal convenientemente identificado y en posesión de la documentación apropiada será autorizado a penetrar en las zonas controladas y/o restringidas, haciéndolo siempre conforme a los procedimientos de seguridad.

Equipos de inspección: todos los equipos de inspección que se describen a continuación se consideran de apoyo en la realización de los controles de seguridad, puesto que están destinados a indicar a sus respectivos operadores la presencia de determinados artículos o materiales; una vez que el operador recibe la indicación de alarma o de presencia de artículos sospechosos, debe resolver la incidencia hasta que la alarma quede aclarada. Para ello, deberá recurrir a inspecciones manuales, aperturas de bultos, inspecciones de vehículos o de carga, etc., según el caso.

3.2-6.1. Medios técnicos para la inspección de personas:

1) **Arcos detectores de metales:**

Son equipos de que permiten revelar la presencia de ciertos objetos prohibidos, al paso de las personas a través de su pórtico, mediante la perturbación de un campo electromagnético originada por la presencia de masas metálicas. Generan una señal que se relaciona con el tipo, el tamaño, la orientación y la posición de cada objeto metálico con respecto al arco.

Por tratarse de detectores de metales, no detectan objetos amenazantes explosivos, plásticos, de madera, de cristal o cerámicos, y se requiere la presencia de un operador para la resolución de las alarmas (19).

En la actualidad, los Arcos Detectores de Metales cuentan con los siguientes elementos:

- Dispositivo de señalización de “detector listo”: Indica los momentos en los que se puede atravesar el arco para ser sometido a inspección.
- Central electrónica: permite su configuración y la extracción de estadísticas; controla su funcionamiento conforme a los parámetros (programa y sensibilidad) introducidos; genera una señal acústica cuando se detecta una masa metálica.
- Pórtico: Dispone de un panel emisor de un campo magnético y un panel receptor, así como de barras luminosas de indicación de zonas, que iluminan

los paneles laterales, a la altura en la que se encuentran las masas metálicas interceptadas.

Figura 16: Arco detector de metales CEIA PMD Plus 2 Elliptic
Fuente: http://www.ceia.net/security/index.aspx

2) **Detectores de metales portátiles:**

Este tipo de detectores, sensibles a los metales magnéticos y no magnéticos, permite al personal de seguridad responsable del control de seguridad, ayudar a resolver las alarmas metálicas generadas en los arcos detectores de metales, aproximándolo a las zonas del cuerpo resaltadas en los paneles laterales, en las que marcan la presencia de pequeñas masas metálicas mediante indicaciones visuales, sonoras o vibración (19). Su principio físico de actuación se basa en la perturbación de un campo electromagnético ante la presencia de un objeto metálico. Se componen de: área de inspección, mandos/display y alarmas.

Figura 17: Detector manual de metales CEIA PD 140 N
Fuente: http://www.ceia.net/security/index.aspx

3) **Detectores de metales en calzado:**

Un porcentaje de calzado que contiene masas metálicas provoca alarmas durante el tránsito a través del arco detector de metales. Este tipo de equipos, complementario a los arcos detectores de metales, permite detectar la presencia de objetos metálicos estáticos cuando se encuentran en el calzado, los pies o los tobillos de las personas inspeccionadas, mediante la generación de una señal que se relaciona con el tipo de objeto, su tamaño, su orientación y su posición (19). Requieren la presencia de un operador durante su utilización.

Los DMC se componen de:

- Unidad de control: permite su configuración y la extracción de estadísticas; controla su funcionamiento conforme a los parámetros (programa y sensibilidad) introducidos; genera una alarma acústica y sonora cuando detecta una amenaza metálica.
- Área de control: dotados de emisores y receptores de campos magnéticos de baja frecuencia que permiten la detección de masas metálicas conforme a los parámetros introducidos en la unidad de control.

Al igual que los arcos magnéticos, no son capaces de detectar objetos amenazantes explosivos, plásticos, cerámicos, de madera o de cristal.

Figura 18: Detector de metales en calzado CEIA SAMD
Fuente: http://www.ceia.net/security/index.aspx

3.2-6.2. Medios técnicos para la inspección de equipajes, bultos y vehículos:

1) **Equipos de RX:**

Son equipos de seguridad que permiten inspeccionar equipajes proporcionando imágenes de alta resolución y calidad del interior, que incorporan funciones de ayuda al operador. Son capaces de presentar imágenes de la composición interna de los objetos inspeccionados, tras la emisión de una radiación electromagnética, invisible, de alta energía y alta penetración, sobre los mismos. Estas radiaciones electromagnéticas son de la misma naturaleza que la luz, si bien su longitud de onda es más corta y les permite atravesar la materia.

Emplean tecnologías de detección de radiación y de procesamiento de imágenes, que son capaces de representar los objetos inspeccionados en monitores a color, al instante. Por medio de la codificación de la información de material, la función de diferenciación de los materiales permite una representación en color casi real de los diferentes materiales (20).

Los equipos de RX se componen de los siguientes bloques de elementos:

- Carcasa: aloja el túnel que los artículos inspeccionados atraviesan mediante una cinta transportadora, en el cual son sometidos a una radiación electromagnética emitida por unos generadores (hasta 5, dependiendo del equipo), parte de la cual atraviesa los cuerpos y es posteriormente captada por unos receptores dispuestos al efecto. Una protección interior de plomo y las cortinillas laterales, del mismo material, contienen la radiación en el interior del equipo.
- CPU y consola: la radiación captada por los receptores dispuestos en la carcasa se digitaliza y se presenta en los monitores, mostrando imágenes completas que corresponden al interior de los artículos. El operador dispone de un panel de mando, en el que puede seleccionar diferentes ayudas para realzar las imágenes (zoom, video inversión blanco-negro/negro-blanco, realzador de contornos, indicador de materiales no penetrables, materiales orgánicos/inorgánicos).

La principal limitación de estos equipos es que, al ser operados por una persona, esta es susceptible de fatigarse con el paso del tiempo; por ello, se recomienda que los

operadores realicen turnos de atención a los monitores, no superiores a los 20 minutos de inspección continuada.

La inspección de vehículos (turismos y vehículos de provisiones y carga) también se puede realizar mediante la operación de equipos de Rayos X convencionales, mucho más potentes y complejos. Algunos son capaces de discriminar de manera automática las cabinas de los espacios de carga y realizar la inspección sin que los conductores tengan la necesidad de bajarse de los vehículos. Otros requieren que no haya personas presentes en un perímetro de seguridad.

Figura 19: Equipo de RX convencional Smiths Heimann Hi-Scan 7555 aTiX (integra detección de explosivos líquidos) para inspección de equipaje de mano
Fuente: http://www.smithsdetection.com/index.php/products-solutions/x-ray-inspection.html

Figura 20: Equipo de RX convencional Smiths Heimann Hi-Scan 130130T 2iS (integra detección de explosivos líquidos) para inspección de suministros, cargas, pallets y equipaje de grandes dimensiones
Fuente: http://www.smithsdetection.com/index.php/products-solutions/x-ray-inspection.html

Figura 21: Equipo Smiths Heimann CIP 300 para la inspección de turismos
Fuente: http://www.smithsdetection.com/index.php/products-solutions/x-ray-inspection.html

Figura 22: Pórtico Smiths Heimann HCVP, de RX convencional, para la inspección de vehículos de carga
Fuente: http://www.smithsdetection.com/index.php/products-solutions/x-ray-inspection.html

2) **Equipos de Detección de Explosivos (EDS/EDX)**:

Son equipos capaces de detectar de manera automática, y así indicarlo por medio de una alarma, sustancias explosivas contenidas en un artículo, independientemente del material del que esté fabricado. Sus principios de funcionamiento son los mismos que los de los equipos de RX, pero combinan dos señales físicas (el número atómico y la densidad) en el caso de los EDS, o utilizan un sistema de rayos X de doble rayo, en el caso de los EDX, mejorando notablemente las capacidades de los equipos convencionales (20).

Sus componentes, al igual que los equipos de RX, carcasa (con túnel, generadores, receptor, cinta cortinillas) y consola con (CPU, monitor y mandos para ayudas).

Si bien se trata de equipos que funcionan en modo automático, son compatibles con la presencia de un operador monitorizando las imágenes de los artículos inspeccionados.

Figura 23: Equipo Smiths Heimann 10080 EDX 2iS de detección automática de explosivos
Fuente: http://www.smithsdetection.com/index.php/products-solutions/x-ray-inspection.html

3) **Sistemas de tomografía computerizada (CTX):**

Realizan un barrido completo de Rayos X, desde diferentes ángulos, proporcionando una visión excelente del interior de los bultos inspeccionados (20). Existen en el mercado diferentes tecnologías de detección e inspección, que se combinan con la tomografía computerizada 3D volumétrica, para la formación de imágenes en tres dimensiones. Proporcionan un índice reducido de falsas alarmas en modo de trabajo automático.

Se trata de equipos muy sofisticados, de alta precisión, que proporcionan al operador una ayuda inestimable en la resolución de alarmas de objetos sospechosos.

Su carcasa aloja un módulo de entrada, otro de toma de imágenes y un tercer módulo de salida; un receptor situado en el módulo intermedio recoge la señal y la envía a una CPU que reconstruye la imagen del artículo inspeccionado en un monitor.

Figura 24: Equipo Smiths Heimann Hi-Scan 10080 XCT, de tomografía computerizada 3D
Fuente: ***http://www.smithsdetection.com/index.php/products-solutions/x-ray-inspection.html***

Equipos de inspección de líquidos explosivos:

Se trata de equipos desarrollados recientemente, que mediante el empleo de diferentes tecnologías sirven para inspeccionar líquidos, aerosoles y geles permitiendo la detección de explosivos (19).

Existen varios tipos de LEDS: los más sencillos requieren impregnar una tira reactiva con el líquido, para su análisis; otros requieren verter una muestra del líquido en un pequeño recipiente, en el cual lo analizan; otros disponen de una cavidad en la que introducir los envases o botellas, analizándolas sin necesidad de abrirlas y los más sofisticados son capaces de realizar el análisis sin necesidad de presentar los artículos líquidos por separado del resto del equipaje.

Figura 25: Detector de explosivos líquidos CEIA EMA
Fuente: ***http://www.ceia.net/security/index.aspx***

4) **Equipos de detección de trazas de drogas y explosivos**:

Permiten detectar restos de explosivos y/o drogas, del tamaño de nanogramos e incluso picogramos, tanto en las personas como en los que portan o que han manipulado previamente. La detección de estos equipos se basa en técnicas de análisis, por métodos físicos, de la superficie de los objetos o del vapor que emiten las superficies contaminadas, mediante la recolección y el análisis de las partículas presentes en las mismas. Cuando encuentran coincidencias con los parámetros que tienen introducidos en sus bases de datos, lo indican por medio de una alarma (21).

Existen varios tipos de equipos detectores de trazas: de tipo pórtico, de sobremesa y manuales.

Figura 26: Detector manual de trazas Rapiscan HE50
Fuente: ***http://www.rapiscansystems.com/en/products/trace_detection/rapiscan_detectra_hx***

3.2-6.3. Inspección con la ayuda de perros:

Los perros se han mostrado un apoyo con capacidades extraordinarias en la detección de todo tipo de artículos: explosivos, drogas, personas, dinero, etc.: entrenados para detectar y marcar la presencia de las sustancias o artículos citados, son extremadamente versátiles y actúan con tremenda eficacia tanto en la inspección de personas como en equipajes, vehículos, naves, edificios y exteriores; también pueden ser entrenados para proporcionar protección y guarda (y acompañar al personal de patrulla).

Asimismo, son un medio disuasorio de protección contra actos ilícitos y proporcionan servicios de atención inmediata a bultos abandonados y equipajes no acompañados (22).

A juicio de algunos expertos, su efectividad es comparable con la de los equipos más desarrollados (23).

3.2-6.4. Sistema de inspección de equipajes facturados, por niveles:

El objetivo principal de la inspección de equipajes por niveles (24) es que todos los equipajes se procesen por el mínimo número de niveles necesarios para conseguir un porcentaje de inspección del 100%: esto significa que, en el supuesto de que un equipaje se aclare en los primeros niveles, no pasa a los siguientes; solo pasan a niveles superiores aquellos equipajes que no se aprueban en un determinado nivel.

Puesto que la inspección es más compleja en la medida en que se eleva el nivel, tarda más en realizarse. Es por ello que el rechazo de un gran número de equipajes puede generar tiempos de inspección altos.

1) **Nivel 1 de inspección**:

   Consiste en un proceso automático que únicamente puede realizarse con un equipo de rayos X con EDS/EDX (Explosive Detection System). Estos equipos no requieren la presencia de un operador, puesto que son capaces de discriminar y rechazar aquellos equipajes que no superan la inspección.

2) **Nivel 2 de inspección**:

   Si bien la inspección de equipajes en el nivel 1 es automática, los equipos EDS disponen de estaciones de trabajo (con CPU y monitor) que muestran todas las imágenes a un operador. Cuando un equipaje no supera el nivel de inspección 1, el sistema alerta al operador y marca los elementos sospechosos para que sean inspeccionados por este personal cualificado. En este punto, la decisión de aprobar el equipaje, o no, corresponde a una persona.

   El operador dispone de diversas utilidades para el realce de la imagen, que le ayudan en su cometido.

3) **Nivel 3 de inspección**:

   Los equipajes que se rechazan en el nivel 2 pasan a ser examinados profundamente en los equipos CTX, de alta capacidad de detección: estos

equipos realizan una inspección automática a la vez que un operador observa las imágenes que presenta el equipo en el monitor; el operador puede rotar y manipular las imágenes su antojo en el monitor, para observarlas desde todos los ángulos.

4) **Nivel 4 de inspección**:

Cuando todavía quedan objetos sospechosos por aclarar tras haber pasado por el equipo CTX, los equipajes se inspeccionan en un equipo de RX convencional y/o se abren en presencia de su propietario. Este paso de denomina "conciliación". En el supuesto de que no se logre encontrar al propietario del equipaje o no se logre aclarar el bulto, se deben articular los procedimientos de seguridad correspondientes.

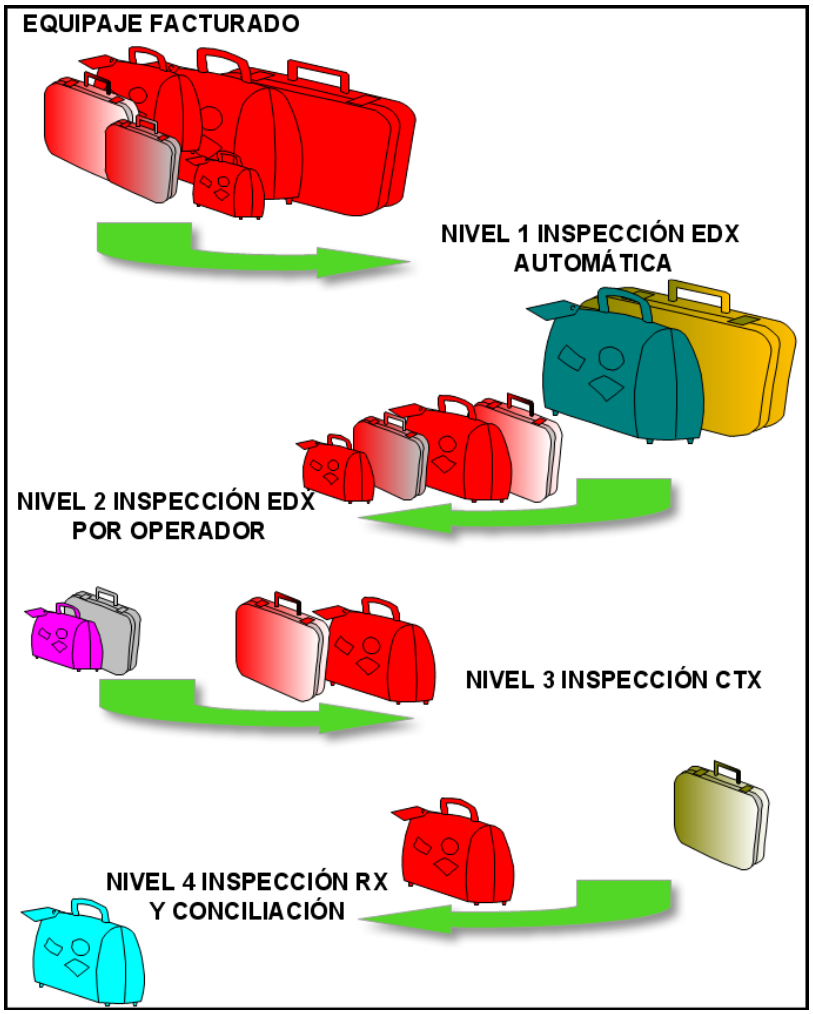


Figura 27: Esquema de inspección de equipajes, por niveles
Los equipajes no aclarados (en rojo) se van aclarando a medida que van alcanzando niveles de inspección más elevados (recuperan color original).
Fuente: el autor

3.2-6.5. Equipaje no acompañado:

El equipaje no acompañado siempre debe pasar procedimientos de inspección más estrictos que el equipaje acompañado, dado que podría ocultar artículos destinados a cometer actos de naturaleza ilícita, sin que sus responsables corriesen grandes riesgos**.** En muchos casos, no se acepta este tipo de equipaje para su transporte (25)**.**

3.2-7. SEÑALIZACIÓN

La colocación de una señalización adecuada tiene por objeto informar convenientemente al público de la existencia de zonas de seguridad y servir de medio preventivo y disuasorio para evitar accesos indebidos (13)**.**

Se considera necesario colocar una señalización permanente que advierta de las zonas de seguridad y de las medidas aplicables en algunos puntos (puntos de inspección u obligatoriedad de portar tarjetas de embarque o acreditativas de la instalación portuaria).

La señalización destinada a ser instalada en la zona marítima debe ser visible desde distancias significativas, tanto durante el día como en la noche.

Es conveniente complementar la señalización con folletos informativos, principalmente en los puntos de inspección, para que las personas que pretenden acceder sean conocedoras de aquellos artículos que pueden, o no, introducir en las zonas restringidas, advirtiendo sobre la responsabilidad que conlleva la introducción de objetos prohibidos.

3.2-8. NIVELES MARSEC

El Ministerio del Interior, a través de la Secretaría de Estado de Seguridad, determina el nivel de amenaza que impera en el entorno marítimo, incluidos puertos, buques, instalaciones portuarias e infraestructuras críticas situadas en las aguas territoriales del Estado, o adyacentes a ellas, impartiendo orientaciones para protegerse contra los sucesos que afecten a la protección. Todas las instalaciones e infraestructuras responderán a los cambios en los niveles MARSEC mediante la implementación de una serie de medidas de protección más intensas cuanto más elevado sea el nivel.

La determinación del nivel de seguridad que ha de aplicarse responde a un proceso multidisciplinar en el que intervienen, en buena medida, los Servicios de Inteligencia del Estado. Entre los factores a tener en cuenta para establecer estos niveles, se evalúa en qué medida es verosímil la información sobre la amenaza o las consecuencias que el suceso puede ocasionar en el ámbito marítimo o portuario; sus efectos modifican los niveles de seguridad que se aplican en las diferentes áreas de actividad de las instalaciones afectadas: control de accesos; controles de seguridad; aceptación de suministros, carga y correo; vigilancia y patrullas; etc.

La difusión y notificación de alteraciones en los niveles de amenaza se realiza por parte de la Secretaría de Estado de Seguridad a los responsables de la Sociedad Estatal de Salvamento y Seguridad Marítima (SASEMAR) o del Ente Público Puertos del Estado, según resulten afectados los buques o instalaciones portuarias, respectivamente (26).

En el caso de que resulte de interés, se pueden facilitar detalles, tales como las áreas geográficas más afectadas por la amenaza, posibles objetivos, duración estimada de la elevación del nivel de amenaza, tipo probable de amenaza y acciones convenientes dirigidas a minimizar el riesgo.

Las entidades afectadas por estas eventualidades deben tener planificada la manera en que responderán (los procedimientos y medidas que se pondrán en producción), en sus respectivos Planes de Protección y todo el personal involucrado debe ser capaz de aplicar con éxito las medidas de refuerzo.

3.2-9. DECLARACIÓN DE PROTECCIÓN MARÍTIMA (DOS)

Una Declaración de Protección Marítima constituye un acuerdo escrito entre una instalación portuaria y un buque con el que realiza operaciones de interfaz, en la que se establece la responsabilidad que asumirá cada parte, en materia de seguridad, mientras dure la visita (27).

Serán los Gobiernos quienes determinarán cuándo se requiere una Declaración de Protección marítima.

En el caso de la Estación Marítima y teniendo en cuenta que la instalación dispondrá de un Plan de Protección aprobado, un buque podrá solicitar que se cumplimente una Declaración de Protección marítima cuando:

1) El buque funcione a un nivel de protección más elevado que la Estación Marítima.
2) Exista un acuerdo sobre la Declaración de Protección marítima entre gobiernos contratantes que regule determinados viajes internacionales o buques específicos en dichos viajes.
3) Se haya producido una amenaza o un suceso que afecte a la protección marítima en relación con el buque o con la instalación portuaria, según sea el caso.

Los responsables de cumplimentar la Declaración de Protección Marítima serán:

1) En el caso del buque, su Capitán o su Oficial de Protección.
2) En el caso de la Estación Marítima, su Oficial de Protección.

3.3- PLAN DE PROTECCIÓN DE INSTALACIÓN PORTUARIA

Para el Puerto de:

Estación Marítima del Puerto de Santander

Realizado por:

Fecha: 01/12/2014

Presentado por <**Nombre de la persona autorizada**>

Cargo: **Oficial de Protección de la Estación Marítima**

Firma……..……

Fecha……..……..……

Clasificación de seguridad…**DIFUSIÓN RESTRINGIDA**

Revisión número…**01**……

Copia número…**01**……

CONTENIDO

Sección 1 – Clasificación del documento

1.1 Autoridad

Este documento (28) (29) ha sido confeccionado por una organización de protección reconocida y aprobado por el Comité Asesor de Protección de la Estación Marítima al objeto de que se remita, para su aprobación, a la Autoridad de Protección Portuaria. A través de su contenido se justifican las medidas y procedimientos de seguridad que se aplicarán en la operativa diaria de la instalación para cumplir adecuadamente con los requerimientos nacionales e internacionales en materia de seguridad marítima y dar continuidad a las operaciones, sin interferir con las del resto de instalaciones portuarias.

Las directrices en él contenidas involucran a todas las organizaciones privadas y públicas que desempeñan cometidos en las diferentes zonas establecidas, dentro de la Estación Marítima, incluyendo a las Fuerzas y Cuerpos de Seguridad.

1.2 Protección del documento y confidencialidad

Objetivo – La protección efectiva del Plan de Protección de la Estación Marítima, en previsión de su difusión no autorizada.

El operador de la Estación Marítima se asegurará, en la medida de sus posibilidades, de que el Plan de Protección de la instalación portuaria se protege de accesos no autorizados, no sufre modificaciones no autorizadas y no llega a ser conocido por terceras personas.

Este documento se califica de “Documento Confidencial” y ha de ser conocido únicamente por las personas y entidades que tengan justificada su necesidad de conocerlo. Será responsabilidad de cada persona que lo posea su custodia y protección al objeto de que no sea difundido de manera no autorizada.

Se mantendrá un registro de las copias emitidas y de las personas que lo reciben.

1.3 Hoja de registro de cambios

En la siguiente tabla se registra el historial de los cambios, revisiones y modificaciones que sufre el documento original.

REGISTRO DE REVISIONES DEL DOCUMENTO				
Versión	**Número(s) de Sección**	**Números de páginas**	**Fecha de la última revisión/cambio**	**Fecha de aprobación**
A	*Todas*	*Todas*	*Diciembre 2014*	*NA*
1				
2				

Nota:
Se emplearán las letras A, B, C, etc. para relacionar las versiones no aprobadas del documento;
Se emplearán los números 1, 2, 3, etc. para relacionar las versiones aprobadas del documento;

1.4 Normativa de referencia

La elaboración de este documento se ha realizado en base a la siguiente reglamentación (30):

1) Código internacional para la protección de los buques e instalaciones portuarias.
2) Código internacional para la protección de los buques e instalaciones portuarias publicado en el BOE.
3) Enmiendas de 2002 al Anexo del Convenio Internacional para la Seguridad de la Vida en la Mar, 1974, adoptadas el 12 de diciembre de 2002 mediante resolución 1 de la conferencia de gobiernos contratantes del Convenio Internacional para la Seguridad de la Vida en la Mar.
4) Reglamento CE 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.
5) Procedimiento por el que se establece y regula el Plan de Formación, homologación, control de calidad y expedición de la certificación acreditativa del OPIP.

6) Directiva 2005/65/CE del Parlamento Europeo y del Consejo de 26 de octubre de 2005 sobre mejora de la protección portuaria.
7) 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.
8) Reglamento CE nº 324/2008 de la Comisión, de 9 de abril de 2008 por el que se fijan los procedimientos revisados para las inspecciones de la Comisión en el ámbito de la protección marítima.

Sección 2 – Objeto y alcance

2.1 Objeto del Plan de Protección

El Plan de Protección se confecciona al objeto de proporcionar a la instalación portuaria los estándares de calidad apropiados para garantizar la seguridad de todos los usuarios y trabajadores, permitir la continuidad de las operaciones y minimizar las posibilidades de que se cometan actos ilícitos y sus hipotéticas consecuencias, a la vez que proteger la integridad física de la propia instalación y de los tráficos que hacen uso de la misma.

2.2 Emplazamiento y justificación de la instalación portuaria

La Estación Marítima se emplazará en los muelles de Maliaño, pertenecientes al puerto de Santander, ocupando una superficie aproximada de 80.000 m2 que permitirá el atraque simultáneo de varios buques. Esta ubicación, en pleno centro urbano, responde a la voluntad de facilitar al usuario el rápido y eficaz acceso al cambio del modo de transporte, al comercio y al resto de servicios que se ofrecen en la ciudad (9).

2.3 Actividad de la Estación Marítima y horario de prestación del servicio

La Estación Marítima permitirá el transporte intermodal a los pasajeros procedentes de transbordadores y buques de crucero, prestando servicio principalmente a tráficos procedentes de Inglaterra y otros puertos atlánticos. Se prevé alcanzar la cifra anual de 400.000 pasajeros, generando un valor añadido para la ciudad, favoreciendo las actividades comerciales y de servicios (9).

Su horario operativo responde a un esquema H.18 y se abre desde las 06:00 horas hasta las 24:00 horas (salvo que deba ser ampliado por necesidades del servicio).

2.4 Alcance del Plan de Protección

El Plan de Protección será efectivo en el interior de las instalaciones y el perímetro marino circundante en él contemplado y todas las personas que tengan acceso a las instalaciones, independientemente de los motivos que justifiquen su presencia, deberán cumplir con las estipulaciones en él establecidas.

Este Plan de Protección deberá integrarse en el Plan de Protección del puerto de Santander.

2.5 Gestor de la Estación Marítima y otros operadores internos

A continuación se relacionan los datos de interés del gestor de la Estación Marítima y del resto de operadores que realizan sus actividades en las instalaciones:

REGISTRO DE OPERADORES				
Número	**Nombre**	**Representante**	**Cargo**	**Actividad**
1	*Estación Marítima*			*Gestor Instalación Portuaria*
2	*Naviera Qostera Bis*			*Transporte Marítimo*
3	*Vinci Ferries Bis*			*Transporte Marítimo*
4				
…				

2.6 Proveedores de servicios y suministros; otros operadores externos

REGISTRO DE OPERADORES				
Número	**Nombre**	**Representante**	**Cargo**	**Actividad**
1	*Hipolimp*			*Servicios limpieza*
2	*Hipomant*			*Servicios mantenimiento*
3	*Restotal Bis*			*Servicios restauración*
4				
…				

Sección 3 – Comunicaciones, consultas y coordinación

Objetivo – La comunicación, consulta y coordinación efectiva de las medidas y los procedimientos de seguridad aplicables en las instalaciones de la Estación Marítima.

1) El mecanismo de consulta entre el operador de la Estación Marítima y el resto de organizaciones que desarrollen operaciones en la misma se formalizará a través del Comité Asesor de Protección de la Estación Portuaria, que se reunirá con carácter Mensual en las instalaciones que se habiliten al efecto.
2) La difusión de los asuntos referentes a la seguridad y a la protección se realizará, a todas las partes involucradas, a través del Comité Asesor de Protección de la Estación Marítima.
3) La Autoridad Portuaria, a través del Oficial de Protección del Puerto, transmitirá al gestor de la Estación Marítima todos aquellos asuntos referentes a seguridad marítima que sean de interés; este canal de comunicación también tendrá efectividad a la inversa, por medio del Oficial de Protección de la Estación Marítima.

3.1 Organización del Sistema de Protección

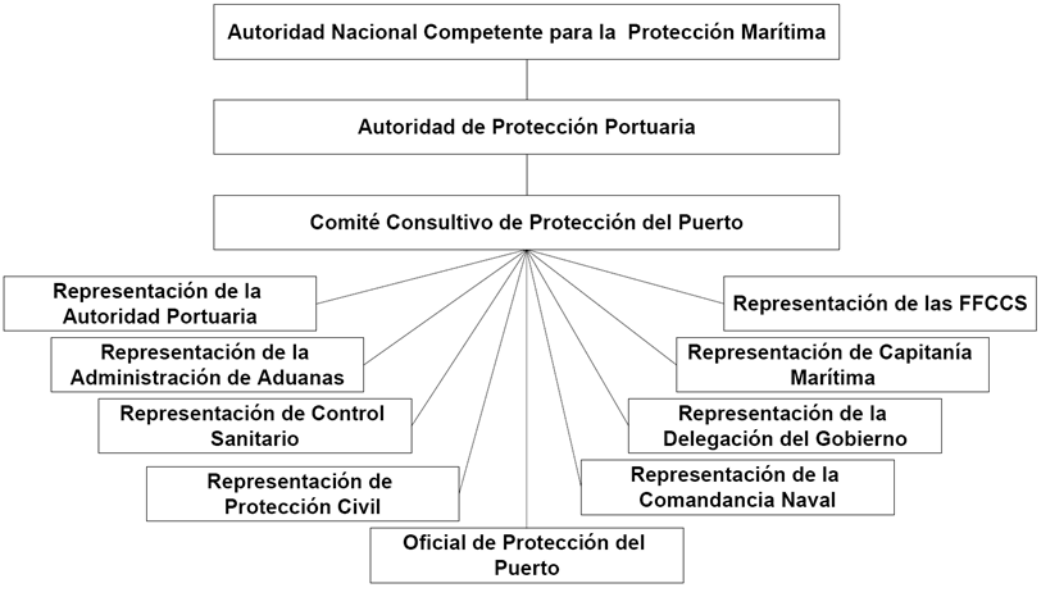


Figura 28: Esquema de organización del Sistema de Protección (31)
Fuente: el autor

3.2 Organización del Sistema de Protección de la Estación Marítima

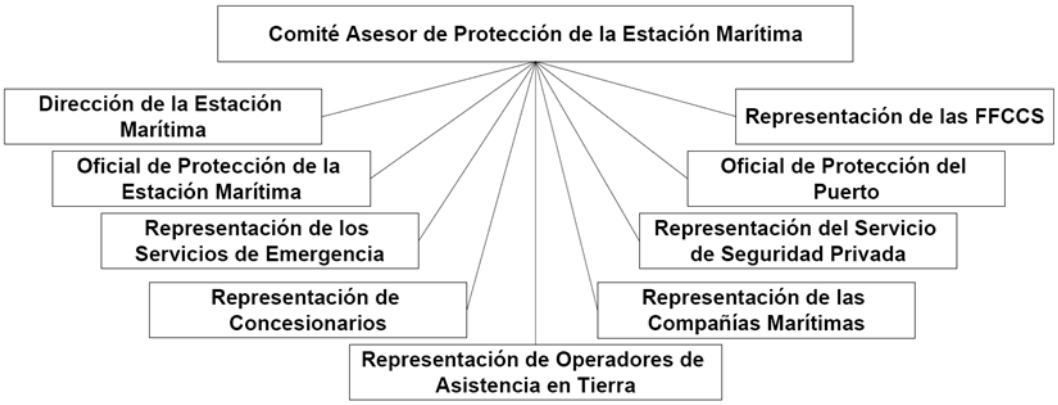


Figura 29: Esquema de organización del Sistema de Protección de la Estación Marítima (31)
Fuente: el autor

3.3 Organización de la Oficina de Seguridad de la Estación Marítima

Figura 30: Esquema de organización de la Oficina de Seguridad de la Estación Marítima
Fuente: el autor

3.4 Comunicación, coordinación y consulta con el resto de organizaciones presentes en el Puerto de Santander

El Plan de Protección de la Estación Marítima no interferirá el cumplimiento de la normativa vigente por parte del resto de empresas y entidades presentes en el Puerto de Santander ni entrará en colisión con los planes de seguridad de otras instalaciones portuarias: para ello, se integrará en el Plan de Protección del Puerto de Santander, previa aprobación por el Comité Consultivo del Puerto de Santander.

La comunicación, consulta y coordinación de las medidas de seguridad establecidas en el Plan se realizará a través del Comité Consultivo del Puerto de Santander, a través del Oficial de Protección del Puerto de Santander. En la medida en que sea oportuno, la Estación Marítima podrá ser representada en dicho comité, previa convocatoria.

3.5 Condiciones generales de seguridad para todas aquellas organizaciones que presten servicios en la Estación Marítima

1) Todas las organizaciones que presten servicios en la Estación Marítima se comprometen a cumplir, íntegramente, las obligaciones prescitas en materia de seguridad marítima, las normas e indicaciones que la complementan y cualesquiera otras que hayan sido establecidas por la Dirección de la instalación portuaria.
2) El coste de todas las medidas que las organizaciones tengan que adoptar a fin de dar cumplimiento a las obligaciones establecidas correrá por su propia cuenta, y se hacen extensivas tanto a su propio personal como a los trabajadores de sus contratas o subcontratas, y de cualquier otra empresa o entidad que tenga algún tipo de relación contractual o de colaboración con ella.
3) Las organizaciones deberán designar responsables de seguridad, que actuarán de interlocutores con la Dirección de la Estación Marítima, en todos los temas relacionados con la seguridad y protección.
4) Solicitarán tarjetas de acreditación personal para todas las personas que deban desempeñar funciones en la Estación Marítima. Las acreditaciones emitidas por la Oficina de Seguridad serán personales e intransferibles y deberán utilizarse con arreglo a las normas de uso correcto de las acreditaciones.

5) Todo el personal acreditado deberá tener conocimientos sólidos en materia de seguridad marítima.
6) Cuando la actividad desarrollada por las organizaciones conlleve la necesidad de acceso de vehículos a la zona restringida, se deberán obtener autorizaciones de acceso de vehículos, siguiendo los procedimientos establecidos al efecto. Las autorizaciones de vehículo emitidas por la Oficina de Seguridad se asignarán para cada vehículo y deberán mostrarse perfectamente visibles mientras dure la necesidad de que los vehículos permanezcan en el interior de dicha área.
7) Los incumplimientos en materia de seguridad portuaria cometidos durante la ejecución de actividades en la Estación Marítima conllevarán, sin perjuicio de las sanciones establecidas por la normativa vigente en materia de seguridad portuaria, la imposición de penalizaciones (32)**.**

3.6 Notificación de cambios en el Nivel de Seguridad Marítimo, y de las directivas de Seguridad

1) Cambios en el Nivel de Seguridad Marítima:

   Las alteraciones en el nivel de seguridad originarán la convocatoria del Comité Asesor de Protección de la Estación Marítima, con carácter ordinario o extraordinario, al objeto de que todas las partes interesadas queden adecuadamente informadas y se traten las medidas que entrarán en vigor mientras permanezca en ese nivel. Se levantará acta de dichas reuniones.
2) Cambios en las directrices de seguridad marítima y/o procedimientos de seguridad:

   Las actualizaciones normativas y de procedimientos locales, y las modificaciones en las directrices de seguridad de la Estación Marítima originarán la convocatoria del Comité Asesor de Protección de la Estación Marítima, con carácter ordinario o extraordinario, al objeto de que todas las partes interesadas queden adecuadamente informadas y se clarifiquen todas las dudas que las mismas puedan suscitar. Se levantará acta de dichas reuniones.

Sección 4 – Revisión y auditoría del Plan de Protección; ejercicios y prácticas; cualificaciones y responsabilidades

4.1 Revisión y Auditoría

Objetivo – Garantizar la efectividad de los procedimientos de revisión y auditoría que aseguren la correcta implementación y mantenimiento del Plan de Protección de la Estación Marítima.

4.1.1 Revisión

El Plan de Protección de la Estación Marítima se revisará y actualizará de manera ordinaria, cada tres años, o de manera extraordinaria cuando se materialice un incidente de seguridad portuaria que ponga de manifiesto alguna deficiencia que requiere ser corregida.

4.1.2 Auditoría

El Plan de Protección de la Estación Marítima se someterá a auditorías externas, realizadas por entidades de reconocido prestigio y con carácter independiente, cada dos años.

El Plan de Protección de la Estación Marítima se someterá a auditorías internas con carácter bianual.

4.2 Ejercicios y prácticas

1) Se realizarán ejercicios de seguridad cada tres meses, salvo que las circunstancias exijan otra cosa, y prácticas cada año, sin que transcurran más de 18 meses entre dos prácticas consecutivas (en éstas podrán participar los oficiales de protección de las instalaciones portuarias, junto con las autoridades de los Gobiernos Contratantes, los Oficiales de Protección de Compañía y los Oficiales de Protección de Buque.
2) Al menos cada dos años, se realizarán ejercicios complejos de alarma general, que requieran de la participación de Autoridades relevantes, FFCCS y de medios de emergencia externos, al objeto de verificar la efectividad de los procedimientos de seguridad y comprobar la adecuación de equipos, métodos de comunicación y de coordinación (27)**.**

4.3 Cualificaciones y responsabilidades

Objetivo – Asegurar que el personal de seguridad de la Estación Marítima se encuentra adecuadamente formado y que tiene los conocimientos apropiados para realizar con garantías sus funciones de supervisión, inspección, control y vigilancia.

4.3.1 Áreas de conocimiento

A nivel general, todo el personal de seguridad de la Estación Marítima deberá disponer de los conocimientos y competencias relevantes para desempeñar con garantías sus funciones en la instalación (33):

De este modo, en la medida de sus responsabilidades, deberán ser conocedores de:

1) La estructura organizativa y administrativa de la Estación Marítima.
2) Las operaciones de embarque y desembarque de pasajeros, equipajes y carga.
3) Los procedimientos de seguridad aplicables en la Estación Marítima.
4) La preparación de respuestas a la emergencia y Planes de Contingencia.
5) El equipamiento de seguridad: medios de seguridad activos y pasivos; principios de funcionamiento y limitaciones de equipos de inspección de personas, vehículos y equipajes, y de sistemas de vigilancia y control de accesos.
6) Métodos de realización de auditorías de seguridad.
7) Métodos de realización de evaluaciones de riesgos de seguridad.
8) Planificación y realización de ejercicios y simulacros de seguridad.
9) Formación en materia de seguridad.
10) Normativa nacional e internacional de seguridad marítima.
11) Funciones y responsabilidades de los FFCCS.
12) Amenazas a la seguridad y patrones de conducta de individuos sospechosos.

4.3.2 Funciones y responsabilidades

1) **Oficial de Protección de la instalación portuaria:**

- Realizar una evaluación inicial de la protección de la instalación portuaria, y otras posteriores con regularidad.
- Garantizar la elaboración y actualización del Plan de Protección de la instalación portuaria.
- Implementar el Plan de Protección de la instalación portuaria y su programa de ejercicios y simulacros de protección.
- Establecer un programa de inspecciones para la protección de la instalación portuaria y dar seguimiento a las medidas detectadas, así como emitir recomendaciones y/o modificaciones al Plan de Protección de la instalación portuaria que permitan corregir deficiencias, buscando siempre puntos de mejora continua.
- Motivar, inducir y capacitar al personal en la toma de acciones preventivas y correctivas de protección de las instalaciones portuarias.
- Asegurarse de que se ha impartido la formación adecuada al personal responsable de la protección de la instalación portuaria.
- Coordinar con el Oficial de Protección del puerto y con las FFCCS todos los aspectos de la seguridad, dando notificación a las autoridades que correspondan, de los sucesos que considere amenazas para las instalaciones portuarias, llevando un registro de control y seguimiento interno de las mismas.
- Coordinar la implementación del Plan de Protección de la instalación portuaria con los Oficiales de Protección de Buques, personal de la empresa y servicios internos y externos asignados a la protección marítima, asegurándose se cumplan con las normas relativas a la protección de las instalaciones.
- Supervisar el funcionamiento, prueba, calibrado y mantenimiento adecuados de los equipos de protección.

2) Apoyar a los oficiales de protección de Buques en la verificación de identidad del personal que aborda las embarcaciones (33)**.**

3) **Fuerzas y Cuerpos de Seguridad**:

Conforme al artículo 104 de la Constitución española, es misión de las Fuerzas y Cuerpos de Seguridad del Estado proteger el libre ejercicio de los derechos y libertades, y garantizar la seguridad ciudadana. En este contexto, La Ley Orgánica 2/86 de Fuerzas y Cuerpos de Seguridad del Estado define las competencias funcionales y territoriales de los diferentes Cuerpos de Seguridad del Estado.

- Guardia Civil: entre otras responsabilidades, la Guardia Civil debe velar por el control de las armas y explosivos; el Resguardo Fiscal del Estado; el tráfico interurbano; la custodia de las vías de comunicaciones, puertos y aeropuertos y la protección de la naturaleza (34).
- Cuerpo Nacional de Policía: corresponde al Cuerpo Nacional de Policía, entre otras, la responsabilidad del control de entrada y salida de nacionales y extranjeros en el territorio nacional, control de documentación, las responsabilidades previstas en la legislación sobre extranjería, refugio y asilo, extradición, expulsión, emigración e inmigración, y el control de la seguridad privada (35).
- Policía Local: tiene asignadas, entre otras, todas las funciones relacionadas con el tráfico y la seguridad vial en el término municipal; la gestión del depósito municipal de vehículos y los objetos perdidos; la vigilancia de espacios públicos y la vigilancia del cumplimiento de las Ordenanzas y Bandos municipales (36).

4) **Servicio de Seguridad Privada**: dependiente del oficial de seguridad de la Estación Marítima, en representación de la Dirección de la instalación para todo lo relacionado con asuntos de seguridad, cuenta con una estructura de medios humanos que se detalla a continuación:

- Coordinador del Servicio de Seguridad:
    - Organizar el Servicio de Seguridad de la Estación Marítima, comprobando la correcta asignación de los recursos necesarios para la prestación de los servicios.
    - Verificar la correcta aplicación de los procedimientos operativos, conforme a los criterios de calidad exigidos, planificando y supervisando los controles internos de cada puesto.

  - Garantizar la adecuada formación del personal bajo su responsabilidad.
  - Garantizar que se cumplen las normas de seguridad de la instalación por el personal propio y por todo el colectivo de trabajadores y usuarios.
  - Registrar todas incidencias o no conformidades y diseñar acciones correctoras inmediatas para enmendarlas; realizar el seguimiento de dichas acciones para verificar su efectividad.
  - Realizar propuestas de mejora, mediante la detección de puntos débiles y puntos mejorables.

- Inspector de Seguridad:
  - Supervisar el Servicio de Seguridad en tiempo real.
  - Atender a todas las cuestiones que surgen en tiempo real, facilitando su resolución mediante la correcta aplicación de la normativa y procedimientos específicos de seguridad.
  - Dirigir al personal bajo su responsabilidad, estableciendo prioridades cuando sea necesario.
  - Coordinar todos los medios materiales de seguridad para lograr la máxima efectividad del servicio.
  - Es el responsable de la custodia y control de llaves.
- Vigilantes de Seguridad:

Al margen de las funciones explícitas que tengan asignadas en los procedimientos operativos de seguridad realizarán las siguientes:

  - VS Centro de Control: en constante comunicación con el resto de VS de servicio, se encarga del control del sistema de CCTV recogiendo imágenes de cualquier incidente, y atiende a llamadas de interfonos; gestiona la apertura remota de puertas automáticas.
  - VS Patrulla terrestre: realiza patrullas periódicas por el interior y exterior del terminal comprobando puertas y otros accesos; intercepta a cualquier persona que no porte visible su identificación personal en las zonas restringidas o controladas.

  - VS Patrulla marítima: comprueba la identidad de toda embarcación que entre dentro del perímetro de seguridad de la instalación, instando a abandonar a aquellas que no deban permanecer en él.
  - VS Controles de acceso: se ocupan de que todas las personas que accedan a través de los puestos que ocupan estén acreditadas conforme a los procedimientos y porten visible su acreditación.
  - VS Controles de seguridad: se ocupan de realizar las inspecciones de seguridad en los puntos de control para asegurar que no se introducen artículos u objetos no permitidos.
- Auxiliares de Seguridad:

Asisten al pasajero en su paso por los controles de seguridad informando de todos aquellos objetos que no se pueden transportar, gestionando los medios materiales que la Estación Marítima pone a disposición, y controlan las salas de recogida de equipajes para solventar las incidencias o reclamaciones que allí se generen.

Sección 5– Medidas y procedimientos de seguridad

Objetivo – Asegurar que existen medidas y procedimientos efectivos y conformes a la normativa vigente para tratar las amenazas de seguridad y el control de accesos.

5.1 Procedimientos básicos de seguridad

Si bien son numerosos los procedimientos que pueden establecerse en función de las particularidades y circunstancias que rodean la operativa de la Estación Marítima, se listan una serie de ellos que parecen indispensables para la correcta gestión de la seguridad y de la protección (27); estos procedimientos locales deberán desarrollarse por personal cualificado, y ser estudiados y aprobados en el seno del Comité Asesor de Protección de la Estación Marítima, con el acuerdo de la mayoría de las organizaciones allí representadas.

1) Procedimiento de emisión de acreditaciones.
2) Procedimientos de vigilancia, control y operaciones de seguridad.
3) Procedimientos de introducción de armas y/o material peligroso autorizado, equipajes no acompañados, provisiones y suministros.
4) Procedimiento de comunicación de incidentes de seguridad.
5) Procedimiento de cambio de nivel de emergencia.
6) Procedimiento para la calificación de la zona restringida temporal.
7) Procedimiento de acceso de medios de emergencia.
8) Procedimiento de evaluación de idoneidad del personal para el libre acceso a las zonas controladas y restringidas de la Estación Marítima.
9) Procedimiento de accesos de tripulaciones, suministradores y prestadores de servicios.
10) Procedimiento de evacuación del edificio terminal y/o instalaciones exteriores.
11) Procedimiento de respuesta a la recepción de señales de alarma de buques en las instalaciones.
12) Procedimiento de notificación de sucesos que afectan a la protección.
13) Procedimiento de difusión de la información contenida en el plan.

14) Procedimiento para facilitar el permiso de tierra del personal del buque, relevos y visitas.
15) Procedimientos de comunicación entre los diferentes actores de seguridad (Oficial de Protección de la Estación Marítima, Oficial de Protección del Buque y Oficial de Protección de Compañía).

5.2 Niveles de Seguridad:

5.2.1 Medidas de control de accesos:

- **Nivel 1:**

1) Se incluyen medidas para verificar la identidad de todas las personas que pretenden acceder a las áreas controladas y restringidas, que deben portar tarjetas de embarque, documentos de tripulante, acreditación portuaria o tarjeta de visitante.
2) El 100 % de las personas que acceden a la zona restringida deberá pasar por los Arcos Detectores de Metales para verificar que no generan alarmas metálicas.
3) Se inspeccionarán de manera aleatoria el 50% de los vehículos que pretendan acceder a las zonas restringidas, al objeto de que no se introduzcan desde el exterior armas, explosivos o material incendiario.
4) Se denegará el acceso de aquellas personas que no deseen o no puedan acreditar su identidad o justificar su presencia en las zonas no abiertas al público; se llevará un registro de las incidencias de este tipo.

- **Nivel 2:**

Se implantan medidas adicionales de seguridad, como sigue:

1) Se verifica la necesidad de acceso a las instalaciones del personal acreditado.
2) Se incrementa la inspección aleatoria de los vehículos que pretenda acceder a la zona restringida, al 75 %.
3) Se incrementan los controles de los equipajes no acompañados, el correo y la carga.
4) Se incrementan las rondas de patrulla interior, exterior y marítima.

5) Se coordina con la Autoridad Portuaria la vigilancia de la zona contigua a la zona marítima controlada.
6) Se controlan los accesos que no se realicen por los puntos de acceso establecidos (únicamente utilizables por personal autorizado de FFCCS).

- **Nivel 3:**

Se aplican algunas o todas, entre siguientes medidas adicionales de seguridad:

1) No se permite el acceso de personas a las zonas restringidas, salvo que su presencia esté justificada por motivos laborales.
2) Se restringe el acceso a las zonas controladas, salvo que se justifique por motivos laborales.
3) Se bloquean los accesos a la zona restringida por todas las lectoras, salvo las correspondientes a los puntos de acceso establecidos.
4) Se realizan, con regularidad, inspecciones exhaustivas del edificio terminal de pasajeros, zona perimetral y zonas contiguas al objeto de detectar bultos o artefactos sospechosos prestando especial atención a los recovecos y lugares que puedan albergar dispositivos ocultos.
5) En referencia al equipaje, carga y correo no acompañados, se determinará en coordinación con las FFCCS, si se acepta mediante inspecciones exhaustivas, si se restringe o se suspende su manipulación, o si se rechaza.
6) Se coordinará la disponibilidad de medios de emergencia con las organizaciones implicadas (protección civil, emergencias, servicio de extinción de incendios, FFCCS…).
7) Restricción de acceso y salida de tripulaciones.
8) Restricción de acceso a las instalaciones, salvo medios de respuesta a incidentes o amenazas a la seguridad.
9) Se suspenden las operaciones de suministro y aprovisionamiento.
10) Se suspenden las operaciones de embarque y desembarque de pasajeros.
11) Se evacúa el terminal y/o perímetro.

5.2.2 Medidas de aceptación de carga, suministros y correo:

- **Nivel 1:**

1) Se comprobará toda la carga, suministros y correo que se introduzca en la instalación, con los albaranes generados por sus respectivos emisarios. En caso de detectar que no se corresponden, se rechazará su entrada en las instalaciones.
2) Se comprobarán todos los precintos y envoltorios de los artículos que se introduzcan en las zonas restringidas destinados a ser transportados como carga, suministros y correo. En caso de detectar que se han manipulado, se rechazarán o se someterán a inspecciones exhaustivas.
3) Se recibirá, de las Compañías Marítimas, información avanzada respecto de la entrega de suministros y provisiones; los proveedores deberán estar en posesión de acreditaciones personales y autorizaciones de vehículos.
4) Se inspeccionarán de manera aleatoria el 50% de los vehículos y el 50% de la carga que se introduzca para ser embarcada.
5) La carga, suministros y correo que haya pasado los controles de seguridad se depositará en una zona concreta establecida al efecto, vigilada y a salvo de manipulaciones.

- **Nivel 2:**

Se implantan medidas adicionales de seguridad, como sigue:

1) Se inspeccionarán de manera aleatoria el 75 % de los vehículos y el 75 % de la carga, suministro, provisiones y correo que se introduzca para ser embarcado.
2) Se vigilarán más frecuente y concienzudamente las zonas de depósito de carga, suministros y correo.
3) Se depositarán por separado en las zonas destinadas al efecto: la carga, los suministros y el correo que vayan a ser embarcados.

- **Nivel 3:**

Se aplican algunas o todas, entre siguientes medidas adicionales de seguridad:

1) Se restringe o suspende el movimiento de carga, suministros o correo.
2) Se confirma el inventario y la localización de todo el material en depósito destinado a ser embarcado.
3) Se rechaza la introducción de suministros, provisiones, carga y correo.

5.2.3 Medidas de vigilancia y control:

- **Nivel 1:**

1) Se vigilarán continuadamente las instalaciones así como sus accesos terrestres y marítimos.
2) Se vigilarán continuadamente las operaciones que se desarrollen en la interfaz buque/puerto.
3) La iluminación artificial será adecuada a los propósitos anteriores.

- **Nivel 2:**

1) Se incrementará el número de patrullas terrestres y marítimas.
2) Se establecerán procedimientos de comunicación regular con el centro de control.
3) Se proporcionará el máximo grado de iluminación.
4) Se destinarán todos los recursos posibles, a este cometido.

- **Nivel 3:**

Se prestará asistencia a las FFCCS, si así fuere requerido (33)**.**

Sección 6– Zonas de seguridad

6.1 Creación de Zonas de Seguridad

La creación de zonas de seguridad responde, en primera instancia, a un esquema conocido como ***defensa en profundidad***, en diferentes entornos sucesivos (asimilables a las capas de una cebolla), desde el exterior hasta el interior de las instalaciones. Con este esquema se pretende detectar en el menor tiempo posible un intento de intrusión, proporcionando de esta manera el menor tiempo de reacción (5). Los siguientes son otros objetivos complementarios:

1) Controlar el movimiento de las personas, vehículos y embarcaciones en el interior de las instalaciones.
2) Restringir los accesos a los mínimos necesarios.
3) Prevenir la interferencia con los pasajeros, trabajadores, embarcaciones e instalaciones.
4) Asegurar la protección.

En este caso, se establecen diferentes zonas de seguridad, en función de la criticidad de cada una de ellas, y se restringen los requisitos de acceso conforme a la necesidad de acceder de las personas (32):

1) Zonas públicas: son zonas de libre acceso, abiertas al tránsito de trabajadores y usuarios; en ellas no se permite la realización de trabajos ni actividades sin el conocimiento y autorización previos de la Oficina de Seguridad.
2) Zonas de acceso controlado: el acceso a estas áreas se autoriza a los trabajadores con necesidad de acceder, únicamente surgida en relación con motivos laborales; los usuarios podrán acceder a estas áreas, exclusivamente en su tránsito a través de las instalaciones o para realizar gestiones relacionadas con sus contratos de transporte con la Compañía Marítima (recogida de equipajes, reclamaciones, acompañamiento de menores…).
3) Zona marítima controlada: el acceso al perímetro marítimo de seguridad se autoriza únicamente a las embarcaciones que deban prestar asistencia o servicios a la instalación marítima o a los buques en ella atracados. Los requisitos de acceso a esta área deberán estar reflejados en un procedimiento.

4) Zonas restringidas de seguridad: se requiere disponer de un documento válido para pasar el control de acceso a estas zonas (acreditación portuaria, acreditación de tripulante, tarjeta de visitante, tarjeta de embarque aceptada por un transportista marítimo…), además de pasar un control de seguridad al objeto de garantizar que no se portan artículos no permitidos que puedan emplearse para la comisión de actos ilícitos. Al igual que en el caso de las zonas de acceso controlado, un procedimiento deberá recoger los requisitos de acceso a la zona restringida, para todo tipo de usuarios (pasajeros, tripulantes, proveedores, empleados), tanto a pie como con vehículo.
5) Zona restringida temporal: zona que puede calificarse de pública o restringida, en función de las necesidades de la Estación Marítima. En el tránsito de zona pública a zona restringida temporal deberá tenerse la certeza de que el área así calificada es estéril; para ello, deberá confeccionarse un procedimiento que así lo contemple.

6.2 Zonas de seguridad en el interior del edificio terminal:

1) Planta de Salidas:

- La zona pública comprende el vestíbulo de facturación y los espacios comerciales.
- La zona de acceso controlado da paso al bloque técnico.
- La zona restringida de seguridad incluye las zonas de embarque, una vez rebasado el control de seguridad.
- La zona restringida de seguridad temporal es un área que puede servir como zona pública o zona restringida, en función de las necesidades, debido al lugar estratégico que ocupa.

2) Planta de Llegadas:

- La zona pública corresponde a la zona de espera para uso púbico.
- Las zonas de acceso controlado incluyen el bloque técnico y las salas de recogida de equipajes nacional e internacional.
- La zona restringida de seguridad abarca el patio de carrillos y la zona previa al control de documentación, en el puesto fronterizo.

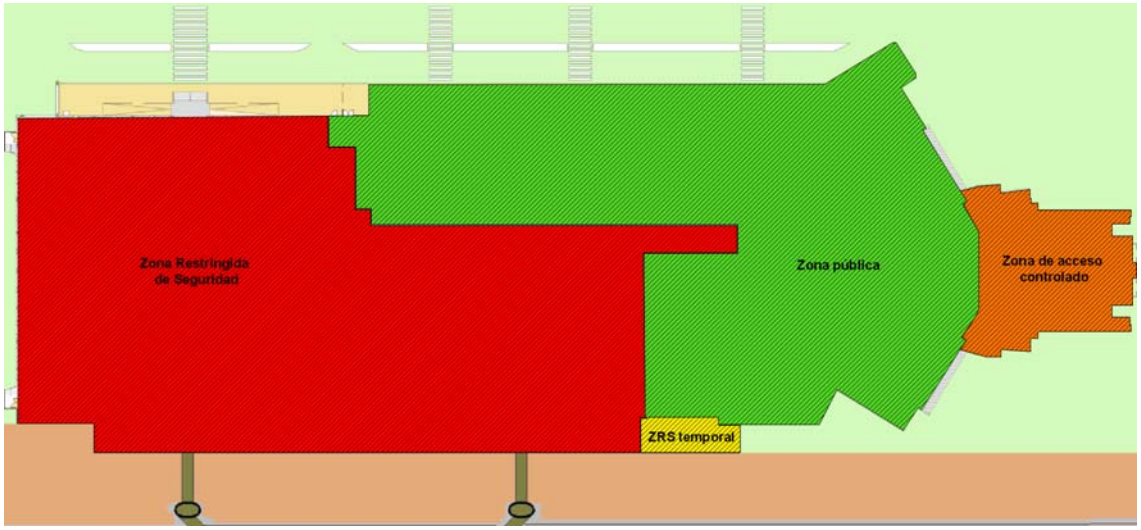


Figura 31: Zonas de seguridad en planta de salidas
Fuente: el autor

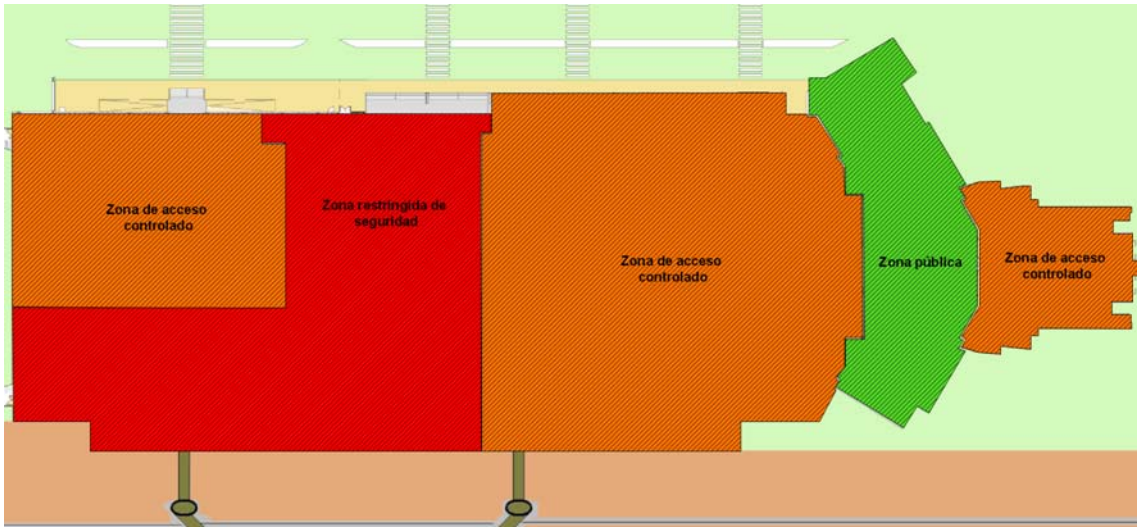


Figura 32: Zonas de seguridad en planta de llegadas
Fuente: el autor

6.3 Zonas de seguridad en el exterior del edificio terminal:

1) Zonas de seguridad terrestres:

- La zona pública se corresponde con los viales de acceso a la Estación Marítima y las áreas destinadas al aparcamiento público de vehículos.
- No se han establecido zonas de acceso controlado exteriores, salvo la marítima.
- La zona restringida de seguridad está cerrada y rodeada por el vallado perimetral; los requisitos de acceso a esta zona son similares al acceso a las zonas restringidas de seguridad interiores. Se considera una zona estéril.

2) Zona de seguridad marítima:

- No se ha determinado una zona restringida de seguridad marítima, dada la dificultad de inspeccionar con profundidad a las posibles embarcaciones que accedan a prestar servicio, para garantizar razonablemente que no se introducen armas no autorizadas ni artículos prohibidos; no obstante, un procedimiento deberá regular el control de las operaciones de todas las embarcaciones que accedan a prestar servicio.
- Se establece una zona marítima controlada que proporciona un perímetro de seguridad delimitado por medio de una barrera flotante; un procedimiento deberá reflejar los requisitos de acceso de las embarcaciones a dicha área.

Figura 33: Zona restringida terrestre
Fuente: el autor sobre fondo de Google Maps

Figura 34: Zona marítima controlada
Fuente: el autor sobre fondo de Google Maps

6.4 Puntos de acceso (puntos de entrada y salida) a las áreas controladas y restringidas:

Los puntos de acceso interiores y exteriores deben reducirse al mínimo y sus propósitos deben estar específicamente definidos.

En este caso, se establecen puntos de acceso a áreas controladas y puntos de acceso a áreas restringidas; los primeros se controlan mediante medios técnicos (lectoras y circuito cerrado de televisión) mientras que el acceso a las zonas restringidas se realiza también con medios humanos, con objeto de garantizar que ninguna persona accede sin los privilegios preceptivos.

1) Puntos de entrada a áreas controladas: existen seis puntos de acceso a áreas controladas (uno exterior para el acceso de embarcaciones a la zona marítima controlada, uno en planta de salidas y otros cuatro en planta de llegadas), dotados de los medios necesarios para realizar el control de acceso, que debe ser conforme a los procedimientos establecidos al efecto.
2) Puntos de entrada a zonas restringidas: existen dos puntos de acceso a zonas restringidas de seguridad dotados de equipos de inspección (uno en la planta de salidas de la Estación Marítima y otro en la cabina de control exterior), por los que pasajeros y trabajadores deberán acceder necesariamente pasando los preceptivos controles de seguridad. Los accesos a estas áreas deberán ser conformes con los procedimientos aplicables.
3) Puntos de salida de zonas controladas: con la excepción de la sala de llegadas nacionales/Schengen, son los mismos que los puntos de entrada; se controlan mediante lectoras para que tanto las entradas como las salidas queden registradas en el sistema.
4) Puntos de salida de zonas restringidas: existen dos puntos de salida de estas zonas (uno interior y otro exterior), y obligan a abandonar las instalaciones por la aduana. Ninguna persona puede abandonar la zona restringida sin ser sometida al control fiscal.

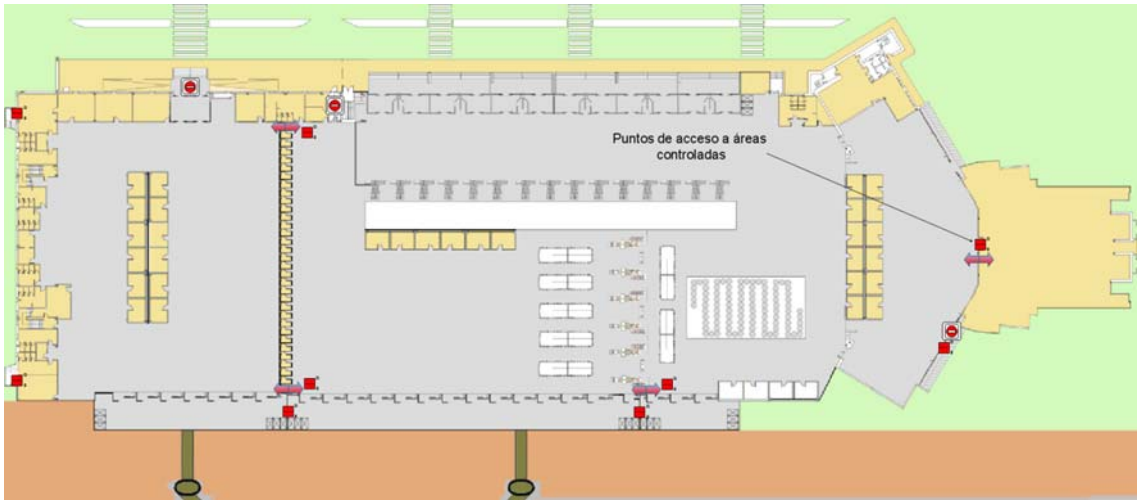


Figura 35: Acceso a área de acceso controlado, en planta de salidas
Fuente: el autor

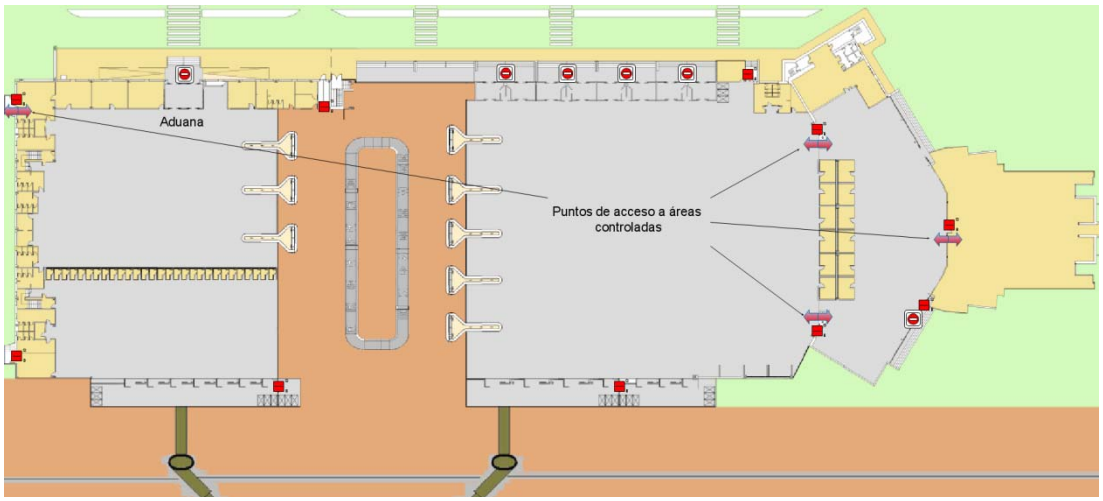


Figura 36: Acceso a área de acceso controlado en planta de llegadas
Fuente: el autor

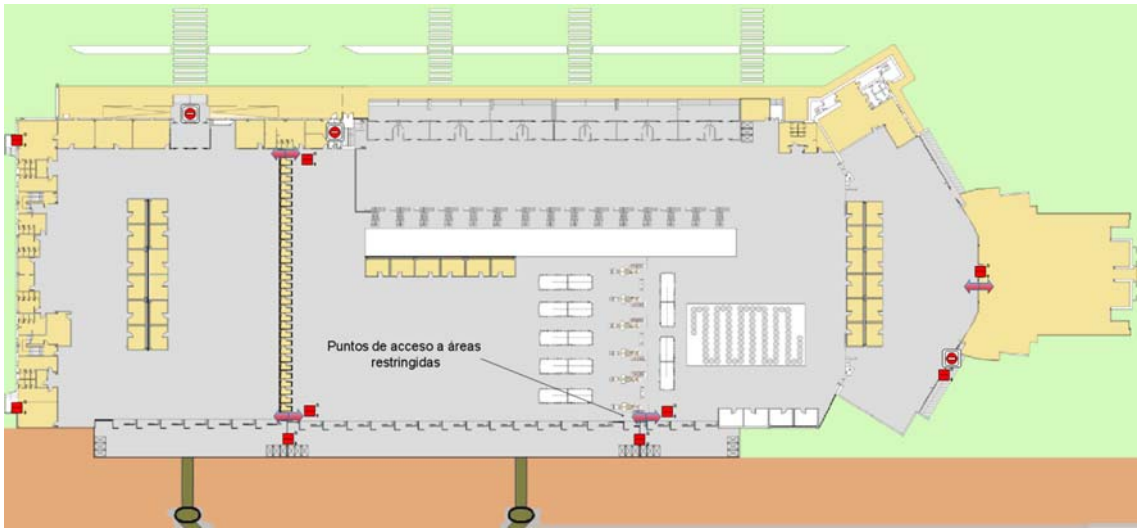


Figura 37: Acceso a zona restringida de seguridad en planta de salidas
Fuente: el autor

Figura 38: Acceso exterior a zona restringida de seguridad
Fuente: el autor sobre fondo de Google Maps

Figura 39: Acceso exterior a zona marítima controlada
Fuente: el autor sobre fondo de Google Maps

Sección 7– Instalaciones particulares de seguridad

7.1 Cerramiento perimetral terrestre

1) Seguridad pasiva

Dada la configuración prácticamente lineal de la zona restringida, se dispone un murete de hormigón de 1 metro de altura en el que se encastren paneles de mallas rectangulares electrosoldados (15) (16), de 2 metros de altura. La parte superior se dota de doble bayoneta de 50 cm., inclinada 45º respecto de la vertical y alambre de espino. La altura total del muro: 3, 25 metros.

Los postes, de acero galvanizado de 60 mm. de diámetro y 1,50 mm. de grosor, se colocan a una distancia de 2,5 m. del adyacente. Su altura mínima es de 2,0 m. desde el encastre hasta el punto en que conectan con las bayonetas.

Las bayonetas dobles de 50 cm. nacen en los extremos de los postes, al objeto de dificultar la intrusión, inclinadas 45º con respecto a la vertical y orientadas hacia el exterior y hacia el interior. Llevan instaladas cuatro líneas de alambre de espino galvanizado.

Para complementar la seguridad pasiva del perímetro se dispondrán bolardos dispuestos en una línea paralela al vallado perimetral, a lo largo de toda su longitud, separados dos metros respecto del murete y vallado, y a una distancia de dos metros uno de otro: estos bolardos impedirán el estacionamiento de vehículos junto al vallado, que podrían servir de trampolín para sortearlo o que podrían contener explosivos. Serán escamoteables en aquellos puntos en los que coincidan con puertas motorizadas automáticas perimetrales.

2) Sistemas activos de seguridad perimetral:

Detección perimetral: instalación de cable microfónico a lo largo de todo el vallado, integrado en los paneles de malla (15), complementado con banda sensora antiasalto en la parte superior.

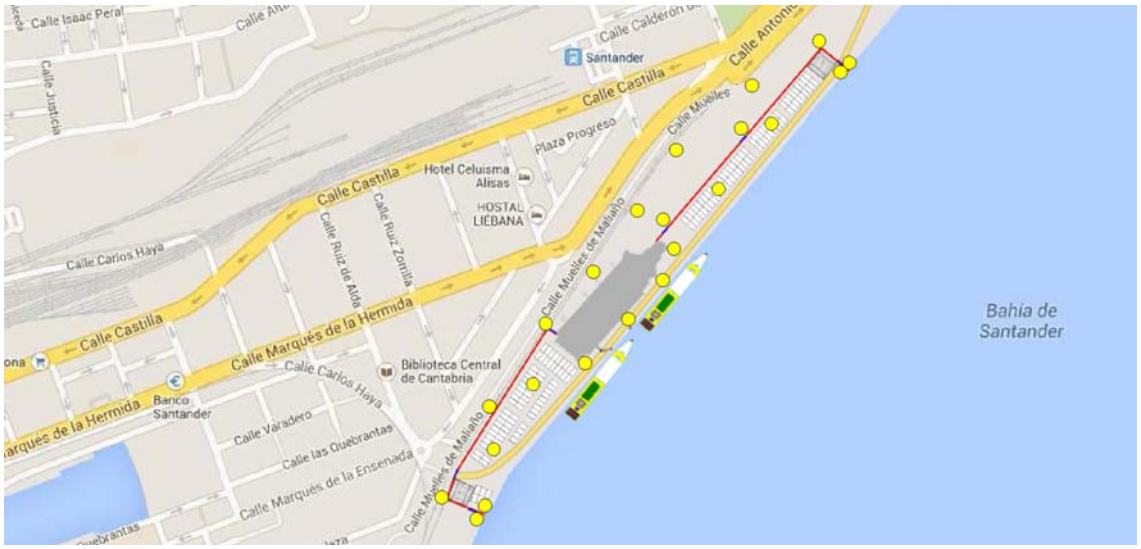


Figura 40: Límite del cerramiento perimetral terrestre (en rojo) y disposición de luminarias de seguridad
Fuente: el autor sobre fondo de Google Maps

7.2 Cerramiento de la zona marítima controlada

Se propone una configuración estándar de flotadores con dos líneas de cable de acero de alta resistencia, capaz de detener eficazmente embarcaciones de pequeñas dimensiones, provista de iluminación nocturna (14).

La altura del cable superior respecto del nivel del mar es de 90 cm., aproximadamente; monta señalización disuasoria y mecanismo de apertura suficiente para el acceso de las embarcaciones a las que sirve.

Figura 41: Límite del cerramiento perimetral marítimo (en rojo)
Fuente: el autor sobre fondo de Google Maps

7.3 Sistema de CCTV

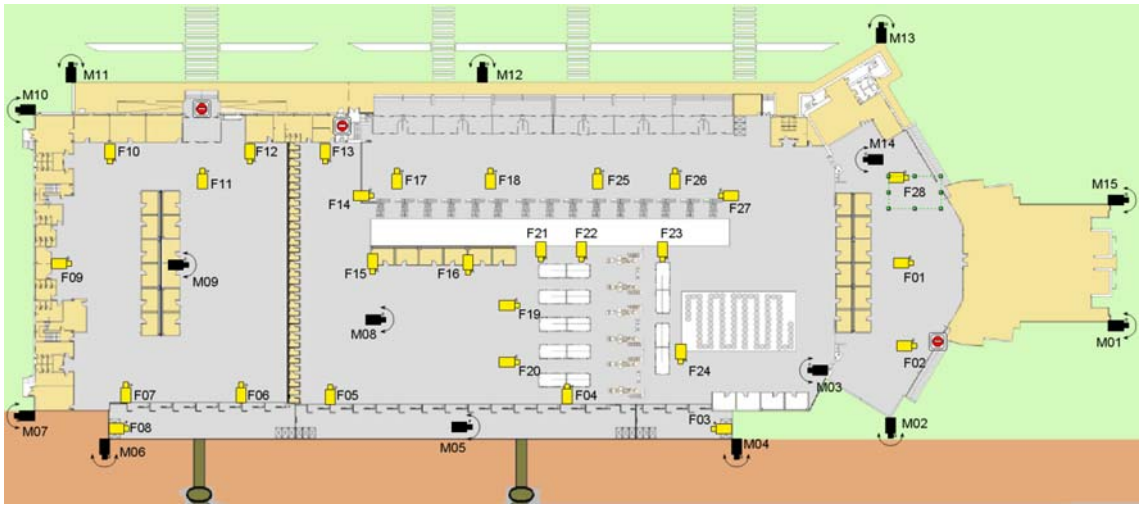


Figura 42: Cámaras y domos en planta de salidas
Fuente: el autor

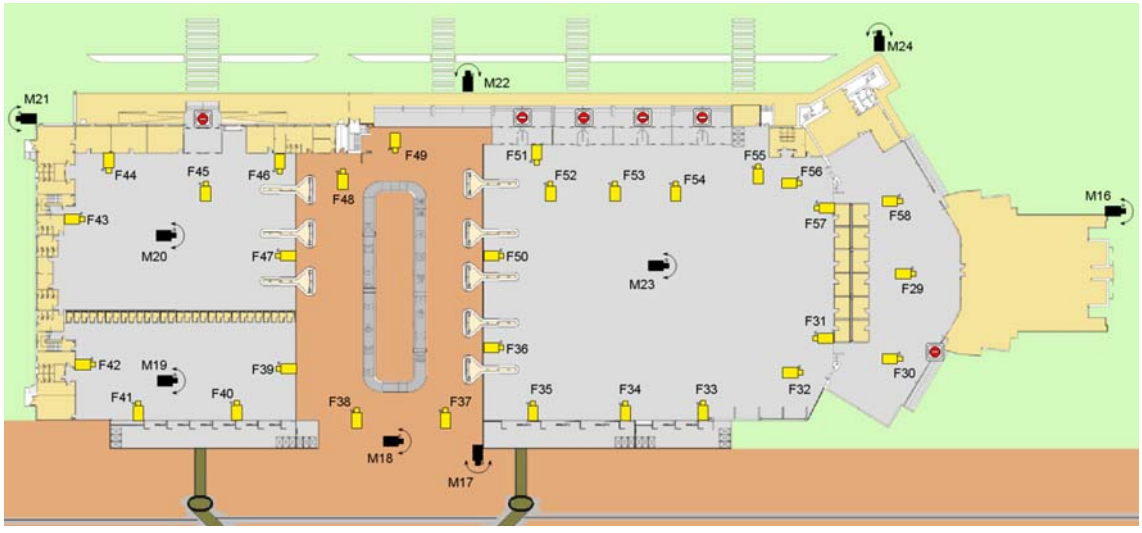


Figura 43: Cámaras y domos en planta de llegadas
Fuente: el autor

Figura 44: Cámaras y domos en exteriores
Fuente: el autor sobre fondo de Google Maps

Listado de cámaras y domos; nomenclatura y datos de interés:

CÁMARAS				
Nº	**MODELO**	**IP**	**Nº SERIE**	**MAC**
F01	Dinion IP 71000 HD	187.101.177.1	55550068245	00-02-62-32-J4-F5
F02	Dinion IP 71000 HD	187.101.177.2	55550057346	00-06-66-78-J3-F0
F03	Dinion IP 71000 HD	187.101.177.3	55553021657	00-09-87-M8-L5-88
F04	Dinion IP 71000 HD	187.101.177.4	55556021684	00-99-93-86-M2-R5
F05	Dinion IP 71000 HD	187.101.177.5	55557024595	00-08-44-KL-9Y-DE
F06	Dinion IP 71000 HD	187.101.177.6	55557021679	00-08-97-54-G7-T1
F07	Dinion IP 71000 HD	187.101.177.7	55550002467	00-33-9T-5H-77-4H
F08	Dinion IP 71000 HD	187.101.177.8	55550002469	00-22-H2-H2-T2-4S
F09	Dinion IP 71000 HD	187.101.177.9	55550009735	00-11-6L-44-G4-D2
F10	Dinion IP 71000 HD	187.101.177.10	55555002137	00-16-63-15-Y7-LA
F11	Dinion IP 71000 HD	187.101.177.11	55550014581	00-28-D8-RY-J8-78
F12	Dinion IP 71000 HD	187.101.177.12	55550008756	00-55-38-76-HD-F7
F13	Dinion IP 71000 HD	187.101.177.13	55550003468	00-66-95-76-HD-P2
F14	Dinion IP 71000 HD	187.101.177.14	55550031695	00-55-9F-5J-Y6-W9
F15	Dinion IP 71000 HD	187.101.177.15	55550031677	00-55-8F-52-TW-4E
F16	Dinion IP 71000 HD	187.101.177.16	55550071167	00-44-59-NB-14-7A
F17	Dinion IP 71000 HD	187.101.177.17	55550074747	00-66-63-96-41-7N
F18	Dinion IP 71000 HD	187.101.177.18	55550094347	00-00-51-3R-0H-Z5
F19	Dinion IP 71000 HD	187.101.177.19	55550074674	00-44-48-15-K2-JH
F20	Dinion IP 71000 HD	187.101.177.20	55550016184	00-44-75-38-FD-VC
F21	Dinion IP 71000 HD	187.101.177.21	55550009565	00-55-56-76-GF-J6
F22	Dinion IP 71000 HD	187.101.177.22	55550074619	00-55-84-14-96-S7
F23	Dinion IP 71000 HD	187.101.177.23	55550014875	00-55-41-5H-8D-FG
F24	Dinion IP 71000 HD	187.101.177.24	55550066575	00-44-95-DS-47-RE
F25	Dinion IP 71000 HD	187.101.177.25	55550036484	00-44-1B-SA-65-D8
F26	Dinion IP 71000 HD	187.101.177.26	55550010861	00-44-DR-84-JL-1D
F27	Dinion IP 71000 HD	187.101.177.27	55550000648	00-55-DS-89-F5-G4
F28	Dinion IP 71000 HD	187.101.177.28	55550010464	00-44-66-8G-04-DP
F29	Dinion IP 71000 HD	187.101.177.29	55550027878	00-44-HB-12-33-41
F30	Dinion IP 71000 HD	187.101.177.30	55550057847	00-55-41-BG-G6-J0
F31	Dinion IP 71000 HD	187.101.177.32	55550099734	00-55-4N-2F-6N-84
F32	Dinion IP 71000 HD	187.101.177.33	55550099437	00-55-FF-8G-00-S9
F33	Dinion IP 71000 HD	187.101.177.34	55557045598	00-44-F9-V7-S5-A2
F34	Dinion IP 71000 HD	187.101.177.35	55550011577	00-55-FV-75-GG-S5
F35	Dinion IP 71000 HD	187.101.177.36	55550099144	00-55-D8-F8-W2-C8

F36	Dinion IP 71000 HD	187.101.177.37	55550011587	00-66-1B-3G-R5-46
F37	Dinion IP 71000 HD	187.101.177.38	55550008872	00-44-9C-R3-S9-F4
F38	Dinion IP 71000 HD	187.101.177.39	55550228848	00-55-DD-99-S6-2W
F39	Dinion IP 71000 HD	187.101.177.40	55550097541	00-44-F9-S6-H7-04
F40	Dinion IP 71000 HD	187.101.177.41	55550014897	00-44-45-8H-FF-D5
F41	Dinion IP 71000 HD	187.101.177.42	55550093456	00-55-07-98-FF-E7
F42	Dinion IP 71000 HD	187.101.177.43	55550014763	00-55-07-24-PP-E7
F43	Dinion IP 71000 HD	187.101.177.44	55550055684	00-55-07-98-YY-SS
F44	Dinion IP 71000 HD	187.101.177.45	55550033298	00-55-07-KK-AA-K9
F45	Dinion IP 71000 HD	187.101.177.46	55550024646	00-55-07-JJ-96-S3
F46	Dinion IP 71000 HD	187.101.177.47	55550010147	00-55-07-ZZ-95-YY
F47	Dinion IP 71000 HD	187.101.177.48	55550003321	00-55-07-SJ-JJ-9F
F48	Dinion IP 71000 HD	187.101.177.49	55550056587	00-55-07-88-D9-67
F49	Dinion IP 71000 HD	187.101.177.50	55550036541	00-55-07-DY-Y9-DY
F50	Dinion IP 71000 HD	187.101.177.51	55550039577	00-55-07-SS-65-YD
F51	Dinion IP 71000 HD	187.101.177.52	55550036541	00-44-VV-65-WR-TS
F52	Dinion IP 71000 HD	187.101.177.53	55550031468	00-44-H6-TT-R3-65
F53	Dinion IP 71000 HD	187.101.177.54	55550041284	00-44-RR-E9-E6-54
F54	Dinion IP 71000 HD	187.101.177.55	55550036666	00-44-R6-E6-S9-B3
F55	Dinion IP 71000 HD	187.101.177.56	55550037777	00-44-RR-G3-0W-0L
F56	Dinion IP 71000 HD	187.101.177.57	55550036677	00-44-ZV-65-FR-TS
F57	Dinion IP 71000 HD	187.101.177.58	55550036111	00-44-EV-65-WG-5S
F58	Dinion IP 71000 HD	187.101.177.59	55550033236	00-44-VA-99-9R-9S
F59	Dinion IP 71000 HD	187.101.177.60	55550038874	00-44-ER-87-A9-T1
F60	Dinion IP 71000 HD	187.101.177.61	55550031121	00-44-62-15-41-T5
F61	Dinion IP 71000 HD	187.101.177.62	55550066584	00-44-87-65-WR-96
F62	Dinion IP 71000 HD	187.101.177.63	55550036694	00-44-TT-65-DC-71
F63	Dinion IP 71000 HD	187.101.177.64	55550030001	00-44-PL-36-21-47
M01	IP Dynamic 7000 HD	187.101.177.65	77770030001	00-77-TY-32-54-77
M02	IP Dynamic 7000 HD	187.101.177.66	77770030002	00-77-GF-32-DS-63
M03	IP Dynamic 7000 HD	187.101.177.67	77770030003	00-77-HG-G6-2G-54
M04	IP Dynamic 7000 HD	187.101.177.68	77770030004	00-77-GW-98-W9-71
M05	IP Dynamic 7000 HD	187.101.177.69	77770030005	00-77-VC-C3-5D-7D
M06	IP Dynamic 7000 HD	187.101.177.70	77770030006	00-77-GF-BB-74-21
M07	IP Dynamic 7000 HD	187.101.177.71	77770030007	00-77-RE-65-54-79
M08	IP Dynamic 7000 HD	187.101.177.72	77770030008	00-77-BB-32-14-36
M09	IP Dynamic 7000 HD	187.101.177.73	77770030009	00-77-WR-1F-6E-9A
M10	IP Dynamic 7000 HD	187.101.177.74	77770030010	00-77-9E-ER-54-74
M11	IP Dynamic 7000 HD	187.101.177.75	77770030011	00-77-QR-SR-87-14
M12	IP Dynamic 7000 HD	187.101.177.76	77770030012	00-77-TY-ZX-BN-22
M13	IP Dynamic 7000 HD	187.101.177.77	77770030013	00-77-TY-VX-T9-2T
M14	IP Dynamic 7000 HD	187.101.177.78	77770030014	00-77-SD-36-5T-7T
M15	IP Dynamic 7000 HD	187.101.177.79	77770030015	00-77-RY-3G-34-9R
M16	IP Dynamic 7000 HD	187.101.177.80	77770030016	00-77-TR-3M-69-71
M17	IP Dynamic 7000 HD	187.101.177.81	77770030017	00-7J-TJ-3J-5R-7R
M18	IP Dynamic 7000 HD	187.101.177.82	77770030018	00-77-GG-NH-JY-88
M19	IP Dynamic 7000 HD	187.101.177.83	77770030019	00-77-TY-3R-R4-75
M20	IP Dynamic 7000 HD	187.101.177.84	77770030020	00-77-TR-DD-VR-MF
M21	IP Dynamic 7000 HD	187.101.177.85	77770030021	00-77-RE-SE-9R-7E
M22	IP Dynamic 7000 HD	187.101.177.86	77770030022	00-77-RS-6S-E8-72
M23	IP Dynamic 7000 HD	187.101.177.87	77770030023	00-77-WX-9F-51-78
M24	IP Dynamic 7000 HD	187.101.177.88	77770030024	00-77-TY-9S-6F-1T
M25	IP Dynamic 7000 HD	187.101.177.89	77770030001	00-77-W9-E9-6S-SS
M26	IP Dynamic 7000 HD	187.101.177.90	77770030025	00-98-21-32-47-32
M27	IP Dynamic 7000 HD	187.101.177.91	77770030026	00-77-RE-YT-U9-K9
M28	IP Dynamic 7000 HD	187.101.177.92	77770030027	00-77-T6-H9-N9-12
M29	IP Dynamic 7000 HD	187.101.177.93	77770030028	00-G9-TY-NM-J6-7K
M30	IP Dynamic 7000 HD	187.101.177.94	77770030029	00-77-M6-14-54-51
M31	IP Dynamic 7000 HD	187.101.177.95	77770030030	00-77-TY-4M-65-12
M32	IP Dynamic 7000 HD	187.101.177.96	77770030031	00-77-KL-S2-7J-4M

7.4 Sistema de CCAA

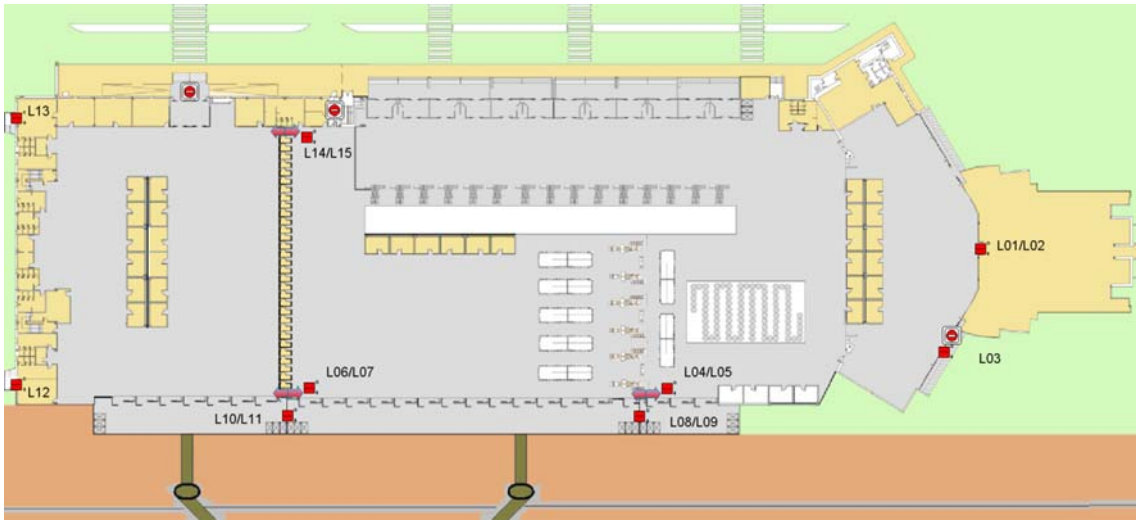


Figura 45: Lectoras de control de accesos en planta de salidas
Fuente: el autor

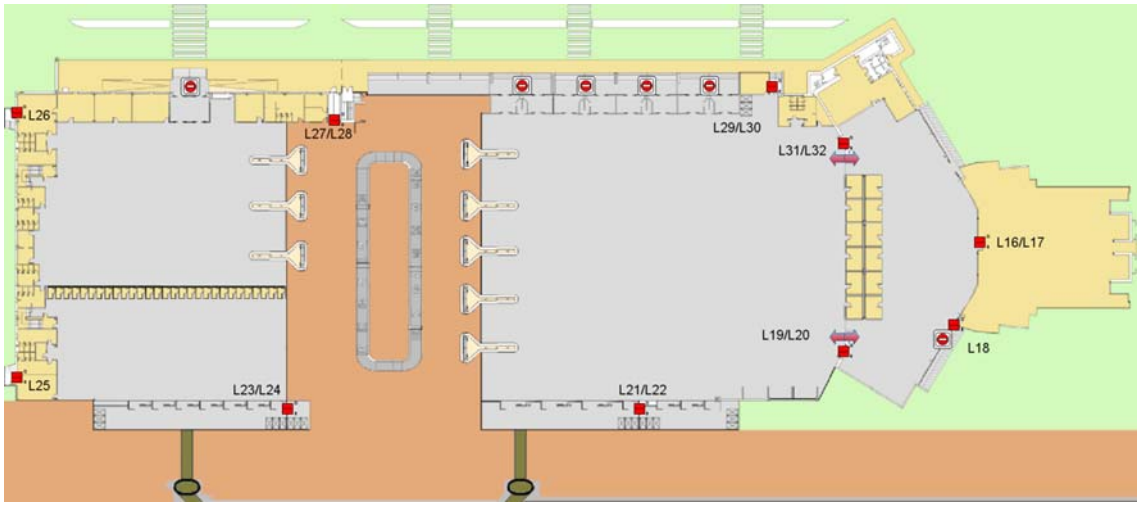


Figura 46: Lectoras de control de accesos en planta de llegadas
Fuente: el autor

Listado de lectoras de control de accesos y sus respectivas controladoras; datos de interés:

LECTORAS Y CPU				
Nº	**Nº CPU**	**IP CPU**	**Nº SERIE CPU**	**MAC CPU**
L01	1	187.101.178.1	RR06824	00-02-32-J4-54-DD
L02		187.101.178.1	RR06824	00-02-32-J4-54-DD
L03	2	187.101.178.2	RR05734	00-06-78-J3-87-DS
L04	3	187.101.178.3	RR02165	00-09-87-M8-74-SS
L05		187.101.178.3	RR02165	00-09-87-M8-74-SS
L06	4	187.101.178.4	RR02168	00-99-86-M2-DD-75
L07		187.101.178.4	RR02168	00-99-86-M2-DD-75
L08	5	187.101.178.5	RR02459	00-08-KL-9Y-SF-87
L09		187.101.178.5	RR02459	00-08-KL-9Y-SF-87
L10	6	187.101.178.6	RR02167	00-08-54-G7-42-SF
L11		187.101.178.6	RR02167	00-08-54-G7-42-SF
L12	7	187.101.178.7	RR00246	03-9T-5H-77-XS-23
L13	8	187.101.178.8	RR00246	00-22-H2-4S-YU-14
L14	9	187.101.178.9	RR00973	00-1L-44-G4-GF-42
L15		187.101.178.9	RR00973	00-1L-44-G4-GF-42
L16	10	187.101.178.10	RR00213	00-16-63-17-54-GF
L17		187.101.178.10	RR00213	00-16-63-17-54-GF
L18	11	187.101.178.11	RR01458	00-28-RY-J8-63-FD
L19	12	187.101.178.12	RR00875	00-58-76-F7-14-QA
L20		187.101.178.12	RR00875	00-58-76-F7-14-QA
L21	13	187.101.178.13	RR00348	00-95-76-P2-93-QA
L22		187.101.178.13	RR00348	00-95-76-P2-93-QA
L23	14	187.101.178.14	RR03165	00-55-5J-Y6-13-JH
L24		187.101.178.14	RR03165	00-55-5J-Y6-13-JH
L25	15	187.101.178.15	RR03167	00-55-52-TW-47-DX
L26	16	187.101.178.16	RR71167	00-44-59-14-91-FL
L27	17	187.101.178.17	RR07474	00-66-96-41-CV-82
L28		187.101.178.17	RR07474	00-66-96-41-CV-82
L29	18	187.101.178.18	RR09447	00-01-3R-0H-CX-52
L30		187.101.178.18	RR09447	00-01-3R-0H-CX-52
L31	19	187.101.178.19	RR07467	00-44-45-K2-MN-14
L32		187.101.178.19	RR07467	00-44-45-K2-MN-14

7.5 Equipos de inspección

Listado de equipos de inspección en puntos de acceso:

PUNTO DE ACCESO EN PLANTA DE SALIDAS		
Horario operativo	Durante todo el horario operativo de la Estación Marítima	
Equipos de seguridad		**Marca/modelo**
6	Equipos convencionales de RX	Smiths Heimann Hi-Scan 7555 aTiX
6	Arcos Detectores de Metales	CEIA PMD2 Plus Elliptic
3	Detectores de Metales en Calzado	CEIA SAMD
1	Equipo Detector de Trazas	Rapiscan HE50
6	Detectores Manuales de Metales	CEIA PD 140 N

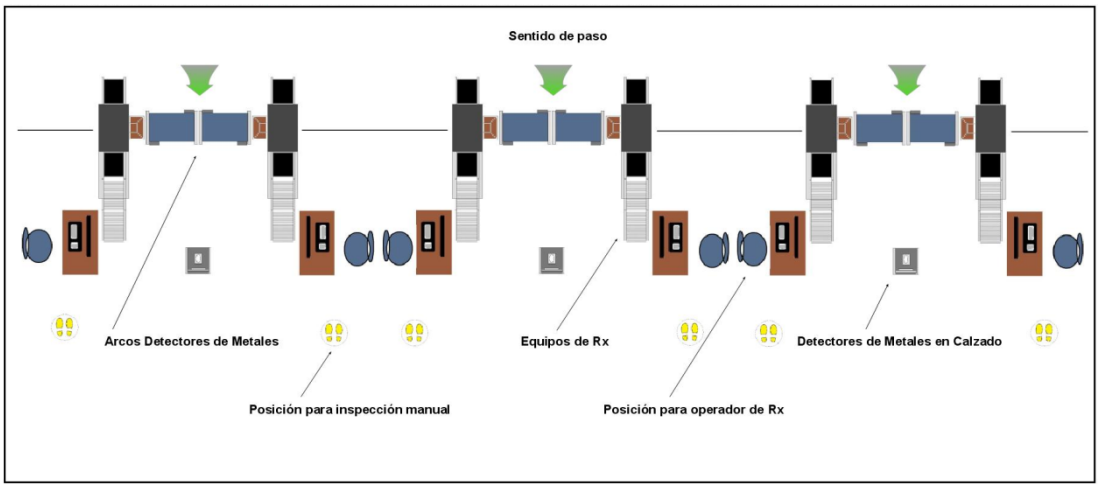


Figura 47: Disposición de equipos de inspección en planta de salidas
Fuente: el autor

PUNTO DE ACCESO EXTERIOR		
Horario operativo	H.24	
Equipos de seguridad		**Marca/modelo**
2	Equipos convencionales de RX	Smiths Heimann Hi-Scan 7555 aTiX
2	Arcos Detectores de Metales	CEIA PMD2 Plus Elliptic
1	Equipo Detector de Trazas	CEIA SAMD
1	Detector de Metales en Calzado	Rapiscan HE50
1	Detector Manual de Metales	CEIA PD 140 N
1	Equipo de Inspección para turismos	Smiths Heimann CIP 300
1	Equipo Inspección vehículos carga	Smiths Heimann HCVP

ADUANA EN PLANTA DE LLEGADAS		
Horario operativo	Durante todo el horario operativo de la Estación Marítima	
Equipos de seguridad		**Marca/modelo**
2	Equipos convencionales de RX	Smiths Heimann Hi-Scan 7555 aTiX
2	Arcos Detectores de Metales	CEIA PMD2 Plus Elliptic
1	Equipo Detector de Trazas	Rapiscan HE50
4	Detectores Manuales de Metales	CEIA PD 140 N

ADUANA EXTERIOR		
Horario operativo	H.24	
Equipos de seguridad		**Marca/modelo**
2	Equipos convencionales de RX	Smiths Heimann Hi-Scan 7555 aTiX
2	Arcos Detectores de Metales	CEIA PMD2 Plus Elliptic
1	Equipo Detector de Trazas	CEIA SAMD
1	Detector Manual de Metales	CEIA PD 140 N
1	Equipo de Inspección para turismos	Smiths Heimann CIP 300
1	Equipo Inspección vehículos carga	Smiths Heimann HCVP

Listado de equipos de inspección de equipajes facturados:

EQUIPOS DE INSPECCIÓN DE EQUIPAJES FACTURADOS		
Horario operativo	Durante todo el horario operativo de la Estación Marítima	
Equipos de seguridad		**Marca/modelo**
2	Equipos EDX	Smiths Heimann 10080 EDX 2iS
2	Equipos CTX	Smith Heimann Hi-Scan 10080 XCT
1	Equipo Detector de Trazas	Rapiscan HE50
2	Equipos convencionales de RX	Smiths Heimann Hi-Scan 7555 aTiX

7.6 Mantenimiento de equipos

El mantenimiento de medios de seguridad debe realizarse con independencia para cada uno de los sistemas que conviven en las instalaciones, y debe planificarse de manera que no entorpezca las operaciones, no se causen molestias al usuario y se preserve su operatividad (37). Para lograrlo, gran parte de las actividades de mantenimiento deben realizarse en horas valle (aquellas en las que la operaciones previstas son mínimas) o en horario nocturno (durante el cierre de la Estación Marítima).

Se deben considerar las siguientes modalidades:

1) Mantenimiento preventivo: consiste en la ejecución de una serie de operaciones y medidas sobre los equipos para chequear, ajustar y limpiar, al objeto de lograr los siguientes objetivos:

- Conservarlos en el mejor estado posible de funcionamiento y operatividad.
- Evitar que se lleguen a producir averías previsibles.
- Obtener el máximo rendimiento.
- Evitar el envejecimiento prematuro.
- Limitar los tiempos de fuera de servicio.
- Proveer de un estudio fiable de la vida de los equipos y su comportamiento a lo largo de ésta.

Las operaciones de mantenimiento preventivo se realizan sobre cada instalación y equipo, de manera cíclica, con periodicidades semanales, quincenales, mensuales, semestrales y anuales, según el tipo de recurso, las recomendaciones de los respectivos fabricantes y los requerimientos de la normativa vigente, a lo largo de toda su vida útil.

2) Mantenimiento correctivo: el objeto de este tipo de mantenimiento es el de reparar las averías que surjan, a la mayor brevedad y de manera eficiente, empleando para ello todos los recursos disponibles. Existen ciertos medios de seguridad activos y pasivos que requieren de su reparación inmediata, en función de su criticidad y su propósito dentro del esquema general de la seguridad de la Estación Marítima.

   Para asignar prioridades en la ejecución del mantenimiento correctivo de los equipos, las incidencias se califican conforme a la siguiente guía:

- Oportunidad de mejora: requerimiento de peticiones o cambios a sistemas existentes, que pueden deberse a modificaciones de aplicaciones o servicios, nuevas funcionalidades, etc.… Esta situación no se relaciona con un problema de operatividad del sistema.
- Incidencia de prioridad baja: pérdida parcial de servicio, si bien existen alternativas. Las incidencias de este nivel se relacionan con situaciones en las que el usuario no puede ejecutar alguna función específica de una aplicación o servicio, pero existen mecanismos de operación que pueden funcionar como alternativa temporal.
- Incidencia de prioridad media: supone la pérdida parcial de servicio y no existen alternativas. Las incidencias de este nivel se relacionan con situaciones en las que el usuario no puede ejecutar alguna función específica de una aplicación o servicio, sin que existan alternativas para la realización de dichas funciones. Se ejecutarán inmediatamente si no existen actividades de prioridad urgente y/o alta.
- Incidencia de prioridad alta: suponen la pérdida absoluta de servicio, si bien existen alternativas. La inactividad de los usuarios es total y no puede utilizar las aplicaciones o sistemas como fueron concebidos, pero existen mecanismos de operación que pueden funcionar como alternativa

temporal. Se ejecutarán inmediatamente si no existen actividades de prioridad urgente.

- Incidencia de prioridad urgente: suponen la pérdida completa del servicio, y no existen alternativas. La inactividad de los usuarios es total, no se puede desarrollar las funciones para las que se diseñó y no existen alternativas de operación disponibles. Se ejecutarán inmediatamente, incluso interrumpiendo otras de nivel 2 a 5, si se carece de los recursos humanos precisos para acometer su resolución simultánea.

3) Mantenimiento evolutivo: consiste en la actualización del software y el firmware de los equipos, al objeto de cumplir normativa, mejorar sus prestaciones y garantizar su máxima compatibilidad con otros equipos de nueva generación que vayan incorporándose al los diferentes sistemas de seguridad.
4) Mantenimiento modificativo: se refiere a actuaciones de reforma que mejoran el estado o el rendimiento de las instalaciones o que responden a un replanteamiento de alguno de los sistemas.

7.7 Disposición de puertas interiores y exteriores gobernadas mediante el sistema de gestión y control.

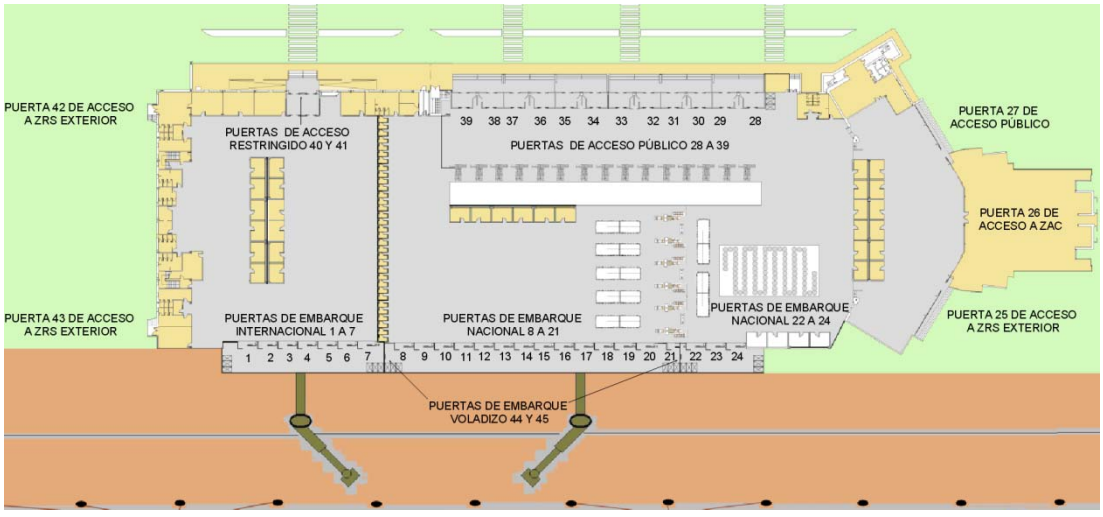


Figura 48: Puertas en planta de salidas
Fuente: el autor

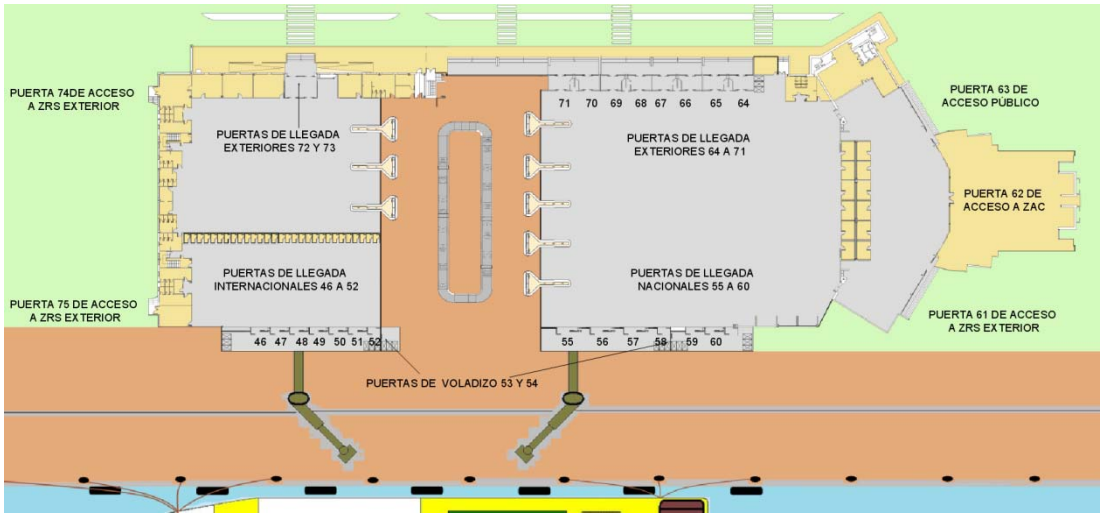


Figura 49: Puertas en planta de llegadas
Fuente: el autor

Figura 50: Puertas en perímetro
Fuente: el autor sobre fondo de Google Maps

Control remoto de puertas a través del sistema; comandos posibles:

	COMANDO			
Nº PUERTA	**APERTURA**	**CIERRE**	**BLOQUEO**	**FUNCIONAMIENTO AUTOMÁTICO**
1	SI	SI	NO	NO
2	SI	SI	NO	NO
3	SI	SI	NO	NO
4	SI	SI	NO	NO
5	SI	SI	NO	NO
6	SI	SI	NO	NO
7	SI	SI	NO	NO
8	SI	SI	NO	NO
9	SI	SI	NO	NO
10	SI	SI	NO	NO
11	SI	SI	NO	NO
12	SI	SI	NO	NO
13	SI	SI	NO	NO
14	SI	SI	NO	NO
15	SI	SI	NO	NO
16	SI	SI	NO	NO
17	SI	SI	NO	NO
18	SI	SI	NO	NO
19	SI	SI	NO	NO
20	SI	SI	NO	NO
21	SI	SI	NO	NO
22	SI	SI	NO	NO
23	SI	SI	NO	NO
24	SI	SI	NO	NO
25	SI	SI	SI	NO
26	SI	NO	NO	NO
27	SI	SI	SI	SI
28	SI	SI	SI	SI
29	SI	SI	SI	SI
30	SI	SI	SI	SI
31	SI	SI	SI	SI
32	SI	SI	SI	SI
33	SI	SI	SI	SI
34	SI	SI	SI	SI
35	SI	SI	SI	SI
36	SI	SI	SI	SI
37	SI	SI	SI	SI
38	SI	SI	SI	SI
39	SI	SI	SI	SI
40	SI	SI	SI	NO

41	SI	SI	SI	NO
42	SI	NO	SI	NO
43	SI	NO	SI	NO
44	SI	SI	NO	NO
45	SI	SI	NO	NO
46	SI	SI	NO	NO
47	SI	SI	NO	NO
48	SI	SI	NO	NO
49	SI	SI	NO	NO
50	SI	SI	NO	NO
51	SI	SI	NO	NO
52	SI	SI	NO	NO
53	SI	SI	NO	NO
54	SI	SI	NO	NO
55	SI	SI	NO	NO
56	SI	SI	NO	NO
57	SI	SI	NO	NO
58	SI	SI	NO	NO
59	SI	SI	NO	NO
60	SI	SI	NO	NO
61	SI	SI	SI	NO
62	SI	NO	NO	NO
63	SI	SI	SI	SI
64	SI	SI	SI	SI
65	SI	SI	SI	SI
66	SI	SI	SI	SI
67	SI	SI	SI	SI
68	SI	SI	SI	SI
69	SI	SI	SI	SI
70	SI	SI	SI	SI
71	SI	SI	SI	SI
72	SI	SI	SI	SI
73	SI	SI	SI	SI
74	SI	NO	SI	NO
75	SI	NO	SI	NO
76	SI	SI	NO	NO
77	SI	SI	NO	NO
78	SI	SI	NO	NO
79	SI	SI	NO	NO

Sección 8 – Recorridos de acceso (entradas y salidas)

8.1 Recorridos de entrada y salida a pie y en vehículo

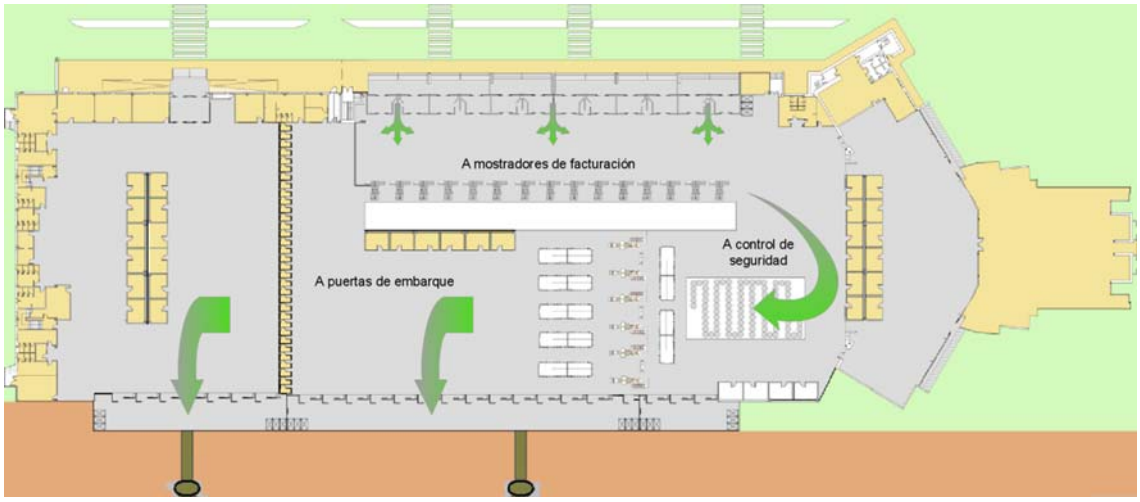


Figura 51: Entrada de pasajeros, tripulaciones y personal por planta de salidas
Fuente: el autor

Figura 52: Entrada y salidas de pasajeros, tripulaciones y personal, con vehículos, por puntos de acceso exteriores
Fuente: el autor sobre fondo de Google Maps

Un procedimiento deberá establecer de qué modo se compatibiliza el acceso de pasajeros con el acceso de proveedores, suministradores, tripulantes y empleados.

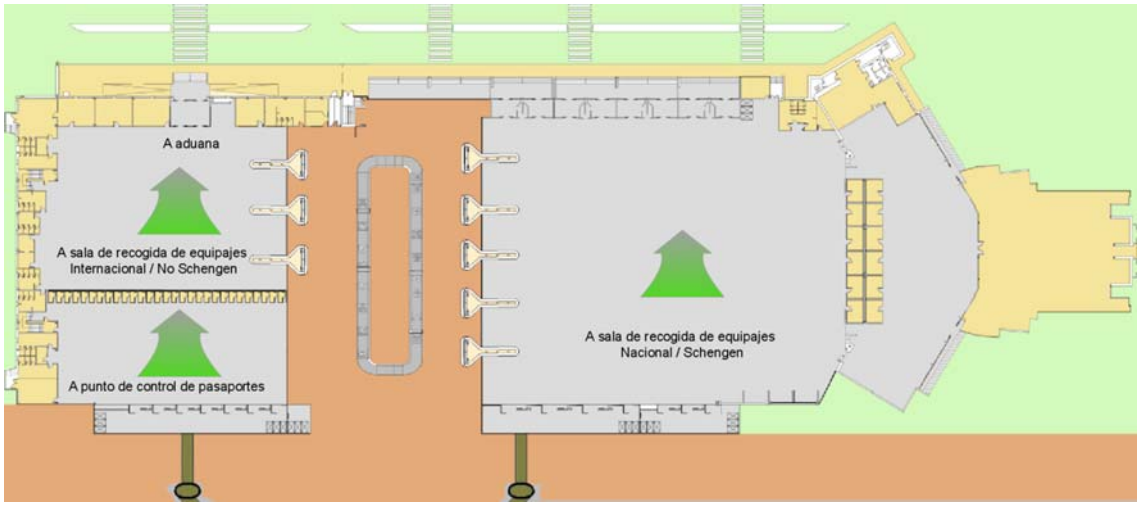


Figura 53: Salida de pasajeros, tripulaciones y personal (éstos, únicamente por la aduana), por planta de llegadas
Fuente: el autor

Los embarques y desembarques de pasajeros se realizarán a través de las pasarelas de embarque, cuando sea posible; en el resto de casos se les guiará por sendas peatonales señalizadas en el pavimento.

Las operaciones de embarque y desembarque de pasajeros tendrán prioridad sobre el resto.

8.2 Evacuación: recorridos de evacuación; punto de encuentro principal y puntos de encuentro secundarios

La evacuación de la Estación Marítima y de sus instalaciones debe efectuarse prioritariamente a la zona pública, salvo que la emergencia se declare en dicha zona (por ejemplo, una amenaza de bomba factible en el frontal del edificio terminal).

Se crearán equipos de alarma y evacuación, que tendrán las siguientes funciones:

1) Se asegurarán de garantizar que se ha dado la alarma y coordinarán la evacuación del sector que tuviesen asignado.
2) Avisarán a las personas que se encuentren en su sector de evacuación.

3) Dirigirán a las personas por las vías de evacuación del modo más rápido y ordenado posible.
4) Comprobarán que no existen personas rezagadas o perdidas.
5) Impedirán que alguna persona retroceda o penetre en una zona ya evacuada.

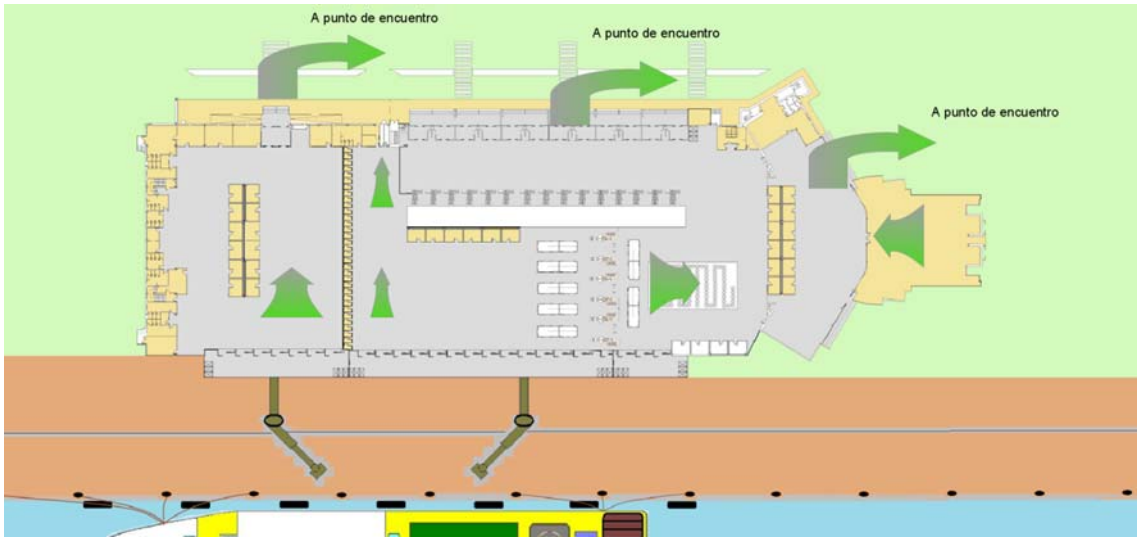


Figura 54: Planta de salidas; recorrido de evacuación a zona pública
Fuente: el autor

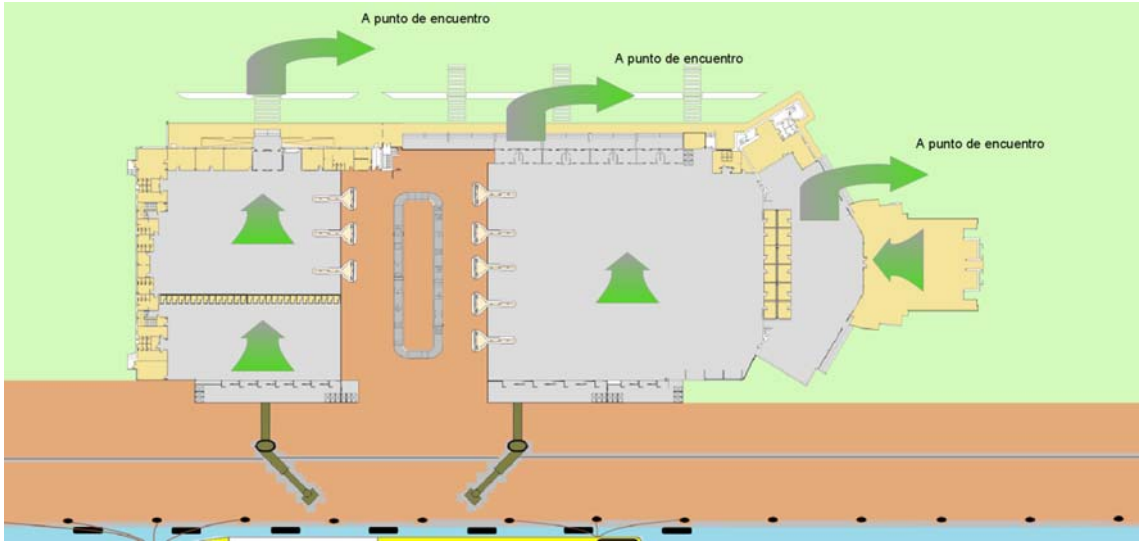


Figura 55: Planta de llegadas; recorrido de evacuación a zona pública
Fuente: el autor

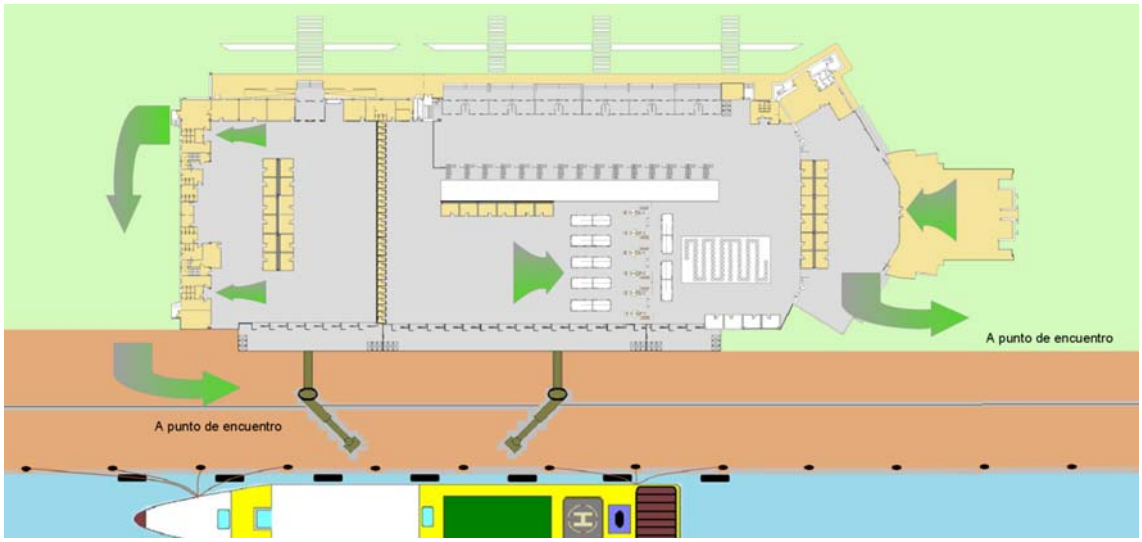


Figura 56: Planta de salidas; recorrido de evacuación a zona restringida
Fuente: el autor

Figura 57: Planta de llegadas; recorrido de evacuación a zona restringida
Fuente: el autor

Figura 58: Punto de encuentro principal y puntos de encuentro secundarios
Fuente: el autor sobre fondo de Google Maps

Sección 9 – Zonas de acopio y almacenamiento de provisiones, equipajes, suministros, carga y correo inspeccionados.

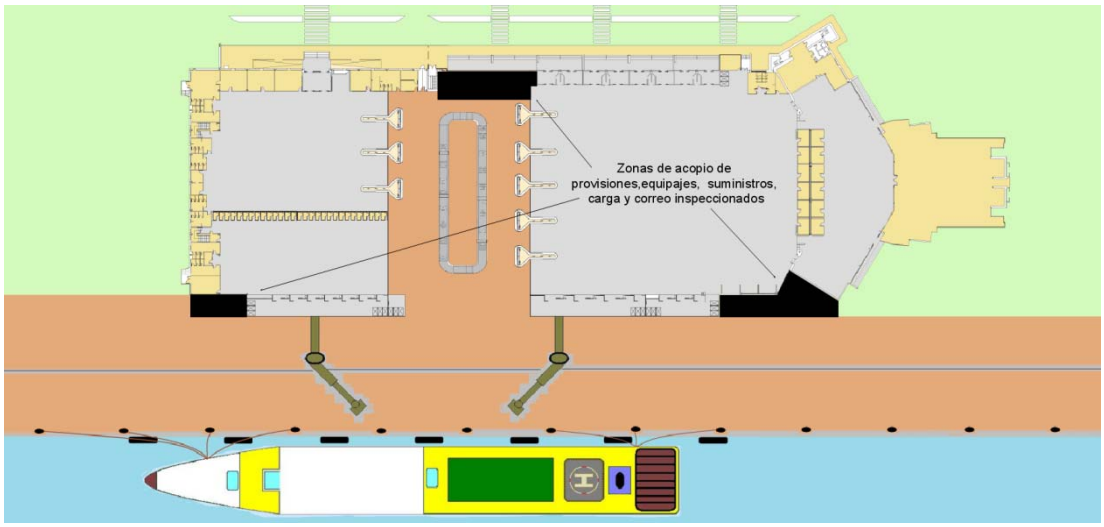


Figura 59: Zonas de acopio
Fuente: el autor

Sección 10 – Señalización de seguridad

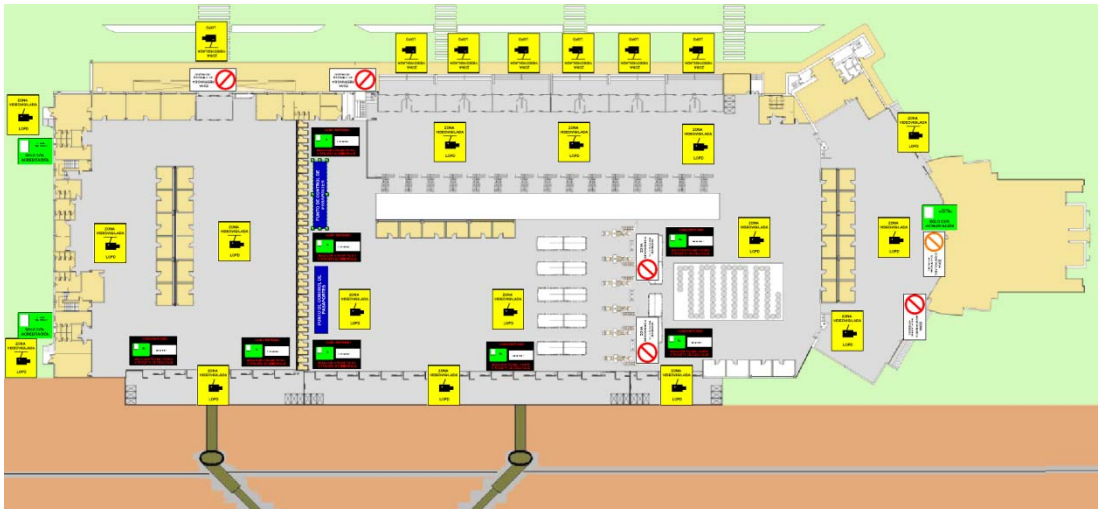


Figura 60: Señalización de seguridad en planta de salidas
Fuente: el autor

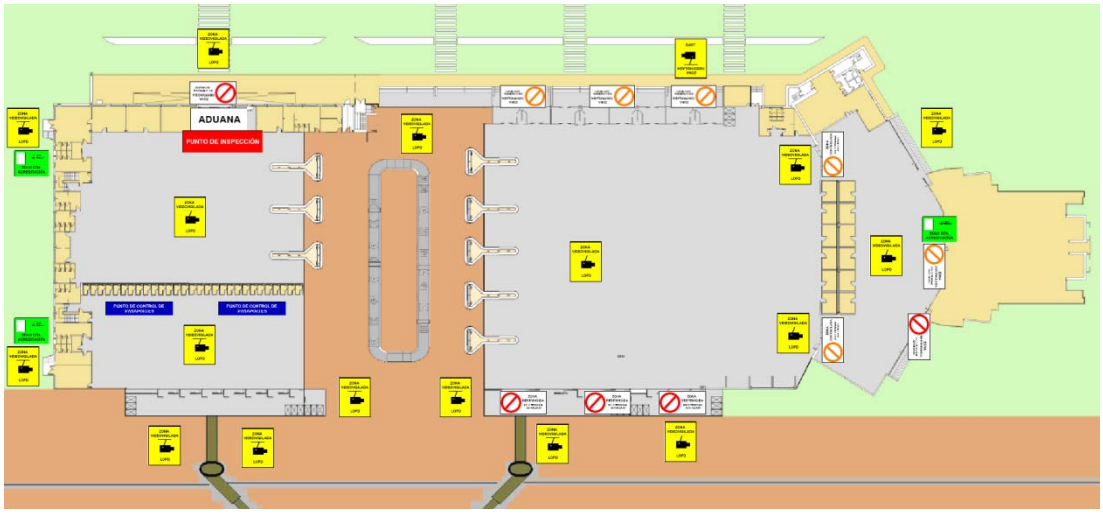


Figura 61: Señalización de seguridad en planta de llegadas
Fuente: el autor

Figura 62: Señalización de seguridad en exteriores
Fuente: el autor sobre fondo de Google Maps

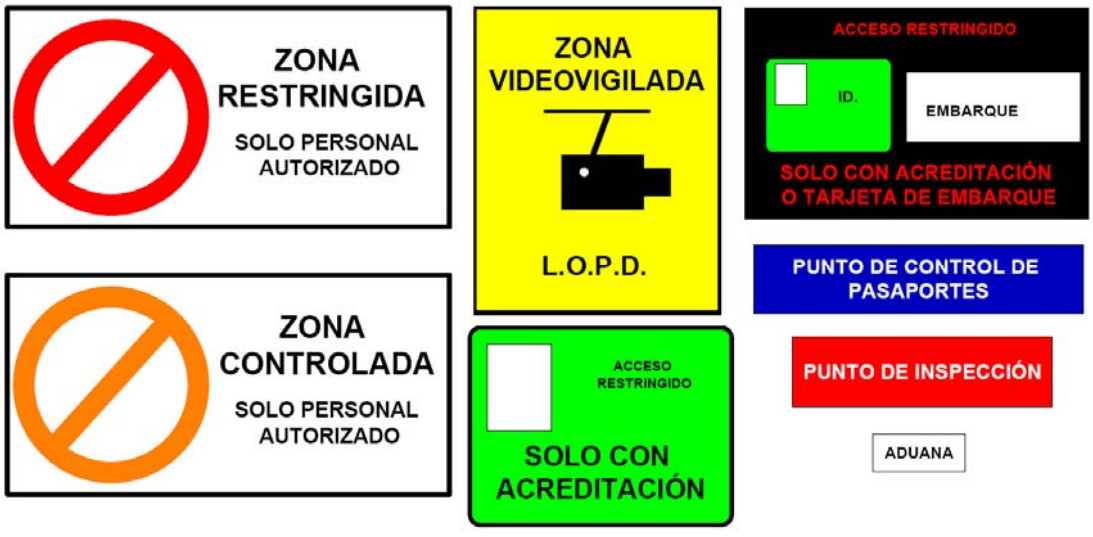


Figura 63: Señales empleadas
Fuente: el autor

Anexo I – Evaluación de riesgos de seguridad

10.1 Variables

A la hora de plantearse una evaluación del riesgo surge un enorme abanico de posibilidades que existen para la comisión de actos de naturaleza ilícita (hurtos, robos, tráfico de drogas, de personas, sabotaje, terrorismo…); seguidamente, se citan algunas variables que pueden definir el escenario de un acto ilícito (38).

1) Las capacidades de los perpetradores de un acto ilícito varían sustancialmente en función de su entorno, los medios técnicos de los que pueden disponer y de su preparación: mientras que algunos trabajadores del ámbito portuario se podrían beneficiar de sus privilegios de acceso a la Estación Marítima para introducir o extraer personas, artículos prohibidos o de contrabando, otro personal foráneo con intenciones de causar daño y que no gozase de esos privilegios de acceso, podría haber sido concienzudamente entrenado para realizar operaciones sofisticadas de sabotaje o terrorismo.
2) Los individuos capaces de realizar actos ilícitos se pueden plantear objetivos muy diversos: el lucro personal a través del tráfico de drogas, artículos o seres humanos; la pérdida de vidas humanas, pérdidas económicas o daños al medio ambiente. En función de las actuaciones que puedan llegar a realizar, pueden lograr uno o varios de esos objetivos simultáneamente.

   En el caso concreto de la Estación Marítima hay que tener en cuenta que, si se pretendiese acabar con un gran número de vidas humanas, el ataque a un buque de crucero, a un transbordador o a la propia instalación constituiría un objetivo atractivo. Si además se lograse cerrar la vía de acceso al puerto, la acción llevaría aparejada una gran pérdida económica derivada de la interrupción parcial o total de las actividades portuarias y del tráfico marítimo; además, se debe tener en cuenta que el hundimiento de un buque podría causar también un daño medioambiental importante.
3) La Estación marítima cuenta con tres zonas de diferente naturaleza que hay que tener en cuenta:
   - El edificio terminal de pasajeros.
   - El perímetro de la instalación y las zonas contiguas exteriores.

- La zona marítima controlada (incluida la submarina).

4) Los objetivos más probables de un hipotético ataque a la Estación Marítima, bien sea con la intención de provocar pérdidas económicas o pérdidas de vidas humanas, serían los propios buques y/o el propio edificio terminal: vestíbulo, sala de recogida de equipajes, plantas de energía, centro de proceso de datos, oficinas, centro de control; centro de operaciones y centro de comunicaciones.
5) Un último aspecto a tener en cuenta serían las tácticas empleadas: introducción abordo de herramientas, armas o explosivos; empleo de pequeñas embarcaciones o aeronaves ligeras cargadas de material explosivo para estrellarlas en el costado de un buque, minas flotantes a la deriva o sujetas a boyas, lanzamiento de misiles desde una plataforma en tierra o desde otra embarcación, colocación de artefactos submarinos bajo la línea de flotación del buque, etc.

10.2 Otros factores de importancia

Otros factores de importancia a analizar por profesionales cualificados, a la hora de valorar el impacto de cada diferente supuesto, son (6):

1) Los registros previos de actividad criminal en la zona.
2) Si se ha detectado actividad de grupos criminales que puedan llevar a cabo actos ilícitos de alguna índole en las instalaciones.
3) El entorno de protección (capacidad de los organismos públicos para reaccionar ante operaciones criminales), disponibilidad y adecuación de fuerzas de respuesta.
4) Adecuación de la protección física.

10.3 Factores que favorecen la vulnerabilidad

1) Carencia de medios disuasorios (presencia personal seguridad, CCTV, señalización).
2) Iluminación deficiente.
3) Presencia inadecuada de personal en zonas controladas o restringidas.
4) Sistema de comunicaciones deficiente.

5) Formación insuficiente o deficiente en materia de seguridad, del personal que presta algún tipo de servicio en la Estación Marítima.
6) Procedimientos de seguridad inadecuados o deficientes.
7) Tiempos de respuesta inadecuados ante emergencias.
8) Deficiencias en los viales de acceso a la Estación Marítima.
9) Medios de seguridad activa y pasiva deficientes o inadecuados (bolardos, vallado perimetral, detección de presencia, control de accesos, control de seguridad).
10) Insuficiencia de medios técnicos para la inspección y/o inadecuada formación de los operadores.
11) Accesos a tejados, galerías, sótanos, almacenes y espacios que no estén suficientemente controlados.

10.4 Valoración del riesgo en las diferentes zonas, según su naturaleza

Si bien existen varias metodologías para la evaluación del riesgo, ésta se basará en la propuesta por la Organización Marítima Internacional y por la Organización Internacional del Trabajo en el documento "Repertorio de recomendaciones prácticas sobre protección en los puertos" (6).

Claves:

1) **Amenaza**: se evalúa la posibilidad de que se produzca un incidente; a la hora de evaluar este parámetro deben tenerse en cuenta varios factores como la presencia de grupos con voluntad y capacidad de atentar, presentes en la zona, histórico y frecuencia de incidentes de la misma naturaleza que los que se consideran, etc.

   El Gobierno de la nación, a través del Ministerio del Interior (Secretaría de Estado de Seguridad) notifica convenientemente las alteraciones del grado de amenaza, a todas las organizaciones afectadas, al objeto de que se tomen las medidas oportunas.

   Escala:

   - 1: Bajo.
   - 2: Medio.
   - 3: Alto.

2) **Vulnerabilidad**: se evalúan las debilidades de la infraestructura respecto de las medidas de protección con las que se cuenta: a mejor protección, menor grado de vulnerabilidad.

   Escala:

   - 1: Las medidas de protección son totalmente eficaces (objetivos muy difíciles de alcanzar; medidas de protección que permiten pasar rápidamente a un nivel superior; objetivos que, pese a ser alcanzados tienen la capacidad de no interrumpir su operación…).
   - 2: Las medidas de protección son satisfactorias (zonas claramente definidas; controles de acceso y seguridad eficaces; personal sensibilizado y formado en materia de seguridad; procedimientos de seguridad eficientemente diseñados; objetivo protegido y difícilmente alcanzable; objetivo con capacidad de continuar operando pese a ser objeto de un ataque…).
   - 3: Las medidas de protección son mínimas (zonas de seguridad que no se encuentran claramente definidas; procedimientos de seguridad ineficaces, controles de seguridad y acceso precarios; falta de sensibilización y de formación en materia de seguridad, del personal que realiza actividades en la instalación; objetivo en el que se pueden interrumpir las operaciones con facilidad, en caso de sufrir un ataque…).
   - 4: Las medidas de protección son inexistentes o ineficaces (medios de protección insuficientes, deteriorados, sin mantenimiento; personal no capacitado; falta de vigilancia y control; objetivo fácilmente alcanzable; operaciones fácilmente paralizables; personal no sensibilizado; personal no formado…).

3) **Impacto o magnitud de las consecuencias derivadas del incidente**: se valora el grado de afección al objetivo potencial y a la Estación Marítima. Se debe considerar que un ataque en una Estación Marítima de este tipo puede llegar a tener una repercusión mundial, en función de los daños ocasionados.

   Escala:

   - 1: Dañino, al menoscabar la confianza de los clientes y usuarios del puerto.

- 2: Dañino para los bienes, la infraestructura, los servicios de suministro de agua, electricidad, etc., y la protección de la carga (probabilidad de paralización parcial o total de las operaciones).
- 3: Dañino para el medio ambiente y para el funcionamiento del puerto (probabilidad de una intervención duradera de las actividades de todo el puerto y de grandes pérdidas económicas; probabilidad de una merma del prestigio internacional).
- 4: Dañino para la seguridad pública y el prestigio nacionales (probabilidad de grandes daños para el medio ambiente y/o ciertos elementos de la seguridad y la salud públicas).
- 5: Dañino para la protección y la seguridad (probabilidad de que se causen muertes y lesiones graves y/o de que se cree un peligro general para la seguridad y la salud públicas).

Puntuación del riesgo: se obtiene multiplicando los valores asignados a la amenaza (riesgo), la vulnerabilidad y el impacto (magnitud de las consecuencias).

Tabla 1 - Puntuación del riesgo en el edificio terminal de pasajeros:

Situación de amenaza	Amenaza	Medidas	Vulnerabilidad	Impacto	Puntuación de riesgo
Hurtos y robos	3	Si	2	1	6
Contrabando	2	Si	2	1	4
Polizones ilegales	1	Si	2	1	2
Robo armado/piratería	2	Si	2	5	20
Sabotaje	2	Si	2	4	8
Terrorismo	1	Si	2	5	10

Tabla 2 - Puntuación del riesgo en el perímetro y zonas contiguas exteriores:

Situación de amenaza	Amenaza	Medidas	Vulnerabilidad	Impacto	Puntuación de riesgo
Hurtos y robos	1	Si	2	1	2
Contrabando	3	Si	2	1	6
Polizones ilegales	3	Si	2	1	6
Robo armado/piratería	2	Si	2	5	20
Sabotaje	2	Si	2	4	16
Terrorismo	3	Si	2	5	30

Tabla 3 - Puntuación del riesgo en la zona marítima controlada:

Situación de amenaza	Amenaza	Medidas	Vulnerabilidad	Impacto	Puntuación de riesgo
Hurtos y robos	1	Si	2	1	2
Contrabando	3	Si	2	1	6
Polizones ilegales	3	Si	2	1	6
Robo armado/piratería	2	Si	3	5	30
Sabotaje	2	Si	2	4	16
Terrorismo	2	Si	3	5	30

Tabla 4 - Clasificación de los riegos en función de su puntuación:

Puntuación del riesgo	Zona	Situación de amenaza
30	Perímetro	Terrorismo
30	Zona Marítima Controlada	Terrorismo
30	Zona Marítima Controlada	Piratería y robo a mano armada
20	Perímetro	Piratería y robo a mano armada
20	Edificio Terminal	Piratería y robo a mano armada
16	Perímetro	Sabotaje
16	Zona Marítima Controlada	Sabotaje
10	Edificio Terminal	Terrorismo
8	Edificio Terminal	Sabotaje
6	Perímetro	Contrabando
6	Perímetro	Inmigrantes y polizones ilegales
6	Zona Marítima Controlada	Contrabando
6	Zona Marítima Controlada	Inmigrantes y polizones ilegales
6	Edificio Terminal	Hurtos y robos
4	Edificio Terminal	Contrabando
2	Perímetro	Hurtos y robos
2	Zona Marítima Controlada	Hurtos y robos
2	Edificio Terminal	Inmigrantes y polizones ilegales

Se puede observar que la puntuación del riesgo se eleva cuando se consideran los riesgos derivados de terrorismo, piratería, robo a mano armada y sabotaje, por ser aquellos que podrían causar la pérdida de vidas humanas y/o paralizar la actividad de la instalación ocasionando mayores daños económicos.

El resto de supuestos, por tratarse de actos de distinta naturaleza, no alcanzan a resultar de la misma gravedad, si bien parece más probable que se registren incidentes de esos tipos.

Tabla 5 - Clasificación de los riesgos en función de la vulnerabilidad:

Vulnerabilidad	Zona	Situación de amenaza
3	Zona Marítima Controlada	Hurtos y robos
3	Zona Marítima Controlada	Piratería y robo a mano armada
2	Zona Marítima Controlada	Inmigrantes y polizones ilegales
2	Zona Marítima Controlada	Contrabando
2	Zona Marítima Controlada	Sabotaje
2	Zona Marítima Controlada	Terrorismo
2	Perímetro	Hurtos y robos
2	Perímetro	Contrabando
2	Perímetro	Inmigrantes y polizones ilegales
2	Perímetro	Piratería y robo a mano armada
2	Perímetro	Sabotaje
2	Perímetro	Terrorismo
2	Edificio Terminal	Hurtos y robos
2	Edificio Terminal	Contrabando
2	Edificio Terminal	Inmigrantes y polizones ilegales
2	Edificio Terminal	Piratería y robo a mano armada
2	Edificio Terminal	Sabotaje
2	Edificio Terminal	Terrorismo

Se observa que la Zona Marítima Controlada y el Perímetro son más vulnerables que el Edificio Terminal por resultar más abiertas, más extensas y más complicadas de controlar que el Edificio Terminal, que se trata de una zona confinada, permanentemente controlada por numerosos medios humanos y materiales.

Tabla 6- Clasificación de los riesgos en función de su impacto:

Impacto	Zona	Situación de amenaza
5	Edificio Terminal	Terrorismo
5	Edificio Terminal	Piratería y robo a mano armada
5	Zona Marítima Controlada	Terrorismo
5	Zona Marítima Controlada	Piratería y robo a mano armada
5	Perímetro	Terrorismo
5	Perímetro	Piratería y robo a mano armada
4	Edificio Terminal	Sabotaje
4	Zona Marítima Controlada	Sabotaje
4	Perímetro	Sabotaje
1	Edificio Terminal	Hurtos y robos
1	Edificio Terminal	Contrabando
1	Edificio Terminal	Inmigrantes y polizones ilegales
1	Zona Marítima Controlada	Hurtos y robos
1	Zona Marítima Controlada	Contrabando
1	Zona Marítima Controlada	Inmigrantes y polizones ilegales
1	Perímetro	Hurtos y robos
1	Perímetro	Contrabando
1	Perímetro	Inmigrantes y polizones ilegales

El hipotético impacto resultante de un ataque en el Edificio Terminal o en un buque atracado al muelle podría causar daños humanos y económicos irreparables, considerándose estos los de mayor envergadura posible; pese a que el perímetro puede ser una zona en la que el daño causado resulte de gran magnitud, se considera que el impacto de un acto ilícito en esa zona sería menos dañino que en las otras dos.

10.5 Opciones

Conocida la puntuación de cada uno de los riesgos en función de su entorno y los factores que favorecen la vulnerabilidad, son posibles varias opciones, que habrán de considerarse para cada una de las amenazas:

1) Asumir el riesgo y operar sin tomar medidas.
2) Evitar el riesgo mediante la eliminación de las causas que lo originan.
3) Limitar el riesgo mediante la implantación de medidas preventivas y mitigadoras.
4) Transferencia del riesgo, mediante la contratación de un seguro.

Resulta evidente que asumir ciertos riesgos sin tomar medidas no es una opción, dada la naturaleza de los bienes a proteger (vidas humanas, infraestructuras, negocio marítimo…); la eliminación de las causas que originan el riesgo, tampoco parece una opción puesto que siempre existen intereses para causar daños indiscriminados, lucrarse mediante actividades delictivas o motivaciones que empujan a los individuos a cometer actos siniestros en perjuicio del bien común.

Si bien la instalación cuenta con numerosas medidas preventivas y mitigadoras, la evaluación de riesgos se realiza con el propósito de conocer las medidas correctivas que han de aplicarse para subsanar las debilidades que no se pueden asumir, a la vez que plantear propuestas de mejora en aquellos aspectos que, sin constituir debilidades no asumibles, se pueden mejorar para proporcionar un mayor grado de seguridad a trabajadores y usuarios.

Las prioridades, por tanto, se basan en diseñar procedimientos locales eficientes, complementarios a las medidas de seguridad física existentes en las instalaciones y en la mejora de aquellos puntos que conviene reforzar.

Tabla 7 – Matriz de riesgos:

	ZONAS		
RIESGOS	**Edificio Terminal**	**Perímetro**	**Zona Marítima Controlada**
Terrorismo			
Piratería y robo a mano armada			
Sabotaje			
Contrabando			
Inmigrantes y polizones ilegales			
Hurtos y robos			

Tabla 8 – Claves:

	Riesgo muy grave no asumible	Evitar
	Riesgo asumible	Limitar
	Riesgo leve asumible	Limitar
	Riesgo muy leve asumible	Plantear acciones de mejora
	Punto fuerte	Asumir

10.6 Acciones correctoras y acciones de mejora

A la vista de la puntuación del riesgo en las diferentes zonas, se observan algunas debilidades del sistema que hay que corregir:

1) Dados los medios de seguridad técnicos y humanos con los que cuenta la instalación, no se han detectado riesgos no asumibles que supongan un peligro inaceptable para la Estación Marítima.
2) Vulnerabilidades que hay que limitar:
    - Edificio terminal: el robo a mano armada se ha manifestado una amenaza a tener en cuenta en un punto muy concreto del edificio terminal de pasajeros (las escaleras que comunican la planta de salidas con la planta de llegadas, por su interior) que no se encuentra vigilado con el sistema de CCTV y es una zona sombría y poco iluminada. Por otra parte, al ser una zona de muy poco tránsito parece un lugar en el que podría cometerse un asalto. Se propone mejorar ostensiblemente el alumbrado y colocar cámaras fijas de CCTV, además de incrementar el número de patrullas de vigilancia en la zona.
    - El perímetro puede resultar una zona vulnerable ante acciones de terrorismo y de piratería o robo a mano armada: puesto que los medios técnicos dispuestos parecen suficientes, se estima conveniente mejorar los medios organizativos (procedimientos, frecuencia de patrullas y coordinación entre organizaciones con responsabilidades en materia de seguridad) al objeto de limitar el riesgo.
    - También en zona marítima controlada se observan hipotéticas amenazas que conviene limitar: si bien existe una patrulla marítima realizando rondas durante todas las horas del día, se estima que los medios técnicos para controlar adecuadamente la zona submarina, y la superficie durante la noche, son mejorables. Se propone equipar la embarcación de patrulla con radar y sonar, y realizar misiones subacuáticas de inspección de los buques atracados, para comprobar que no se han colocado artefactos explosivos adosados al casco. Por

otra parte, se estima oportuno colocar una cámara térmica para la vigilancia nocturna de la superficie acuática.

3) Otro de los riesgos que se podrían materializar es el de sabotaje (en el perímetro y en la zona marítima controlada): por una parte se estima que las acciones de mejora que se han planteado en el punto anterior reducirán este riesgo; por otra, se estima oportuno que los privilegios de accesos asignados a las tarjetas de acreditación personal sigan criterios muy restrictivos para que ninguna persona permanezca en lugares a los que no debe acceder.
4) Se observan riesgos asumibles que presentan oportunidades de mejora en todas las zonas: no se cree necesario invertir en medios técnicos y los procedimientos de seguridad parecen correctos. Se estima oportuna la realización de una campaña de concienciación en materia de seguridad, y la formación del personal.
5) También existen puntos fuertes que no requieren acciones correctoras ni acciones de mejora.

10.7 Otras medidas complementarias

1) Control de calidad de la seguridad: se realiza mediante el establecimiento de unos indicadores objetivos y medibles que sirvan para facilitar el control exhaustivo del servicio; son numerosos los indicadores que pueden marcarse y pueden abarcar todos los aspectos de la seguridad. En función de la evolución de cada uno de ellos, se observan los puntos fuertes y aquellos que necesitan mejorarse. Se trata de una acción de mejora que se muestra efectiva y no requiere inversión.
2) Formación de cierto personal de seguridad en técnicas de detección del comportamiento: en países como Israel o EEUU se han estudiado patrones de comportamiento y se ha observado que los individuos con intenciones de cometer actos violentos muestran algunos indicadores de comportamiento reconocibles; estas técnicas se basan en la observación y en la entrevista, y son complementarias al resto de medios de seguridad.

10.8 Implantación y seguimiento de las medidas correctoras y acciones de mejora

Estas medidas se implantarán en el plazo de 12 meses y se observará si han contribuido a reducir la vulnerabilidad ante las amenazas detectadas, mejorando el nivel de seguridad de la instalación marítima.

Anexo II – Declaración de seguridad (DoS)

(Para ser empleada entre un buque y la Estación Marítima)

Nombre del Buque: _____
Puerto de Registro: _____
Indicativo: _____
Estación Marítima del Puerto de Santander: _____

Esta Declaración de Seguridad (29) tendrá validez desde…… hasta……., para la realización de las siguientes actividades:

1. *Embarque y desembarque de pasajeros, equipajes, correo y carga (vehículos incluidos.)*
2. *Aprovisionamiento del buque.*

Bajo los siguientes niveles de seguridad:

Nivel (es) de seguridad para el buque: _____
Nivel (es) seguridad Estación Marítima: _____

Tanto la Estación Marítima del Puerto de Santander como el buque acuerdan las siguientes medidas de seguridad al objeto de garantizar el cumplimiento de los requerimientos normativos de la legislación Española.

	La impresión de las iniciales del OSIP o del OSB bajo estas columnas indica que la actividad se realizará conforme al Plan relevante de seguridad aprobado, por	
Actividad	La Estación Marítima:	El buque:
Garantizar la prestación de todos los servicios de seguridad		
Vigilar las áreas restringidas para garantizar que únicamente el personal acreditado accede a ellas		
Controlar el acceso a las instalaciones de la Estación Marítima		
Controlar el acceso al buque		
Vigilar la Estación Marítima, incluido el muelle y la zona marítima adyacente		
Vigilar el buque, incluido el muelle, y su zona marítima adyacente		
Manipulación de la carga		
Entrega de provisiones		
Manipulación del equipaje no acompañado		
Control del embarque de personas y sus efectos personales		
Asegurar la disponibilidad de los medios de comunicación entre el buque y la Estación Marítima		

La firma de este acuerdo certifica que las medidas de seguridad aplicables por el buque y por la Estación Marítima durante la ejecución de las actividades anteriormente detalladas satisfacen la normativa Española en materia de seguridad marítima y se adoptarán conforme aparecen estipuladas en los respectivos Planes de Protección de ambas partes.

En……Santander…… a……de……de…201……

Firmado en representación de	
La Estación Marítima:	El buque:
(Firma del Oficial de Seguridad de la Estación Marítima)	*(Firma del Capitán o del Oficial de Seguridad del Buque)*

Nombre y cargo de la persona firmante	
Nombre:	Nombre:
Cargo:	Cargo

Detalles de contacto *(Se indicarán los números de teléfono o frecuencias de radio a ser empleadas)*	
Para la Estación Marítima:	Par el buque:

Estación Marítima

.....

Oficial de Seguridad de la Estación Máritima

.....

Capitán

.....

Oficial de Seguridad del Buque

.....

Compañía

.....

Oficial de Seguridad de la Compañía

.....

Anexo III – Registros

Se registrarán y conservarán los documentos justificativos (33) correspondientes a:

1) Declaraciones de Seguridad acordadas con buques.
2) Incidentes de seguridad y violaciones de la protección.
3) Cambios de niveles de protección activados.
4) Formación de seguridad marítima recibida por el personal de la Estación Marítima.
5) Ejercicios y simulacros de seguridad realizados.
6) Mantenimiento, calibración y ensayos de los de equipos de seguridad.
7) Auditorías y revisiones internas de seguridad.
8) Actualizaciones del Plan de Protección de la Estación Marítima.
9) Enmiendas al Plan de Protección de la Estación Marítima.

4. CUARTA PARTE: CONCLUSIONES

Este trabajo pretende ser ilustrativo del presente contexto, nacional e internacional, en materia de protección marítima y de las medidas preventivas, proactivas o mitigadoras que pueden ser aplicables a una instalación portuaria como la Estación Marítima, destinada a facilitar el transporte intermodal de las personas en su paso de los medios terrestre al marítimo, y viceversa: de ese modo, se plantea una estructura humana de seguridad que gestionará los recursos y adaptará constantemente las medidas y controles a las normativas que se desarrollan a nivel internacional y que posteriormente se transponen al ordenamiento jurídico español; también se alude a un buen número de los medios técnicos, equipos y ayudas que actualmente se utilizan para garantizar la seguridad y la continuidad del transporte marítimo; por último, se proponen medidas organizativas (como la zonificación, la inspección de equipajes facturados, por niveles, o el establecimiento de un sistema de acreditaciones personales) dirigidas a maximizar la efectividad de los controles y favorecer el cometido del personal de seguridad.

Hay que tener en cuenta que una infraestructura en la que convergen intereses privados (todos aquellos que participan directa e indirectamente en el negocio marítimo) y públicos (el control de los puntos fronterizos y todos los aspectos que abarca, de carácter policial, sanitario, fiscal, etc.) requiere de la colaboración de todas las organizaciones involucradas, una absoluta coordinación y cierto grado de conocimiento sobre determinadas parcelas de responsabilidad ajenas.

Asimismo, hay que considerar que los bienes a proteger son de enorme valor desde el punto de vista económico, y más valiosos aún desde el punto de vista humano (las instalaciones o los propios buques, frente a la integridad física de las personas), que las probabilidades de que se materialicen amenazas (como la terrorista o las derivadas del crimen organizado) existen, y que en caso de materializarse las consecuencias pueden llegar a ser desastrosas.

Llegados a este punto y contando con la absoluta certeza de que en el momento presente existen numerosas personas que a título personal o adheridos a organizaciones criminales se ven dispuestas a arriesgarlo todo y cometer actos ilícitos para alcanzar sus objetivos (lucro personal, propaganda, objetivos motivados por razones políticas o religiosas…) cabe preguntarse en qué medida habrían de reforzarse o relajarse las medidas de seguridad y cuál es la inversión que debería

realizarse en medios de seguridad, a sabiendas de los importantes costes que lleva asociados (si bien en este trabajo no se han presupuestado los costes derivados del servicio de seguridad, adquisición y mantenimiento de medios activos y pasivos de protección, formación, etc., se puede adivinar que a mayor número de personas involucradas en la protección, los importes se multiplican, y que el empleo de tecnologías punteras y efectivas es de elevado coste).

Con todo, y dado que la seguridad total es prácticamente imposible de garantizar (39) y que cuanto más nos aproximamos a ella mediante la aplicación de medidas y controles más severos, en mayor medida invadimos la esfera privada y los derechos de los usuarios, parece que se debe optar por un equilibrio entre la inversión y la importancia de los bienes a proteger, sin descuidar la calidad del servicio, intentando optimizar los recursos: en el caso concreto de este trabajo y al objeto de proporcionar un marco útil para su desarrollo y para la confección del Plan de Protección de la Estación Marítima, se plantea un horario operativo continuo H.18, que podría no ser el adecuado para dar servicio a 400.000 pasajeros anuales (como prevé actualmente el Puerto de Santander) (9); es posible que hubiese que reducir ese horario y los recursos humanos de seguridad privada mientras no se llevasen a cabo operaciones, o llegar a acuerdos con las Fuerzas y Cuerpos de Seguridad del Estado para que ellos se hiciesen cargo de la vigilancia de las instalaciones, más allá del horario operativo; en referencia al equipamiento de inspección propuesto, señalar que bien podría servir para atender a un número mucho más elevado de usuarios, pero se ha considerado que con esta configuración se pueden conseguir excelentes tiempos de paso por los controles de seguridad (que resultan violentos a algunos usuarios, por lo que el gestor portuario debe procurar poner los medios para minimizar las molestias) y una óptima operatividad del sistema de inspección.

Según se indica en la memoria anual del Puerto de Santander, correspondiente al año 2013, durante ese año el Puerto de Santander dio servicio a 12 buques de crucero que transportaron a 13.745 pasajeros; el resto de pasajeros que eligieron las instalaciones para sus desplazamientos (196.076), lo hicieron para embarcar o desembarcar de transbordadores (un gran número, transportando mercancías en camiones) (40): hay que señalar que la infraestructura propuesta es capaz de servir a una estación de partida o de destino de buques de crucero y no solo a un puerto de escala, en virtud del equipamiento con el que se ha dotado.

Cabe destacar que la concienciación en materia de seguridad de todo el personal que realice actividades en la Estación Marítima constituye uno de los grandes patrimonios a proteger y a fomentar, puesto que nadie mejor que los trabajadores que conocen el entorno y las instalaciones puede detectar y notificar actitudes sospechosas, intentos de intrusión, la presencia de personas sin acreditar en lugares en los que no deben permanecer, la presencia de objetos abandonados y otros tipos de incidencias que, si bien pueden parecer nimias, pueden resultar importantes o concluyentes.

Finalmente, hay que mencionar que un porcentaje importante de los actos ilícitos cometidos en los puertos son realizados por personas que tienen autorizado el acceso a las instalaciones; es por ello que hay que desarrollar métodos para evaluar la idoneidad de los solicitantes de acreditaciones personales con acceso a zonas controladas o restringidas y denegarlas a quienes tengan antecedentes delictivos coincidentes con ciertos supuestos (4) (una posible opción sería la de requerir certificados de antecedentes penales como condición indispensable para la emisión). En este sentido, también hay que comprender que se desconocen los antecedentes de los tripulantes de los buques que recalan en la instalación y que se debe facilitar su tránsito, hacia y desde tierra, sin permitirles moverse libremente por la zona restringida.

Índice de figuras:

Referencias:

1. **Herbert-Burns, R., Bateman, S., Lehr, P.** *Lloyd's MIU Handbook of Maritime Security.* Boca Raton, London , New York : Auerbach, 2009. 13: 978-1-4200-5480-4.

2. **Gobierno de España: Ministerio de Defensa .** *European Union Maritime Security Strategy.* s.l. : Instituto Español de Estudios Estratégicos, 2014.

3. **Gobierno de España: Presidencia del Gobierno.** *Estrategia de Seguridad Marítima Nacional.* 2013.

4. **Bakir, N. O.** *A Brief Analysis of Threats and Vulnerabilities in the Maritime Domain.* s.l. : Create Research Archive, 2007.

5. **Mc Nicholas, M.** *Maritime Security: An Introduction.* Boston : Butterworth-Heinemann, 2008.

6. **International Maritime Organization.** *Maritime Security Manual: Guidance for Port Facilities, Ports and Ships, V 2.0.* 2011.

7. **Greenberg, M.D., Chalk, P., Willis, H.H., Khilko, I., Ortiz, D.S.** *Maritime Terrorism: Risk and Liability.* s.l. : RAND Center for Terrorism, 2006.

8. **Lipton, E.** Trying to keep Nation's Ferries safe from terrorists. *The New York Times.* 20 Marzo 2005.

9. **Puerto de Santander.** *Plan Director de Infraestructuras 2012-2022 (versión preliminar).* Santander : s.n., 2012.

10. **Gobierno de España: Ministerio del Interior.** Acuerdo de Schengen. [En línea] [Citado el: 01 de 12 de 2014.] http://www.interior.gob.es/web/servicios-al-ciudadano/extranjeria/acuerdo-de-schengen.

11. **Business Alliance for Secure Commerce.** *Guía para establecer la seguridad del perímetro como primera línea de defensa y protección en la organización.*

12. **U.S. Government Accountability Office.** *Maritime Security: Varied actions taken to enhance cruise ship security, but some concerns remain.* 2010.

13. **Australian Government: Department of Infrastructure and Regional Development.** Port Operators' responsibilities and obligations. *Appropiate Signage for Maritime Security Zones.* [En línea] [Citado el: 15 de 12 de 2014.] http://www.infrastructure.gov.au/transport/security/maritime/security_plans/port_operators.aspx.

14. **Worthington Waterway Barriers.** Small Craft Barriers; SCB-32 (Brochure). [En línea] [Citado el: 08 de 06 de 2014.] http://www.tuffboom.com/docs/2009%20SCB-32%20Flyer.pdf.

15. **Sicuralia.** Vallado Perimetral Antiescalado. [En línea] [Citado el: 31 de 05 de 2014.] http://www.sicuralia.com/sensor%20vallado%20VPA.htm.

16. **U.S. Government Department of Defense.** *Unified Facilities Criteria: Security Fences and Gates.* 2013.

17. **Gardner, R. A.** *Rural & Small Town Airport Security Manual and Checklist.* 2002.

18. **Bosch Group.** Bosch Security Systems Worldwide. [En línea] [Citado el: 27 de 05 de 2014.] http://www.boschsecurity.com/startpage/html/index.htm.

19. **Costruzioni Elettroniche Industriali Automatismi S.P.A.** http://www.ceia.net. [En línea] [Citado el: 20 de 06 de 2014.] http://www.ceia.net/security/index.aspx.

20. **Smiths Detection.** http://www.smithsdetection.com. [En línea] [Citado el: 26 de 12 de 2014.] http://www.smithsdetection.com/index.php/es.html.

21. **Rapiscan Systems.** Detección de trazas de explosivos. *Rapiscan Detectra HX*. [En línea] [Citado el: 30 de 06 de 2014.] http://www.rapiscansystems.com/es/products/trace_detection/rapiscan_detectra_hx.

22. **U.S. Department Of Homeland Security: Transportation Security Administration.** TSA Dogs & Aviation Security. *National Explosives Detection Canine Team.* [En línea] [Citado el: 30 de 10 de 2014.] http://www.tsa.gov/about-tsa/tsa-dogs-aviation-security.

23. **IAPA Blogs.** The first destination for frequent flyers. *Are dogs the answer to bomb detection?* [En línea] [Citado el: 30 de 10 de 2014.] http://www.iapa.com/index.cfm/travel/blog.article/blog/community/art/Are-dogs-the-answer-to-bomb-detection.

24. **Airport International.** Hold Baggage Screening Systems. *X-ray & Baggage Screening.* [En línea] [Citado el: 2014 de 10 de 21.] http://www.airport-int.com/article/hold-baggage-screening-systems.html.

25. **Gobierno de España: Ministerio de Fomento.** Programa Nacional para la Seguridad de la Aviación Civil (público). 2014.

26. **Santalices, R.** *La Seguridad Portuaria: El contexto internacional. La situación en la UE y en España.* A Coruña : Instituto Universitario de Investigación sobre Seguridad Interior.

27. **El Parlamento Europeo y el Consejo de la Unión Europea.** Reglamento CE Nº 725/2004 relativo a la mejora de la protección de los buques y las instalaciones portuarias. 2004.

28. **Australian Government: Department of Infrastructure and Regional Development.** Port Operators' responsibilities and obligations. *Guide to preparing a Maritime Security Plan for Port Facility Operators.* 2014.

29. —. Port Operators' responsibilities and obligations. *Guide to preparing a Maritime Security Plan for Port Operators.* 2014.

30. **Puerto de la Bahía de Cádiz.** Autoridad Portuaria de la Bahía de Cádiz. *Departamentos APBC/Planificación y Explotación/Normativa PBIP-ISPS.* [En línea] [Citado el: 17 de 10 de 2014.] http://www.puertocadiz.com/opencms/PuertoCadiz/es/menu/departamentos/planificacion/normativa.html.

31. **Gobierno de España: Ministerio de la Presidencia.** 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.

32. **AENA: Aeropuerto de Ibiza.** Pliego de Cláusulas Particulares. *Expediente para la contratación del Servicio de Mantenimiento del Sistema de CCAA y CCTV.* 2014.

33. **Government of Canada: Minister of Justice.** Marine Transportation Security Regulations. 2014.

34. **Gobierno de España: Ministerio del Interior.** Guardia Civil: Información Institucional. *Misiones.* [En línea] [Citado el: 15 de 09 de 2014.] https://www.guardiacivil.es/es/institucional/misiones/index.html.

35. —. Dirección General de la Policía. *Portada/CNP/Competencias.* [En línea] [Citado el: 15 de 09 de 2014.] http://www.policia.es/cnp/competencias/competencias.html.

36. **Ayuntamiento de Santander.** Ayuntamiento/Áreas y Concejalías/Protección Ciudadana/Servicios/Protección Ciudadana. *Policía Local.* [En línea] [Citado el: 15 de 09 de 2014.] http://portal.ayto-santander.es/portal/page/portal/inet_santander/ficha/ficha_ayto?itemId=560733.

37. **AENA: Aeropuerto de Bilbao.** Pliego de Prescripciones Técnicas. *Expediente para la contratación del mantenimiento del Sistema de CCAA y CCTV.* 2011.

38. **Parfomak, P.W., Fritelli, J.** *CRS Report for Congress: Maritime Security. Potential Terrorist Attacks and Protection Priorities.* s.l. : Congressional Research Service, 2007.

39. **Fritelli, J.** *CRS Report for Congress: Port and Maritime Security Background and Issues for Congress.* s.l. : Congressional Research Service, 2005.

40. **Puerto de Santander.** *Memoria anual.* Santander : s.n., 2013.

Aviso:

Este documento es el resultado del Trabajo Fin de Grado de un alumno, siendo su autor responsable de su contenido.

Se trata por tanto de un trabajo académico que puede contener errores detectados por el tribunal y que pueden no haber sido corregidos por el autor en la presente edición.

Debido a dicha orientación académica no debe hacerse un uso profesional de su contenido.

Este tipo de trabajos, junto con su defensa, pueden haber obtenido una nota que oscila entre 5 y 10 puntos, por lo que la calidad y el número de errores que puedan contener difieren en gran medida entre unos trabajos y otros,

La Universidad de Cantabria, la Escuela Técnica Superior de Náutica, los miembros del Tribunal de Trabajos Fin de Grado así como el profesor tutor/director no son responsables del contenido último de este Trabajo.”