MINISTERIO DE OBRAS PÚBLICAS Y TRANSPORTES

DIVISIÓN MARITIMO PORTUARIA
DIRECCION DE NAVEGACIÓN Y SEGURIDAD

MANUAL PARA LA APLICACIÓN DEL CÓDIGO PBIP EN INSTALACIONES PORTUARIAS

ELABORACIÓN
JUNIO, 2013

Contenido

1. INTRODUCCIÓN

La Protección de las Instalaciones Portuarias está sujeta a las normas jurídicas, técnicas y de seguridad vigentes tanto a nivel nacional como internacional. Estas normas son las adoptadas en el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (PBIP) y las disposiciones que el Gobierno de Costa Rica a través de las autoridades competentes implemente en todos los muelles y puertos marítimos y/o fluviales habilitados para el comercio exterior de mercancías, servicios y de pasajeros de transporte internacional

Las medidas y procedimientos de protección establecidos y los que se establezcan, se aplicarán en las instalaciones portuarias de modo que reduzcan al mínimo los inconvenientes o demoras para los pasajeros, los buques, el personal y los visitantes de los buques, las mercancías y los servicios.

2. OBJETIVOS

Objetivo General:

Establecer las disposiciones necesarias para que las instalaciones portuarias del país utilizadas para el comercio internacional, cumplan a las disposiciones del Capítulo XI-2 “Medidas Especiales para Incrementar la Protección Marítima” del Convenio SOLAS; así como lo establecido en el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias, que fueron adoptadas el 12 de diciembre del 2002 por la Conferencia de los Gobiernos Contratantes del Convenio Internacional para la Seguridad de la Vida Humana en el Mar, SOLAS (Safety Of Life at Sea) 1974.

Objetivos Específicos

- Definir las funciones y responsabilidades de los entes encargados de la protección,
- Garantizar la recopilación y el intercambio de información.
- Establecer una metodología para efectuar evaluaciones y planes de protección, garantizando el establecimiento de medidas preventivas de protección adecuadas y proporcionadas, contra los sucesos que afecten a la protección de los buques o instalaciones portuarias utilizadas para el comercio internacional.
- Establecer una metodología para efectuar las auditorías externas a las instalaciones portuarias.
- Establecer parámetros básicos para el manejo de la documentación digital.

3. RESEÑA HISTÓRICA

Tras los trágicos acontecimientos del 11 de septiembre de 2001, la vigésima segunda Asamblea de la Organización Marítima Internacional OMI, celebrada en noviembre de 2001, acordó por unanimidad que se debían elaborar nuevas medidas en relación con la protección de los buques y de las instalaciones portuarias, las cuales se adoptarían en una Conferencia de los Gobiernos Contratantes del Convenio Internacional para la seguridad de la vida humana en el mar, 1974. (Convenio SOLAS 1974 por sus siglas en inglés).

Asimismo, la Conferencia diplomática sobre protección marítima celebrada en Londres en diciembre de 2002 adoptó nuevas disposiciones del SOLAS 1974, así como el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias, PBIP, para incrementar la protección marítima. Estas nuevas prescripciones constituyen el ordenamiento internacional que permite a los buques y las instalaciones portuarias puedan cooperar para detectar y prevenir actos que supongan una amenaza para la protección del sector del transporte marítimo.

Las disposiciones del capítulo XI-2 del Convenio SOLAS 1974 y del Código PBIP son aplicables a los buques y a las instalaciones portuarias. La ampliación del Convenio SOLAS 1974 a las instalaciones portuarias se acordó partiendo de la base que ese Convenio ofrece el medio más rápido para conseguir que las medidas necesarias relativas a la protección marítima entren en vigor y se apliquen prontamente. No obstante, se acordó asimismo que las disposiciones relativas a las instalaciones portuarias se aplicarán únicamente a la interfaz buque-puerto.

En nuestro país, el Código PBIP fue incorporado inicialmente a nuestra legislación por medio del Decreto N° 31 848–MOPT, se divulga el Reglamento para la protección de los buques e Instalaciones Portuarias, publicado en el Alcance N° 27 Gaceta N° 119, del viernes 18 de junio del 2004. Posteriormente, el Convenio SOLAS fue incorporado a nuestra legislación por medio de la Ley N° 8708 del 23 de diciembre del 2010.

4. BASE LEGAL

- Ley N° 4786 de julio de 1971 (Ley de Creación del Ministerio de Obras Públicas y Transportes).
- Ley N° 7091 (Convenio de las Naciones Unidas sobre el Derecho del Mar) ratificado por Costa Rica mediante Ley Nº 7291 de fecha 12 de marzo de 1992, que establece en su artículo 146 que se deben adoptar las medidas que sean necesarias para asegurar la eficaz protección de la vida humana en el mar. Con este objeto, la Autoridad puede establecer normas, reglamentos y

procedimientos apropiados que complementen el derecho internacional existente.

- Ley N° 8708 publicada en el Alcance Digital N°4 a La Gaceta N° 249 del 23 de diciembre de 2010 (Convenio Internacional sobre la vida humana en el mar (conocido como SOLAS, por sus siglas en inglés).
- Código Internacional de Protección de Buques y de las Instalaciones Portuarias (Código PBIP).
- Decreto Ejecutivo Nº 31845-MOPT (Reglamento para la Protección de los Buques y de las Instalaciones Portuarias (Código PBIP).
- Decreto Ejecutivo N°28869-MOPT "Reglamento para regular el ingreso de Naves Extranjeras en el Territorio Nacional".
- Decreto Ejecutivo N° 29547-MOPT (Reforma organizativa y funcional del Ministerio de Obras Públicas y Transportes).
- Circular MSC/1192 de la OMI.

5. DEFINICIONES

Para la interpretación de los términos que no se hallen listados aquí, deberá referirse a la Regla XI-2/1 y Código de Protección del Buque y de las Instalaciones Portuarias en su parte "A". Así como en el Capítulo XI-2 del Convenio SOLAS.

Accesibilidad: grado de facilidad para acceder a la instalación portuaria. El término se relaciona con las barreras físicas y geográficas que pueden disuadir una amenaza, sin necesidad de protección.

Actividad buque a buque: toda actividad no relacionada con una instalación portuaria que suponga el traslado de mercancías o personas de un buque a otro.

Auditoría: Proceso sistemático, independiente y documentado para obtener pruebas de auditoría y evaluarlas objetivamente con el fin de determinar en qué medida se cumplen los criterios de auditoría.

Amenaza: Posibilidad de que un incidente de protección ocurra.

Administración Marítima: Involucra a aquellos órganos de la Administración Pública que velan por los intereses del país vinculados a la navegación y al transporte marítimo, lo que incluye además la seguridad de la navegación (vidas humanas, buques, bienes, medio marino, etc.) y la protección marítima.

Capitanía de Puerto: Oficinas Regionales marítimas a cargo de un capitán de puerto, establecidas para el desarrollo de las competencias de la Dirección de Navegación y Seguridad (DNS).

Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (Código PBIP): Documento que contiene una Parte A, cuyas disposiciones son de carácter obligatorio, y una parte B, cuyas disposiciones tendrán carácter de recomendación, adoptado el 12 de diciembre de 2002 mediante la resolución 2 de la Conferencia de los Gobiernos Contratantes del Convenio internacional para la seguridad de la vida humana en el mar, 1974, según sea enmendado por la Organización Marítima Internacional.

Conclusión: Observación o incumplimiento.

Comité de Protección Portuaria (CPP): Es el Comité conformado por autoridad de alto mando de jurisdicción, entidades gubernamentales y privadas, ubicadas en las cercanías del puerto y que de una forma u otra sus funciones estén ligadas a la protección nacional y del puerto. (DNS, Dirección de Inteligencia y Seguridad (DIS), Organismos de Investigación Judicial (OIJ), Cruz Roja, Bomberos, Ministerio de Seguridad Pública (MSP), Dirección de Migración y Extranjería, Servicio Nacional de Guardacostas, K9).

Considerar: Significa que las estrategias para mitigar serán analizadas caso por caso. El plan de protección de las instalaciones portuarias contendrá los incidentes evaluados, los resultados y las razones por las cuales las medidas para mitigar los daños fueron o no elegidas**.**

Consejo Nacional de Educación Superior (CONESUP): Organismo adscrito al Ministerio de Educación Pública creado mediante Ley No. 6693 el 27 de noviembre de 1981.

Criterios de auditoría: Conjunto de políticas, prácticas, procedimientos, principios, prescripciones o requisitos frente a los cuales el auditor compara las evidencias recogidas.

Cumplimiento: Observancia de una prescripción.

Declaración de Cumplimiento de la IP (DCIP): documento expedido por la DNS, mediante el cual avala que una IP cumple satisfactoriamente con lo establecido en el Código PBIP.

Declaración de Protección Marítima (DPM): acuerdo alcanzado entre un buque y una instalación portuaria u otro buque con el que se realiza operaciones de interfaz, en el que se especifican las medidas de protección que aplicará cada uno.

Dirección de Navegación y Seguridad (DNS): Dirección de la División Marítimo Portuaria del Ministerio de Obras Públicas y Transportes que tiene a cargo la Administración Marítima Nacional y por ende la ejecución de la rectoría en materia marítima. Responsable de la implantación de las disposiciones relativas a la protección de la IP y a la interfase buque-puerto.

Documentar: En el proceso de evaluación de protección, implica que el incidente tal vez no amerite analizar la necesidad de aplicar una medida de mitigación y, por lo tanto, sólo debe documentarse de modo que sea considerado en las próximas revisiones del Plan. Sin embargo, cuando se trate de medidas con bajo costo de implementación, corresponde evaluar su aplicación.

Documentación secreta: Información o conocimiento que es restringida; para poder acceder a los documentos clasificados como secretos se necesita un permiso de un funcionario autorizado.

Documentación reservada: Información o conocimiento que es privado o que no debe darse a conocer.

Documento: Instrumento o escrito con información y su soporte

Evaluación de Protección de la Instalación Portuaria (EPIP): Es un análisis de riesgo de todos los aspectos de las operaciones de la instalación portuaria para determinar qué elemento o elementos de éstas son más susceptibles y/o tiene más probabilidad, de sufrir un ataque.

Equipaje no acompañado: Se refiere a todo equipaje, incluido los enseres personales, que no esté con el pasajero o el miembro del personal del buque en el lugar de la inspección o registro.

Incidente de protección de la IP: Es cualquier circunstancia, activa, pasiva o sospechosa, en la cual elementos humanos intenten o concreten actos ilícitos contra la instalación portuaria, sus facilidades, las cargas, las personas o los buques que operen en ella, o que concreten dichas acciones contra terceros utilizando la instalación o al buque, su carga o su tripulación, como intermediario de estos actos ilícitos. Comprende asimismo la utilización de la instalación portuaria, como objeto o intermediario para llevar a cabo actos de piratería, hurto, terrorismo, contrabando, tráfico de drogas o precursores, tráfico de armas, esclavitud, inmigración ilegal, etc.

Incumplimiento: Situación observada en la que hay pruebas objetivas que indican que no se ha cumplido una determinada prescripción.

Información: Datos significativos.

Instalación portuaria (IP): Es el área donde tiene lugar la interfaz buque-puerto. Esta incluye, según sea necesario, las zonas como los fondeaderos, atracaderos de espera y accesos desde el mar a los puertos y muelles de comercio exterior, y operados o no por sociedades portuarias,

Interfaz Buque-Puerto: Interacción que tiene lugar cuando un buque se ve afectado directa e inmediatamente por actividades que involucran el movimiento de personas o mercancías o la provisión de servicios portuarios al buque o desde éste.

Medidas correctivas: Medidas para eliminar la causa de un incumplimiento detectado u otra situación no deseada.

Medidas preventivas: Son aquellas medidas para eliminar la causa de un posible incumplimiento u otra posible situación no deseada.

Mitigar: Cualquier medida tendiente a reducir el nivel de riesgo. En el proceso de evaluación de protección, significa que necesariamente deben implementarse acciones para reducir el riesgo **(mitigación)**. Estas estrategias pueden incluir medidas y/o procedimientos de protección, a fin de reducir el riesgo para dicho incidente de protección.

Nivel de Protección (NP): Graduación del riesgo en caso de que ocurra o se intente provocar un suceso que afecte a la protección marítima. La Dirección de Navegación y Seguridad determinará los niveles de protección para las instalaciones portuarias Nacionales e impartirá, según sea necesario, las instrucciones oportunas y facilitará información sobre los aspectos de protección a los buques y las instalaciones portuarias que puedan verse afectados.

Nivel de Protección 1 (NP1): Es el nivel en el cual se deberán mantener medidas mínimas adecuadas de protección en todo momento.

Nivel de Protección 2 (NP2): Es el nivel en el cual se deberán mantener medidas adecuadas de protección adicionales durante un periodo de tiempo, como resultado de un aumento del riesgo de que ocurra un suceso que afecte a la protección marítima.

Nivel de Protección 3 (NP3): Es el nivel en el cual se deberán mantenerse más medidas concretas de protección durante un periodo de tiempo limitado cuando sea probable o inminente un suceso que afecte a la protección marítima.

Observación: Exposición de hechos formulada durante una auditoría y justificada con pruebas objetivas.

Oficial de Protección del Buque (OPB): Persona a bordo del buque, responsable ante el capitán y designada por la compañía para responder por protección del buque, incluidos la implantación y el mantenimiento del PPB, y para la coordinación con el oficial de la compañía para la protección marítima y con los oficiales de protección de las instalaciones portuarias.

Oficial de la Compañía para la Protección Marítima (OCPM): persona designada por la compañía para asegurar que se lleve a cabo una evaluación sobre la protección del buque y que el plan de protección del buque se desarrolla, se presenta para su aprobación, y

posteriormente se implanta y mantiene, y para la coordinación con los oficiales de protección de las instalaciones portuarias y con el oficial de protección del buque.

Oficial de Protección de la Instalación Portuaria (OPIP): persona designada para asumir la responsabilidad de la elaboración, implantación, revisión y actualización del plan de protección de la instalación portuaria, y para la coordinación con los oficiales de protección de los buques y con los oficiales de protección de las compañías para la protección marítima.

Operador Portuario Entidad pública o privada que tiene a su cargo la administración y operación de una o varias terminales portuarias.

Organización de Protección Reconocida (OPR): Organización debidamente especializada en cuestiones de protección y con un conocimiento adecuado en cuestiones de protección y en operaciones de los buques y de los puertos autorizada para realizar una actividad de evaluación, o de verificación, o de aprobación, o de certificación prescrita en el presente Manual o en concordancia al Código PBIP.

Plan de Protección del Buque (PPB): plan elaborado para asegurar la aplicación a bordo del buque de medidas destinadas a proteger a las personas que se encuentren a bordo, la carga, las unidades de transporte, las provisiones de a bordo o el buque de los riesgos de un suceso que afecte a la protección marítima.

Plan de Protección de la Instalación Portuaria (PPIP): plan elaborado para asegurar la aplicación de medidas destinadas a proteger la instalación portuaria y los buques, las personas, la carga, las unidades de transporte y las provisiones de los buques en la instalación portuaria de los riesgos de un suceso que afecte a la protección marítima.

Prescripciones: Necesidad o expectativa formulada, generalmente implícita u obligatoria.

Procedimiento: Manera específica de llevar a cabo una actividad o un proceso.

Proceso: Serie de actividades interrelacionadas o interactivas que transforman los aportes en resultados.

Prórroga: Es el acto mediante el cual la DNS a amplía el termino de vigencia de una autorización o certificación.

Pruebas de auditoría: Registros, exposiciones de hechos u otra información que guarden relación con los criterios de auditoría y se puedan verificar.

Pruebas objetivas: Información cuantitativa o cualitativa, registros o exposiciones de hechos, basados en observaciones, medidas o análisis y que puedan verificarse

Refrendo: Es el acto de visado efectuado por la DNS, en el cual se certifica que durante las verificaciones periódicas, se mantienen las condiciones iniciales que dieron origen a la

expedición del certificado. Este acto se realiza durante el tiempo de vigencia de una certificación.

Registros: Documentos que exponen los resultados alcanzados o que dan prueba de las actividades realizadas.

Renovación: Es el acto de expedición de una nueva certificación antes de su vencimiento previa verificación de todos los aspectos relativos al cumplimiento de los requerimientos del Código de Protección de Buques e Instalaciones Portuarias (PBIP)

Riesgo: efecto combinado de la gravedad de un incidente, la amenaza de ocurrencia del mismo y la vulnerabilidad del elemento

Riesgo = Gravedad x Amenaza x Vulnerabilidad

- **Gravedad:** Consecuencia de un incidente en caso que éste se concrete, medido en pérdidas de vidas humanas, lesiones personales, daño ambiental, daño a los bienes o en perjuicio económico

- **Amenaza:** Posibilidad de que un incidente de protección ocurra.

- **Vulnerabilidad**: Predisposición o susceptibilidad que tiene un elemento a ser afectado por un incidente de protección. Consta de 4 (cuatro) elementos que deberán ser considerados y se detallan a continuación:

  Disponibilidad: La presencia y predicción en relación a la habilidad de planear un ataque.

  Accesibilidad: Facilidad de producir el incidente, en relación a las barreras físicas y geográficas que determinan la amenaza sin seguridad orgánica.

  Protección orgánica: La habilidad del personal de seguridad para detener un incidente, esto incluye los planes de seguridad, capacidad de comunicación, guardia, detección de intrusos y tiempo de reacción de las fuerzas externas para prevenir el incidente.

  Estructura de la instalación: La capacidad de la instalación portuaria de soportar un incidente específico basado en la complejidad del diseño y los materiales de construcción.

Suceso que Afecta a la Protección Marítima: todo acto o circunstancia que levante sospechas y que constituya una amenaza para la protección de un buque, incluidas las

unidades móviles de perforación mar adentro y las naves de gran velocidad, de una instalación portuaria, de una interfaz buque-puerto o de una actividad buque-buque.

Verificación: Confirmación, mediante la aportación de pruebas objetivas, de que determinadas prescripciones se han cumplido

6. SIGLAS

CCTV	Circuito Cerrado de Televisión
CONARE	Consejo Nacional de Rectores
CONESUP	Consejo Nacional de Educación Superior
CPP	Comité de Protección Portuaria.
DCIP	Declaración de Cumplimiento de la IP
DMP	División Marítimo Portuaria.
DNS	Dirección de Navegación y Seguridad
DPM	Declaración de Protección Marítima
EPIP	Evaluación de Protección de la Instalación Portuaria
IMO	Siglas en inglés de la Organización Marítima Internacional.
INCOP	Instituto Costarricense de Puertos del Pacífico
IP	Instalación Portuaria
JAPDEVA	Junta de Administración Portuaria y de Desarrollo Económico de la Vertiente Atlántica de Costa Rica
MARPOL	Siglas en inglés de Convenio Internacional para prevenir la contaminación por los Buques
MOPT	Ministerio de Obras Públicas y Transportes
NP	Nivel de Protección
NP1	Nivel de Protección 1
NP2	Nivel de Protección 2
NP3	Nivel de Protección 3

OCPM	Oficial de la Compañía para la Protección Marítima
OMI	Organización Marítima Internacional.
OPB	Oficial de Protección del Buque
OPIP	Oficial de Protección de la Instalación Portuaria
OPR	Organización de Protección Reconocida
PBIP	Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias.
SOLAS	Convenio Internacional para la Seguridad de la Vida Humana en el Mar (Safety Of Life at Sea).
PPB	Plan de Protección del Buque
PPIP	Plan de Protección de la Instalación Portuaria
NVIC	Navigation and Vessel Inspection Circular
RBDM	Toma de Decisiones Basada en el Riesgo

7. GUIA PARA EL DESARROLLO DE LA EVALUACIÓN DE PROTECCIÓN DE LAS INSTALACIÓN PORTUARIA (EPIP)

La Evaluación de Protección de las Instalación Portuaria (EPIP) consiste fundamentalmente en un análisis del riesgo de todos los aspectos del funcionamiento de la Instalación Portuaria (IP), para determinar qué partes de ella son más susceptibles, y/o el objetivo más probable para que se ocasione un incidente de Protección.

Es una atribución del Gobierno de Costa Rica en materia de protección realizar, examinar y aprobar la evaluación de la protección de las instalaciones portuarias y sus respectivas modificaciones; la cual es parte integrante y esencial del proceso de elaboración y actualización del plan de protección de la instalación portuaria.

Las Autoridades Portuarias, INCOP y JAPDEVA, presentarán una Evaluación de Protección de la Instalación Portuaria bajo su fiscalización, utilizando la metodología y forma descritas en este manual, para el correspondiente estudio y análisis y eventual aprobación por parte de la DNS.

Es responsabilidad de la Dirección de Navegación y Seguridad (DNS) revisar, aceptar y conservar la evaluación de la protección de la IP, por un el término no menor de cinco (5) años.

El Gobierno de Costa Rica a través de la DNS podrá autorizar a una organización de protección reconocida (OPR) para que realice la evaluación de la protección de una determinada instalación portuaria situada en su territorio.

7.1. Aspectos a incluir en la Evaluación de Protección de la IP

La Evaluación de la IP deberá contener como mínimo los siguientes aspectos:

a) Identificación y evaluación de los bienes e infraestructuras que son importantes proteger.
b) Identificación de las posibles amenazas para esos bienes e infraestructura y la probabilidad de ocurrencia, a fin de establecer medidas de protección y el orden de prioridad de las mismas.
c) Identificación, selección y clasificación por orden de prioridad de las medidas para contrarrestar las amenazas y de los cambios de procedimientos y su grado de eficacia para reducir la vulnerabilidad.
d) Identificación de los puntos débiles, incluidos los relacionados con el factor humano, infraestructura, políticas y procedimientos.

7.2. Aspectos de las instalaciones portuarias a considerar en un EPIP

En toda EPIP deben considerarse los siguientes aspectos de la instalación portuaria:

a) protección física;
b) integridad estructural;
c) sistemas de protección del personal;
d) normas y procedimientos;
e) sistemas radioeléctricos y de telecomunicaciones, incluidos los sistemas y redes informáticos;
f) infraestructura de transporte;
g) servicios públicos; y
h) otras zonas que, al sufrir daños, o ser utilizadas como punto de observación para fines ilícitos, podrían poner en peligro a las personas, los bienes o las operaciones que se realicen dentro de la instalación portuaria.

La EPIP se ajustará al proceso de evaluación que se muestra en el punto 7.5 denominado "*Guía para el análisis de riesgos en la evaluación de la protección en una instalación portuaria*", en caso contrario se presentará previamente el método de evaluación a utilizar a la Dirección de Navegación y Seguridad (DNS).para su correspondiente visto bueno.

7.3. Solicitudes de evaluación de protección de una instalación

Cuando el operador portuario esté interesado en obtener la Evaluación de Protección de una Instalación Portuaria, deberá presentar solicitud por escrito ante la DNS, en la que precise lo siguiente:

a) Nombre, denominación o razón social del operador portuario;
b) Domicilio social del operador portuario;
c) Instalación Portuaria a evaluar, y
d) En caso de representante legal, señalar su nombre y domicilio.

La solicitud, deberá estar acompañada de los siguientes documentos:

e) Mandato o poder del representante legal, si éste es quien promueve;
f) Plano de la instalación portuaria a evaluar, con identificación de sus distintas áreas de operación, incluyendo fondeaderos, atracaderos de espera, accesos desde el mar y boyas de amarre;
g) Lista del personal destinado a la protección o seguridad de la instalación portuaria;
h) Lista de equipos destinados a la seguridad y la operación de la instalación portuaria, y
i) En su caso, planes de protección y seguridad aplicables a la instalación portuaria.

Una vez presentados los requisitos completos (solicitud de evaluación y la documentación correspondiente), la DNS comunicará al solicitante la fecha en que procederá a realizar la evaluación. La duración de la evaluación no será mayor a treinta días hábiles.

Concluida la evaluación, en un plazo máximo de veinte días hábiles la Administración Marítima entregará al interesado el resultado que corresponda. La evaluación que emita por Administración Marítima, tendrá una vigencia de tres meses, plazo durante el cual tendrá que presentarse para su aprobación el Plan de Protección de la Instalación Portuaria.

Si se vence el periodo de tres meses de vigencia sin que el interesado presente el plan de protección, se deberá gestionar una nueva solicitud de evaluación e iniciar el proceso correspondiente.

Las evaluaciones de la protección de la instalación portuaria se revisarán y actualizarán periódicamente, teniendo en cuenta los posibles cambios de las amenazas o los cambios menores en la instalación portuaria y en todos los casos, se revisarán y actualizarán cuando se registren cambios importantes en la IP.

7.4. Formato guía para la evaluación de protección de una instalación portuaria de acuerdo al código PBIP

7.4.1. Carátula Principal/Revisión y Aprobación de la Evaluación de Protección de la Instalación Portuaria

<table>
<tr><td rowspan="4">Logo de la IP</td><td rowspan="4">EVALUACIÓN DE PROTECCIÓN DE LA INSTALACIÓN PORTUARIA

(Nombre de la IP)</td><td>Edición</td><td>Modificación</td><td rowspan="4"></td></tr>
<tr><td>00/00/00</td><td>00/00/00</td></tr>
<tr><td>Versión</td><td>Control</td></tr>
<tr><td>00</td><td>DNS / IP</td></tr>
</table>

EVALUACIÓN DE PROTECCIÓN DE LA INSTALACIÓN PORTUARIA (EPIP)[1]

Ejemplar No: _____

(Nombre de la Instalación Portuaria)

(Foto)

Aprobado por el Director de la Dirección de Navegación y Seguridad: Nombre:_____ Fecha _____ Firma: _____	**V/B°. por el Director General de la División Marítimo Portuaria:** Nombre:_____ Fecha: _____ Firma: _____
La Evaluación de Protección de la Instalación Portuaria, ha sido elaborada y aprobada bajo prescripciones aplicables según el Capítulo XI-2, Regla 10 del Convenio SOLAS, enmendado, el Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias - Código PBIP, y Decreto Nº 31845-MOPT Reglamento para la Protección de los Buques y de las Instalaciones Portuarias.	

[1] Documento Confidencial/ Secreto. Queda prohibido difundir o reproducir total o parcialmente, sin la debida autorización y control.

7.4.2. Identificación y antecedentes de la instalación portuaria

7.4.2.1. Identificación

Para la identificación se debe cumplir con el llenado de la tabla 1A y 1B como se detalla a continuación

Tabla 1A

IDENTIFICACIÓN DE LA RAZÓN SOCIAL Y JURÍDICA DE LA INSTALACIÓN PORTUARIA		
1	Nombre de la Empresa:	
2	Cédula Jurídica:	
3	Representantes Legales:	
	(1)	(2)
4	Tel. de Oficina:	Tel. de Oficina:
	Fax:	Fax:
	Celular:	Celular:
	E-mail:	E-mail:
5	Dirección y Localización de las Oficinas en Costa Rica:	

Tabla 1B

IDENTIFICACIÓN DE LA INSTALACIÓN PORTUARIA		
1	Nombre de la Instalación Portuaria:	
2	Tipo de Administración:	
3	Propiedad:	
4	Datos de Contacto del OPIP	Datos de Contacto del Gerente
	Tel. de Oficina:	Tel. de Oficina:

	Fax:	Fax:
	Celular:	Celular:
	E-mail:	E-mail:
5	Dirección y Localización de la Instalación Portuaria	
	Litoral:(Costa Pacífico/Atlántico)	Provincia:
	Cantón:	Distrito:
	Área:	
	Latitud:	Longitud:

7.4.2.2. Récord de Distribución y Control de la Evaluación de Protección de la Instalación Portuaria

Control de Ejemplares de la EPIP

Se debe estampar una descripción textual de la responsabilidad, edición, distribución y mantenimiento de la evaluación de protección, indicar cuantos ejemplares hay en existencia, quienes tienen acceso a ellos y quienes custodian la llave.

Además, se debe indicar cómo se garantiza la información confidencial contenida en la EPIP, ya sea en papel o formato electrónico.

También se debe detallar cual es el personal autorizado para la manipulación de la EPIP, en documento físico y digital y las medidas a seguir para garantizar la confidencialidad de la información y como se salvaguarda el resto de la documentación de protección.

Así mismo se debe completar información según criterio del OPIP.

En cumplimiento de lo anterior se debe crear una tabla con la identificación de la distribución de ejemplares aprobados por la DNS, según se indica a continuación en la tabla 2,

Tabla 2

Control de Ejemplares de la EPIP

No. Ejemplar	Responsable(Nombre y Cargo)	Ubicación del ejemplar aprobado (Lugar Específico)	Nombre de los funcionarios con acceso a la información	Firma

Igualmente, se debe llevar un control para las revisiones y actualizaciones parciales considerando los aspectos establecidos en la tabla 3.

Tabla 3

DOCUMENTO DE CONTROL PARA LAS REVISIONES Y ACTUALIZACIONES PARCIALES DE LA EVALUACIÓN DE PROTECCIÓN PORTUARIA					
No.	Ref. EPIP	Cambios /Actualización	Fecha:	Nombre y Firma Responsable	
				IP (OPIP)	Revisado y Aprobado por AMP(DNS)
01					
02					
03					
04					
05					
06					
07					
08					
09					
10					

7.4.2.3. Información general de la instalación portuaria

Propiedad y ejecutivos

En este apartado se debe incluir los datos de contacto para ubicar a los representantes legales del operador portuaria y al OPIP, durante las 24 horas del día los 7 días a la semana.

Actividad de la instalación portuaria

En este ítem se hace una descripción general de las actividades que se desarrollan en la instalación portuaria, incluyendo clase de tráfico, tipos de buques que prestan servicios, naturaleza de la carga y pasajeros que utilizan la instalación.

7.4.2.4. Información externa de la instalación portuaria

Entorno

1. Con respecto al entorno se debe presentar plano de ubicación geográfica en que se demarquen los límites físicos de la instalación, vías de aproximación y acceso, ubicación de la Administración Marítima, delegaciones policiales, bomberos y servicios médicos. De igual manera, se deben completar los datos pertinentes en la tabla 4 siguiente.

Tabla 4

INFORMACIÓN EXTERNA DE LA INSTALACIÓN PORTUARIA (ENTORNO)					
Entidad/ Servicios	**Dirección**	**Actividades que se desarrolla**	**Teléfono**	**Distancia**	**Tiempo Estimado**

2. Se identifican las características del entorno con énfasis en las que resultan ser un riesgo para sus operaciones.

7.4.2.5. Información interna de la IP

La información solicitada en esta sección es la versión ampliada de la identificación y los antecedentes de la instalación portuaria, expuestos en las secciones anteriores, pero con detalle de lo referente a la parte físico

operativa general del puerto para un análisis adecuado en materia de protección.

Instalaciones

1. Descripción física de las instalaciones.
2. Características.

También se debe indicar si el terminal para buques cargueros es compartido con los buques de pasaje. Si existe instalación exclusiva para buques de pasaje, describir sus características y medidas de protección para los tripulantes, pasajeros y equipaje acompañado.

3. Presentar plano que contenga la siguiente información:
   a. Almacenamiento de Mercancías Peligrosas;
   b. Depósitos o surtidores de combustible;
   c. Sistema de agua de potable;
   d. Áreas y Barreras perimetrales;
   e. Áreas de aforo y desaforo;
   f. Área de almacenamiento bajo techo;
   g. Área de depósito descubiertas;
   h. Área de estacionamientos;
   i. Muelles;
   j. Áreas de edificios administrativos, empresas privadas y de bienestar a la gente de mar y los trabajadores portuarios.
   k. Estaciones Reefer para la carga;
   l. Equipos de manipulación de carga y utilería;
   m. Puertas de acceso y salida; y
   n. Detallar los servicios esenciales con sus respectivos equipos de reserva de los que dependa la instalación, como son: agua, electricidad, gas, teléfono, alcantarillado u otros, y su incidencia en las operaciones normales de la entidad.

7.4.3. Generalidades

En la EPIP debe considerarse al menos, los siguientes aspectos:

1. Protección física;
2. Integridad estructural;
3. Sistema de protección del personal;
4. Normas y procedimientos de protección;

5. Sistemas radioeléctricos y de comunicaciones, incluidos los sistemas y redes informáticas;
6. Infraestructura de transporte, servicios públicos; y
7. Otras zonas que, al sufrir daños o ser utilizadas como punto de observación para fines ilícitos, podrían poner en peligro a las personas, los bienes o las operaciones que se realicen dentro de la IP.

7.4.4. Identificación y evaluación de los bienes e infraestructuras que se deben proteger

Se requiere establecer la importancia relativa de las distintas estructuras e instalaciones para el funcionamiento de la IP. Se debe considerar en esta evaluación el impacto que pueda causar una emergencia o atentado con consecuencia de pérdidas de vidas, paralización de actividades y daños en las zonas de importancia económica del puerto. Así, como, la capacidad para restablecer los servicios que pudieren resultar dañados.

Adicionalmente, se debe establecer un orden de prioridades de protección basado en la identificación y evaluación de la importancia relativa de los bienes e infraestructuras.

Los bienes e infraestructura que deben considerarse importantes de proteger pueden ser, entre otros, los siguientes:

1. Accesos, entradas, vías de acercamiento, fondeaderos a la gira y zonas de maniobra y atraque;
2. Instalaciones para carga, tales como terminales, zonas de almacenamiento y equipos de manipulación de la carga;
3. Sistemas de distribución eléctrica, sistemas de comunicaciones, sistemas y redes informáticos;
4. Sistemas de gestión de tráfico de buques en el puerto y ayudas a la navegación;
5. Plantas eléctricas, maquinarias y cintas transportadoras de transferencia de carga, conductos de suministros de agua;
6. Puentes, vías férreas, carreteras;
7. Embarcaciones de servicio del puerto, que incluyen embarcaciones de prácticos, remolcadores, gabarras, etc.;
8. Equipos y sistemas de protección y vigilancia; y
9. Control sobre las aguas adyacentes a la IP.

La identificación clara de los bienes e infraestructura es un proceso que puede requerir realizar consultas con las autoridades pertinentes en relación con las estructuras adyacentes a la IP que pudieran causar daños dentro de la instalación o utilizarse para causar daños a la instalación, así como para ser usados para observar con fines ilícitos la instalación o desviar la atención.

7.4.5. Identificación de las posibles amenazas para los bienes e infraestructuras y cálculo de la probabilidad de que dichas amenazas se materialicen a fin de establecer medidas de protección y el orden de prioridad de las mismas

Se requiere la identificación de toda acción que pueda ser una amenaza para la protección de las cargas, bienes e infraestructuras, así como, los métodos en que estos hechos pueden ser llevados a cabo, lo anterior, permite evaluar las condiciones de vulnerabilidad en que se encuentra un determinado bien o lugar. Determinada la vulnerabilidad, queda en evidencia las fallas a la protección, y por ende las necesidades de adoptar medidas para contrarrestar aquellas amenazas.

La Evaluación de Protección de la Instalación Portuaria debe incluir las amenazas para cada IP, inclusive las determinadas por la Administración Marítima u organizaciones gubernamentales competentes.

En la evaluación deben examinarse todas las posibles amenazas que afectan la protección marítima, entre las que pueden encontrarse los siguientes tipos de sucesos:

1. Daños o destrucción de una IP o de un buque, por ejemplo, mediante artefactos explosivos, incendio provocado, sabotaje o vandalismo;
2. Secuestro o captura de un buque o de las personas a bordo;
3. Manipulación indebida de la carga, del equipo o sistemas esenciales del buque o de las provisiones del buque;
4. Accesos o usos no autorizados, lo que incluye la presencia de polizones;
5. Contrabando de armas o equipos, incluidas las armas de destrucción masiva;
6. Utilización del buque para el transporte de quienes tengan la intención de causar un suceso que afecte a la protección marítima y su equipo;
7. Utilización del propio buque como arma o como medio destructivo o para causar daños;
8. Bloqueo de las entradas al puerto, esclusas, accesos, etc.;
9. Ataque químico, biológico o nuclear;

10. Utilización no autorizada de sistemas tales como: sistemas informáticos, de distribución eléctrica y de comunicaciones;
11. Destrucción de estructuras adyacentes a las instalaciones; y
12. Desordenes por paralizaciones y huelgas.

7.4.6. Identificación, selección y clasificación por orden de prioridad de las medidas correctivas y de los cambios en los procedimientos y su eficacia para reducir la vulnerabilidad

La identificación de las medidas correctivas y el establecimiento de un orden de prioridad para las mismas, tienen por objeto garantizar que se utilizan las más eficaces para reducir la vulnerabilidad de la IP o de la interfaz buque-puerto, ante las posibles amenazas.

Las medidas de protección deben elegirse en función de factores, tales como, su eficacia para reducir la probabilidad de que se produzca un ataque, y deben evaluarse basándose, entre otros, en los datos de :

1. Los reconocimientos, inspecciones y auditorias de protección;
2. Las consultas con los administradores de la instalación portuaria y, si procede, de las estructuras adyacentes;
3. Los antecedentes existentes de sucesos que hayan afectado a la protección marítima;
4. Las operaciones que se realicen en la instalación portuaria.

7.4.7. Identificación de los puntos vulnerables

En la identificación de los puntos vulnerables se deben tener en cuenta los siguientes aspectos:

1. Accesos por mar y tierra a la instalación portuaria y a los buques que estén atracados en ella;
2. Integridad estructural de los muelles, las instalaciones y las estructuras conexas;
3. Procedimientos y medidas de protección existentes, incluidos los sistemas de identificación;
4. Procedimientos y medidas de protección existentes relativos a la infraestructura y los servicios portuarios;
5. Medidas para proteger el equipo radioeléctrico y de telecomunicaciones, la infraestructura y los servicios portuarios, incluidos los sistemas y redes informáticas;
6. Zonas adyacentes que puedan utilizarse durante un ataque o para lanzarlo;

7. Acuerdos existentes con compañías privadas de seguridad que ofrezcan servicios de protección marítima en tierra y en las aguas del puerto; incluyendo también, el área marítima dada en concesión por la Administración Marítima de Costa Rica;
8. Incompatibilidades entre los procedimientos y medidas de seguridad y los de protección;
9. Incompatibilidades entre las tareas asignadas en la instalación portuaria y las tareas de protección;
10. Limitaciones de personal o de ejecución;
11. Deficiencias detectadas al impartir la formación o durante los ejercicios; y
12. Deficiencias detectadas durante las operaciones diarias, después de un suceso o alerta, indicados en los informes sobre aspectos de protección preocupantes, al ejercer las medidas de control, al realizar una auditoría, etc.;
13. Anillos de protección;
14. Blancos potenciales.

7.4.8. Confección de tablas de análisis de riesgos

Con la información de los antecedentes anteriores y de acuerdo a las indicaciones que se sugieren en la sección 6.5 "*Guía para el análisis de riesgos en la evaluación de la protección en una instalación portuaria"*, se deben confeccionar las siguientes tablas:

Tabla 1.- Lista de escenarios posibles.
Tabla 2.- Nivel de consecuencias.
Tabla 3.- Puntuación de vulnerabilidad.
Tabla 4.- Matriz de vulnerabilidad y consecuencias.
Tabla 5.- Determinación de mitigación.
Tabla 6.- Implementación de mitigación.
Tabla 7.- Determinación de mitigación.
Tabla 8.- Implementación de mitigación.

7.4.9. Antecedentes que acompañan la evaluación:

Identificación del evaluador

Nombre:……...
No. de Identificación……
Cargo:.....
Empresa:.....

No. de Cédula Jurídica…….
Fecha Evaluación:.....
Firma Oficial de Protección Portuaria:.....
Visto bueno Gerente Instalación Portuaria.

7.4.10. Anexos de la EPIP

A. Estadísticas Marítimas Portuarias

- Información obtenida de los Operadores Portuarios (Se debe presentar todo lo relacionado con movimientos de naves, movimientos de cargas y otras series de información del ámbito marítimo).

B. Antecedentes y Estatus de Sucesos (Globales, Regionales y Locales)

- Antecedentes de situaciones delictivas en el último año. Se debe considerar la situación y efecto de la entidad en el entorno. Esto quiere decir, la situación delictiva propicia del escenario portuario como son: narcotráfico, contrabando, robos, polizones, acciones terroristas, daños a las personas, infraestructura y al medio ambiente.

- Cualquier otra información como soporte para la evaluación de protección.

C. Metodología de Verificaciones de Protección Portuaria

Son las metodologías establecidas para facilitar el reconocimiento y/estatus de la seguridad, protección y el grado de implementación de sistemas de protección en las instalaciones portuarias.

D. Tablas y Formularios de Análisis de Riesgo

- Son las metodologías establecidas para desarrollar los cálculos de la probabilidad de que las amenazas se materialicen, a fin de establecer medidas de protección y el orden de prioridad de las mismas.

E. Croquis/Mapas

- Es la inclusión de mapas, planos, esquemas u otra ayuda que identifique claramente la instalación portuaria.

F. Fotos

- Son el complemento de la Evaluación de Protección.

7.5. Guía para el análisis de riesgos en la evaluación de la protección en una instalación portuaria

La presente guía es un extracto de la publicación *Navigation and Vessel Inspection Circular N° 11-02 (NVIC 11-02)* del 13 de enero 2003 del Servicio de Guardacostas de los Estados Unidos de Norte América.

La Toma de Decisiones Basada en el Riesgo (RBDM) es una de las mejores herramientas para desarrollar y determinar las medidas apropiadas de seguridad para una instalación portuaria.

La RBDM es un proceso sistemático y analítico utilizado para considerar la probabilidad de que una violación de la seguridad ponga en peligro un activo, individuo o función e identificar las acciones que reducirán la vulnerabilidad y mitigarán las consecuencias.

Una evaluación de seguridad es un proceso que identifica las debilidades en estructuras fijas, sistemas de protección personal, procesos u otras áreas que puedan conducir a una violación de seguridad y puede sugerir opciones para eliminar o mitigar esas debilidades.

Estas evaluaciones pueden identificar vulnerabilidades en las operaciones de una Instalación, seguridad del personal y seguridad física y técnica.

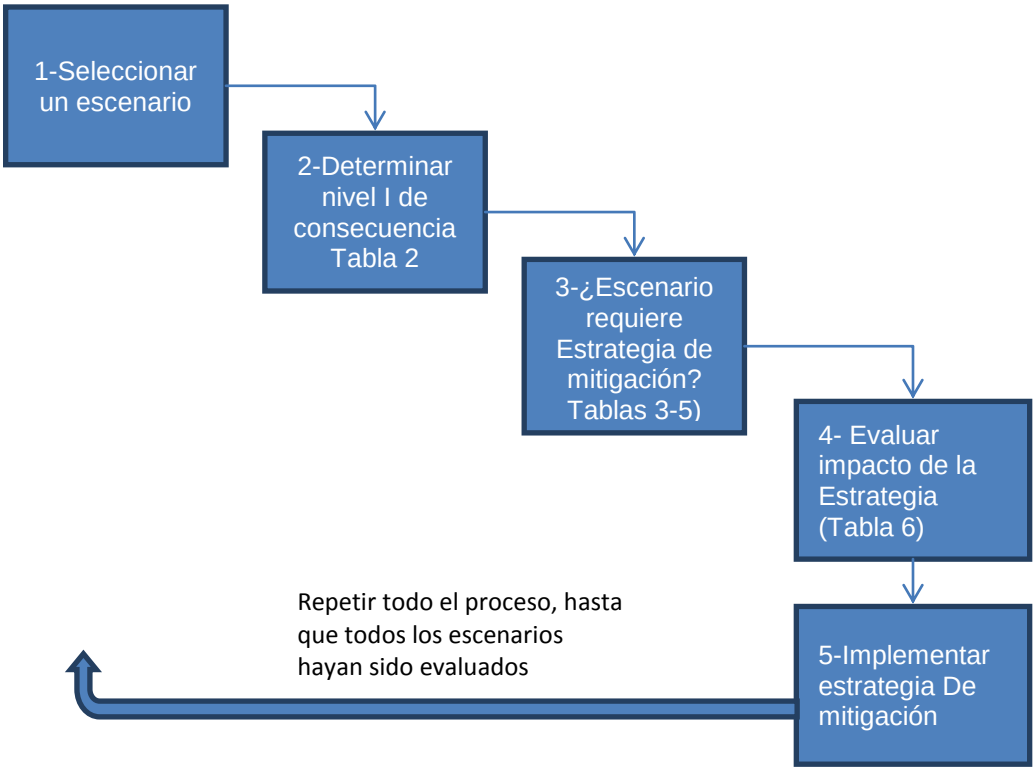
Por ejemplo, una evaluación de seguridad podría revelar fallas en los sistemas de seguridad de una organización, puntos de acceso desprotegidos, como el perímetro de una instalación no iluminada o puertas no aseguradas o no monitoreadas durante horas.

Para mitigar la vulnerabilidad, una instalación deberá implementar procedimientos para asegurar los accesos o disponer que sean verificados por alguien. Otra medida para mejorar la protección puede ser colocar mecanismos de cierre y/o mallas de alambre en puertas y ventanas que proveen acceso a áreas restringidas con el fin de prevenir el acceso de personal no autorizado a esas áreas.

El proceso y sus resultados, deben ser documentados cuando se prepare la evaluación.

El siguiente es un ejemplo de evaluación simplificada de protección basada en el riesgo, la cual puede ser afinada y adaptada a instalaciones portuarias específicas.

Diagrama de Flujo de una Evaluación de Seguridad Basada en Riesgo



7.5.1. Paso 1 – Amenazas Potenciales

Para comenzar una evaluación se necesita considerar escenario(s) de ataque que consiste(n) en una amenaza potencial bajo circunstancias específicas.

Es importante que el o los escenarios desarrollados estén dentro del ámbito de posibilidades y como mínimo, consideren las capacidades e intenciones conocidas de acuerdo a las evidencias de eventos pasados y la inteligencia disponible. Estos deben ser también consistentes con los escenarios usados para desarrollar el plan de Protección de la instalación portuaria.

La Tabla No. 1 muestra una lista de escenarios posibles, los que pueden ser combinados con objetivos críticos específicos para ser desarrollados y evaluados en el proceso de análisis de protección portuaria. Por ejemplo, una amenaza de bomba a una instalación petroquímica es un escenario posible.

Tabla No.1

LISTA DE ESCENARIOS POSIBLES		
Escenario típico		**Ejemplos de Aplicación**
Introducir y/o tomar control del objetivo y…	Dañar /destruir el objetivo con explosivos	Intruso instala explosivos
	Dañar/ destruir el objetivo por actos maliciosos.	El intruso toma el control de una nave y la vara o colisiona intencionalmente con algo. Abre válvulas para vaciar combustible que puede ser encendido
	Crea un incidente peligroso sin destruir el blanco Toma rehenes / mata	Abre válvulas para derramar materiales tóxicos, o los ha traído consigo. Meta del intruso es matar gente
Atacar externamente a la Instalación por medio de....	• Lanzamiento de armas desde alguna distancia. • Colocar explosivos adyacentes al objetivo: - Desde el agua - Desde el muelle - Desde el fondo	Disparar al blanco usando rifle, misil, para dañar o destruir estanques, carga peligrosa. Auto o camión bomba
Usar la Instalación como un medio de transferir	Materiales, droga/ dinero Como un medio contrabando hacia o desde el país. Personas desde y hacia el país.	Instalación es usada como un vehículo para crear incidentes de seguridad durante el transporte.

El número de escenarios se deja a juicio del equipo evaluador. Una evaluación inicial completa debe al menos considerar los escenarios expuestos en la Tabla No. 1. Debe tenerse en cuenta el debido cuidado de evitar un número excesivo de evaluaciones innecesarias sobre escenarios que sean de baja consecuencias. Por esta razón la evaluación de la criticidad debería ser realizada inicialmente para apuntar los esfuerzos sobre objetivos críticos. Las variaciones menores en escenarios similares no necesitan ser evaluados separadamente a no ser que haya diferencias sustanciales en las consecuencias o las vulnerabilidades.

7.5.2. Paso 2 – Estimación de Consecuencias

En este paso se debe determinar el Nivel de Consecuencia apropiado para la Instalación (3, 2, 1), determinado de la Tabla No. 2.

El nivel de apropiado de Consecuencia debe estar basado en la "descripción" de la Instalación (Ej. Si transfiere, almacena o de alguna manera contiene "ciertos cargamentos peligrosos", tendrá un Nivel de Consecuencia 3).

Tabla No. 2

NIVEL DE CONSECUENCIAS	
Nivel de Consecuencia	**Descripción**
3	Instalaciones que transfieren, almacenan o manipulan "cargamentos peligrosos".
2	Instalaciones que: 1) Reciben buques certificados para transporte de pasajeros, o 2) Reciben buques en viajes internacionales.
1	Instalaciones que no son las arriba indicadas.

7.5.3. Paso 3 – Estimación de Vulnerabilidad

Cada escenario debiera ser evaluado en términos de la vulnerabilidad de la Instalación a un ataque. Los cuatro elementos de vulnerabilidad que deberán ser considerados son:

1. **Disponibilidad**: Presencia de la Instalación y la predicción de cómo se relaciona con la capacidad de planificar un ataque.
2. **Accesibilidad**: Facilidad que tiene la Instalación al escenario de ataque. Esto se relaciona con las barreras físicas y geográficas que disuaden la amenaza sin seguridad/ protección orgánica.
3. **Seguridad Orgánica**: La habilidad del personal de seguridad de disuadir un ataque. Esto incluye los Planes de Seguridad/ Protección, las capacidades de comunicación, la fuerza de vigilancia, los sistemas de detección de intrusos y la oportunidad con que las fuerzas externas pueden prevenir un ataque.
4. **Dificultad del Objetivo**: Es la capacidad que tiene la Instalación de resistir el ataque específico, basado en la complejidad del diseño de la instalación y las características del material de construcción.

El equipo evaluador o el OPIP, deberá analizar cada elemento de vulnerabilidad para un escenario dado. La evaluación inicial de la vulnerabilidad debería ser vista sin nuevas estrategias que signifiquen una disminución de las vulnerabilidades, aún si hay estrategias y medidas de seguridad ya adoptadas.

La evaluación de la vulnerabilidad sin estrategias proporcionará una ponderación base más acuciosa para el riesgo general asociado con el escenario. Después que la evaluación inicial ha sido llevada a cabo, una evaluación de comparación puede ser hecha con las nuevas estrategias y medidas de protección consideradas, generando un mejor entendimiento del riesgo general asociado con el escenario y como las nuevas estrategias y medidas de seguridad mitigarán el riesgo.

En el entendido de que la instalación portuaria tiene mayor control sobre la accesibilidad y la seguridad orgánica, esta herramienta solo toma en consideración estos elementos (No considerando disponibilidad ni dificultad del objetivo) en la evaluación de cada escenario. El puntaje y criterio de vulnerabilidad y ejemplos de referencia son descritos en la Tabla No. 3. Cada escenario debe ser evaluado para obtener un puntaje de accesibilidad y de seguridad orgánica. De la suma de estos elementos, se obtendrá el puntaje total de vulnerabilidad (paso 3 de la Tabla No. 5). Este puntaje deberá ser usado como puntaje de vulnerabilidad cuando se evalúe cada escenario en el próximo paso.

Tabla No.3

PUNTUACIÓN DE VULNERABILIDAD		
Puntaje	**Accesibilidad**	**Seguridad Orgánica**
3	Sin disuasión (es decir, acceso irrestricto a la Instalación y movimiento interno irrestricto)**.**	Sin capacidad de disuasión (es decir, sin planes, sin fuerza de vigilancia, sin comunicaciones de emergencia, sin capacidad de detección, fuerza policial no está disponible oportunamente).
2	Disuasión regular (barrera sustancial, simple; acceso no restringido hasta 100 metros de los objetivos).	Capacidad de disuasión regular (plan de seguridad mínimo, algunas comunicaciones, fuerza de seguridad de tamaño limitado, fuerza externa con limitada disponibilidad para prevenir, sistemas limitados de detección.
1	Buena disuasión (se espera disuada el ataque); acceso restringido hasta 500 metros de los objetivos barreras geográficas y/o físicas múltiples.	Buena capacidad de disuasión (se espera que disuada el ataque) plan detallado de seguridad, comunicaciones efectivas de emergencia, equipo de personal de seguridad bien entrenado, sistema de detección múltiple (Rayos X, cámaras, etc.) Fuerza externa para prevenir oportunamente.

7.5.4. Paso 4 – Mitigación

A continuación se debe determinar qué escenarios requieren de una estrategia de mitigación. Esto se logra determinando dónde se posiciona el escenario en la Tabla No. 4, basado en el Nivel de Consecuencia y Puntuación de Vulnerabilidad. La Tabla No. 4 es una herramienta relativa y amplia para ayudar en el desarrollo del Plan de Seguridad /Protección.

Mitigar: significa que se deben desarrollar estrategias de atenuación, tales como medidas protectoras de seguridad, para reducir el riesgo del escenario. Un Apéndice del Plan de Seguridad /Protección debe contener los escenarios evaluados, el resultado de la evaluación y las medidas de mitigación elegidas.

Considerar: significa que se deben desarrollar estrategias de mitigación, en una base caso a caso. El Plan de Seguridad/ Protección debe contener los escenarios evaluados, el resultado de la evaluación y las razones por las cuales las medidas de mitigación fueron o no elegidas.

Documentar: significa que el escenario puede no necesitar una medida de mitigación y por lo tanto sólo necesita ser documentado. Sin embargo, las medidas que tengan un bajo costo pueden ser consideradas. El Plan de Seguridad/Protección debe contener los escenarios evaluados y los resultados de la evaluación.

Tabla No. 4

MATRIZ DE VULNERABILIDAD Y CONSECUENCIA VULNERABILIDAD TOTAL Y LA CATEGORÍA DE MITIGACIÓN				
		Puntuación Total de Vulnerabilidad (Tabla 3)		
		2	3-4	5-6
Nivel de Consecuencia (Tabla No.2)	3	Considerar	Mitigar	Mitigar
	2	Documentar	Considerar	Mitigar
	1	Documentar	Documentar	Considerar

7.5.5. Paso 5 – Métodos de Implementación

Para determinar qué escenarios requieren medidas de mitigación, puede ser útil usar la Tabla No. 5. La instalación portuaria, puede registrar los escenarios considerados, el nivel de consecuencias (Tabla No. 2), el puntaje de vulnerabilidad de cada elemento (Tabla No.3), el puntaje total de vulnerabilidad y la categoría de mitigación (Tabla No. 4). El efecto deseado es reducir el riesgo asociado con las combinaciones objetivo/escenario que han sido identificadas en el proceso. Es necesario tener presente que, al momento de la consideración de las estrategias de mitigación, a menudo es más fácil reducir las vulnerabilidades que las consecuencias o amenazas.

El evaluador deberá tener presente que las estrategias de mitigación deben ser puestas en vigor en formas proporcional con los diferentes niveles de protección y a través de la autoridad apropiada. Las estrategias de mitigación efectivas y que son posibles de adoptar deberían ser consideradas para su utilización en el nivel de protección más bajo (Nivel 1). Las estrategias efectivas pero parcialmente posibles de implementar deberían ser consideradas en niveles de protección 2 y 3.

Las estrategias deben finamente mantener permanentemente un nivel de protección equivalente a pesar de los cambios en los niveles de amenaza.

Tabla No.5

HOJA DE TRABAJO PARA LA DETERMINACIÓN DE LA MITIGACIÓN					
Paso1	**Paso 2**	**Paso 3**			**Paso 4**
Descripción/ Escenario	Nivel de Consecuencia (Tabla No.. 2)	**Puntaje de Vulnerabilidad (Tabla No. 3)**			Mitigar, Considerar, o Documentar (Tabla No. 4)
		Accesibilidad +	Orgánica =	Puntaje Seguridad Total	
	Una vez que la Instalación ha sido categorizada el Nivel de Consecuencia Permanece igual				

Para ayudar a evaluar estrategias de mitigación específicas (Medidas de Protección) puede ser útil el uso de la Tabla No.6

Tabla No. 6

HOJA DE TRABAJO DE IMPLEMENTACIÓN DE MITIGACIÓN						
1	**2**	**3**	**4**			**5**
Estrategia de Mitigación (Medidas de Protección)	Escenarios que son Afectados por la Estrategia de Mitigación (De paso 1 Tabla No. 5)	Nivel de Consecuencia (Tabla No. 2)	**Puntaje de Vulnerabilidad (Tabla 3)**			Nuevos Resultados de Mitigación (Tabla No. 4)
			Accesibilidad +	Orgánica =	Puntaje Seguridad Total	
1.	1.					
	2.					
	3.					
2.	1.					
	2.					
	3.					

Los pasos siguientes corresponden a cada columna de la Tabla No. 6.

1.- Para aquellos escenarios señalados como **considerar** o **mitigar**, se deben idear estrategias de mitigación (Medidas de Protección) y registrarlas en la primera columna de la tabla No. 6.
2.- Usando el escenario (s) de la tabla No. 5, hacer un listado de todos los escenarios que serán afectados por la estrategia de mitigación seleccionada.
3.- El nivel de consecuencia permanece igual que el determinado en la tabla No. 2 para cada escenario.
4.- Reevaluar los puntajes de accesibilidad y seguridad orgánica (Tabla No. 3) para ver si las nuevas estrategias de mitigación reducen el puntaje de vulnerabilidad total para cada escenario.
5.- Con el nivel de consecuencias y el nuevo puntaje de vulnerabilidad total, use la tabla 4 para determinar las nuevas categorías de mitigación.

7.5.6. Implementación de Mitigación

Una estrategia se considera efectiva si su implementación baja la categoría de mitigación (Ej. de mitigar a considerar). Se considera parcialmente efectiva si al implementarla por si sola o junta a otra(s), se baja la puntuación de vulnerabilidad.

Por ejemplo en una Instalación con Nivel de Consecuencia 2, una estrategia de mitigación baja la vulnerabilidad de “5-6” a “3-4”, la categoría de mitigación baja de mitigar a considerar, se considera que la estrategia es efectiva.

Para una Instalación con un Nivel de Consecuencia 3 y una estrategia de mitigación baja la vulnerabilidad de “5-6” a “3-4”, la categoría de mitigación permanece igual, **mitigar**, y la estrategia es parcialmente efectiva.

Si una estrategia de mitigación, considerada individualmente, no reduce la vulnerabilidad, se pueden considerar estrategias múltiples en combinación.

Al considerar las estrategias como un todo, se debería bajar la vulnerabilidad a un Nivel aceptable.

Una estrategia se considera factible si puede ser implementada con poco impacto operacional o de fondos en relación con la disminución de la vulnerabilidad esperada. Será parcialmente factible si requiere de cambios o costos significativos en relación a la reducción de vulnerabilidad prevista. Será no factible si su implementación es extremadamente problemática o su costo prohibitivo.

La factibilidad de una estrategia de mitigación puede variar en base al Nivel de Protección, por lo tanto algunas estrategias no pueden ser garantizadas en el Nivel de protección 1 pero si pueden serlo en los Niveles de Protección 2 y 3.

Las estrategias de mitigación deben asegurar en general, que el nivel de riesgo de una instalación permanezca constante en relación con el incremento de la amenaza.

Las tablas Nos. 7 y 8, dan un ejemplo abreviado de cómo las tablas 5 y 6, pueden completarse para una instalación que recibe buques de pasaje y recibe buques en viajes internacionales. Este ejemplo asume que la instalación portuaria tiene una buena capacidad de disuasión con su seguridad orgánica sin embargo no tiene una defensa perimetral para restringir los accesos a la instalación

Tabla No. 7

EJEMPLO DE HOJA DE TRABAJO DE DETERMINACIÓN DE MITIGACIÓN					
Paso1	**Paso 2**	**Paso 3**			**Paso 4**
Descripción/ Escenario	Nivel de Consecuencia (tabla No. 2)	**Puntaje de Vulnerabilidad (Tabla No.3)**			Mitigar, Considerar, o Documentar (tabla No.4)
		Accesibilidad +	Orgánica =	Puntaje Seguridad Total	
1. Logra entrada no autorizada a Instalación.	2	3	2	5	Mitigar
2. Ataque externo a Instalación con Arma de Fuego.		3	2	5	Mitigar
3. Usa la instalación como un medio para transferir gente desde un buque a un vehículo para ingreso ilegal al país.		3	2	5	Mitigar

Tabla No. 8

EJEMPLO HOJA DE TRABAJO DE IMPLEMENTACIÓN DE MITIGACIÓN				
1	**2**	**3**	**4**	**5**
Estrategia	Escenarios que Son	Nivel de	**Puntaje de Vulnerabilidad (Tabla 3)**	Nuevos

de Mitigación (Medidas de Protección)	Afectados por la Estrategia de Mitigación (Tomado de paso 1 tabla No. 5)	Consecuencia (Tabla 2)	Accesibilidad +	Orgánica =	Puntaje Seguridad Total	Resultados de Mitigación (tabla 4)
1. Cerco perimetral que restringe acceso a la Instalación	**1**.Intruso ingresa a la Instalación.	2	2	2	4	Considerar
	2. Uso de la Instalación como un medio para transferir gente desde un buque a vehículo para ingreso ilegal		2	2	4	Considerar

8. GUIA PARA EL DESARROLLO DEL PLAN DE PROTECCIÓN DE LAS INSTALACIONES PORTUARIAS (PPIP)

Cada Instalación Portuaria elaborará un plan de protección de la instalación portuaria adecuado para la interfaz buque-puerto, basándose en la evaluación de la protección de la instalación portuaria, Dicho plan de protección estará redactado en idioma español, estará basado en procedimientos detallados que claramente definan las actividades de preparación, prevención y respuesta que tendrán lugar en cada nivel de amenaza, a cumplir por la organización o el personal que será responsable de llevar a cabo esas actividades.

El plan contemplará los tres niveles de protección que se definen en la Parte A del Código PBIP y podrá ser confeccionado por una organización de protección reconocida (OPR), considerando los conceptos y las orientaciones de la Parte B del Código de Protección de los Buques y las Instalaciones Portuarias (PBIP). Dicho plan debe referirse como mínimo a los siguientes puntos:

1. Acceso a la instalación portuaria;
2. Zonas restringidas dentro de la instalación portuaria;
3. Manipulación de la carga;
4. Entrega de las provisiones del buque;
5. Gestión de equipajes no acompañados;
6. Vigilancia de la protección de la instalación portuaria.

El Plan de Protección de la Instalación Portuaria (PPIP) y sus enmiendas deberá ser aprobado por la Dirección de Navegación y Seguridad del Ministerio de Obras Públicas y Transportes, para lo que considerará como requisito mínimo lo siguiente:

1. Las medidas previstas para evitar que se introduzcan a bordo de un buque o en la instalación portuaria armas, sustancias e instrumentos que puedan ser utilizados contra personas, bienes, buques o puertos cuyo transporte no esté autorizado;
2. Las medidas destinadas a evitar el acceso no autorizado a la instalación portuaria, a los buques fondeados, buques atracados y a las zonas restringidas de la instalación portuaria;
3. Los Procedimientos para dar respuesta a las amenazas para la protección a un fallo de las medidas de protección, incluidas las disposiciones para mantener el funcionamiento esencial de la instalación portuaria o de la interfaz buque-puerto;
4. Los procedimientos para dar respuesta a toda instrucción de protección que pueda dar la Dirección de Navegación y Seguridad (DNS) u otro organismo de seguridad competente, en el nivel de protección 3;
5. Los procedimientos para la evacuación en caso de amenaza para la protección o de fallo de las medidas de protección;

6. Las tareas de protección asignadas al personal de la instalación portuaria y además otro personal de la instalación portuaria con responsabilidades en materia de protección;
7. Los procedimientos relativos a la interfaz con las actividades de protección del buque;
8. Los procedimientos para la revisión periódica del Plan y su actualización;
9. Los procedimientos para notificar sucesos relativos a la protección marítima;
10. La identificación del Oficial de Protección de la Instalación Portuaria, con sus datos de contacto para las 24 horas del día;
11. Las medidas para garantizar la protección de la información que figura en el Plan;
12. Las medidas para garantizar la protección eficaz de la carga y del equipo para la manipulación de la carga en la instalación portuaria;
13. Los procedimientos para verificar periódicamente la eficacia del Plan de Protección de la Instalación Portuaria, en todo momento;
14. Los procedimientos para dar respuesta cuando se haya activado el sistema de alerta de protección del buque en la instalación portuaria;
15. Los procedimientos para facilitar el permiso de tierra del personal del buque o los cambios de personal, así como, el acceso de los visitantes al buque, incluidos los representantes de las organizaciones para el bienestar de la gente de mar y de los sindicatos;
16. Indicación del personal que realiza las auditorías internas de las actividades de protección especificadas en el Plan o que evalúa su implantación, será independiente de las actividades objeto de verificación, a menos que esto no sea factible por el tamaño y la naturaleza de la instalación portuaria;
17. El plan de protección de la instalación portuaria podrá combinarse con el plan de protección del puerto o cualquier otro plan del puerto para situaciones de emergencias, o formar parte de ellos;
18. La Dirección de Navegación y Seguridad (DNS) determinará qué cambios del plan de protección de la instalación portuaria no se implantarán sin que esta haya aprobado las correspondientes enmiendas a ese plan;
19. La Dirección de Navegación y Seguridad podrá autorizar que el plan de protección de una instalación portuaria abarque más de una instalación portuaria cuando el explotador, la ubicación, el funcionamiento, el equipo y el proyecto de tales instalaciones sean semejantes;
20. El plan podrá mantenerse en formato electrónico. En tal caso estará protegido mediante procedimientos destinados a evitar que se borre, destruya o altere sin autorización;
21. El plan se protegerá contra el acceso o divulgación no autorizados;
22. Una copia del plan impresa (física) será depositada en la DNS;
23. Otros que se estimen oportunos.

8.1. Orientaciones sobre la preparación y contenido del plan de protección

La preparación del Plan de Protección de la Instalación Portuaria (PPIP) es responsabilidad del OPIP. Aunque no es necesario que el OPIP lleve a cabo

personalmente todas las tareas que corresponden a ese puesto, siempre será él personalmente responsable de asegurarse de que se realiza adecuadamente.

El contenido de cada PPIP variará en función de las circunstancias especiales de la instalación o instalaciones portuarias a que se aplique. Al preparar el PPIP, es preciso tener en cuenta estas características y otras consideraciones de protección locales o nacionales, a fin de tomar las medidas de protección necesarias para minimizar el riesgo de un fallo de protección y las consecuencias de materialización de los posibles riesgos.

En la evaluación de la protección de la instalación portuaria se deben identificar las características especiales de la instalación portuaria y las posibles amenazas que han llevado a la necesidad de nombrar un OPIP y preparar un PPIP.

Todo Plan de Protección de Instalaciones Portuarias (PPIP) debe contener:

1. La explicación detallada de la organización de la Protección de la Instalación Portuaria;
2. Indicación detallada de los enlaces de la organización con otras autoridades competentes y la configuración de los sistemas de comunicación necesarios para el funcionamiento eficaz en todo momento de la organización y de sus enlaces con otras entidades, incluidos los buques que se hallen en el puerto;
3. Indicación detallada de las medidas básicas de protección, de carácter tanto operacional como físico, que se han adoptado para el nivel de protección 1;
4. Indicación detallada de las medidas adicionales que harán posible que la instalación portuaria pase sin demora al nivel de protección 2 y, si es necesario, al nivel de protección 3;
5. Indicación del control y la revisión periódica del PPIP, y su posible enmienda en consonancia con la experiencia adquirida o en respuesta a un cambio de circunstancias;
6. Explicación detallada de los procedimientos de notificación a los pertinentes puntos de contactos (la DNS y otras autoridades u organismos públicos y privados con responsabilidad en el ámbito de protección).

8.2. Organización y realización de las tareas de protección de la instalación portuaria

Además de las orientaciones y los conceptos para la preparación y contenido de un PPIP, este debe incluir los siguientes elementos para todos los niveles de protección:

1. La función y la estructura de la organización de la protección de la instalación portuaria;
2. Las funciones, responsabilidades y requisitos de formación de todo el personal de la instalación portuaria que tenga funciones de protección marítima y las medidas de control del rendimiento necesarias para evaluar la eficacia de cada persona;

3. Definir los enlaces, lista de contactos y coordinaciones de la organización de Protección de la Instalación Portuaria con la DNS y otras autoridades u organismos públicos y privados con responsabilidad en el ámbito de protección;
4. Los sistemas de comunicaciones de los que se dispone para mantener comunicaciones continuas y eficaces en todo momento entre el personal de Protección de la Instalación Portuaria, los buques que se hallen en el puerto y, si es necesario con las autoridades nacionales y locales con responsabilidades en las tareas de la protección;
5. Los procedimientos con:
    5.1. Las medidas de precaución necesarios para que estas comunicaciones continuas estén garantizadas en todo momento.
    5.2. Las prácticas para salvaguardar la información confidencial sobre protección disponible en papel o en formato electrónico.
    5.3. Lo necesario para evaluar la eficacia en todo momento de los procedimientos y el equipo de protección, entre los que se incluyen los procedimientos para identificar y subsanar un fallo o un funcionamiento defectuoso del equipo.
    5.4. Los criterios para presentar y evaluar informes relativos a posibles transgresiones o aspectos de protección preocupantes.
    5.5. Concernientes a la manipulación de la carga.
    5.6. Concernientes a los proveedores y servicios destinados a los buque.
    5.7. Los procedimientos para elaborar, mantener y actualizar un inventario de mercancías peligrosas o sustancias potencialmente peligrosas, si las hay, especificando su ubicación en la IP.
    5.8. Los medios para poner sobre aviso y obtener los servicios del Servicio Nacional de Guardacostas y equipos de búsqueda especializados, incluidos los expertos en búsqueda de bombas, búsquedas submarinas y obtener sus servicios.
    5.9. Los procedimientos para ayudar a los oficiales de protección del buque a confirmar la identidad de las personas que deseen subir a bordo, cuando se solicite.
    5.10. Los procedimientos para facilitar permisos en tierra al personal del buque o con objeto de efectuar cambios del personal, así como el acceso de visitantes al buque, incluidos los representantes de autoridades gubernamentales (Ministerio de Trabajo, Ministerio Salud u otros) relacionados con el bienestar de las gentes de mar.
    5.11. Los procedimientos para registro y documentación relativos a la protección.
    5.12. Los Procedimientos para la realización de prácticas, ejercicios y Auditorías internas de protección.
    5.13. Todos aquellos que se estimen pertinentes.

8.3. Formato para la presentación del plan de protección de una instalación portuaria (aspectos a considerar)

8.3.1. Conformación del PPIP

Los PPIP seguirán en general las pautas indicadas, en las que se han incluido los elementos indispensables que deberá contener el mismo y que se detalla a continuación:

Tipo de letra:
Se utiliza letra Arial o Times New Román tamaño 11.

Carátula:
La información mínima que deberá contener será el nombre de la instalación portuaria y su Administrador o Concesionario, información de revisión y aprobación del plan (ver Figura 1).

Carpeta:
Tamaño: A4, de dos anillas, tapa dura, etiqueta autoadhesiva en el lomo donde conste Nº de Declaración de Cumplimiento, Nombre de la IP y puerto.

En la tapa:
Etiqueta autoadhesiva de tamaño 210 mm x 148.5mm donde figurará: nombre de la IP, Nº de Declaración de Cumplimiento, puerto, OPIP/s con datos para su localización durante las 24 horas (celular, nextel, etc.).

Tamaño papel:
A4

Configuración de la página:
Margen izquierdo: 2,5 cm
Margen derecho: 0,5 cm
Margen superior: 2,5 cm
Margen inferior: 2,0 cm

Ordenamiento del plan:
Los capítulos que lo conforman irán identificados con separadores con orejetas en el margen derecho que permita su identificación y localización de manera ágil. No así los subíndices que los conformen.

8.3.2. Contenido

8.3.2.1. Carátula Principal/ Revisión y Aprobación del Plan de Protección de la Instalación Portuaria

Logo de la IP	PLAN DE PROTECCIÓN DE LA INSTALACIÓN PORTUARIA (Nombre de la IP)	Edición	Modificación	
		00/00/00	00/00/00	
		Versión	Control	
		00	DNS / IP	

PLAN DE PROTECCIÓN
DE LA INSTALACIÓN PORTUARIA (PPIP)[2]

(Nombre de la Instalación Portuaria)

Ejemplar No: ____

Instalación Portuaria	
Responsable en la elaboración del Plan de Protección: Nombre:_____ Fecha: _____ Firma: _____	Revisado por el Gerente General de la Instalación Portuaria: Nombre:_____ Fecha: _____ Firma: _____
División Marítima Portuaria - Dirección de Navegación y Seguridad	
Aprobado por el Director DNS Nombre:_____ Fecha:_____ Firma: _____	VB°. Director División Marítimo Portuaria Nombre:_____ Fecha: _____ Firma: _____

[2] Documento Confidencial/ Secreto, Control DNS/ OPIP. Queda prohibido difundir o reproducir total o parcialmente, sin la debida autorización de la Dirección de Navegación y Seguridad.

8.3.2.2. Índice General del PPIP

El índice debe contener todas aquellas referencias necesarias para la ubicación pronta de los principales aspectos del Plan de Protección.

8.3.2.3. Record de distribución y control del Plan de Protección de la Instalación Portuaria.

Control de Ejemplares de los Planes de Protección:

[Estampar una breve descripción textual de la responsabilidad, edición, distribución y mantenimiento del plan, cuantos ejemplares hay, quienes tiene acceso, bajo llave][3].

Se debe Garantizar la protección de la información confidencial contenida en el plan, ya sea en papel o formato electrónico. El plan podrá mantenerse en formato electrónico; en tal caso estará protegido mediante procedimientos destinados a evitar que se borre, destruya o altere sin autorización. Al mismo tiempo, se protegerá contra acceso o divulgaciones no autorizadas.

[Detallar el personal autorizado para la manipulación del PPIP físico y digital, medidas a seguir para garantizar la confidencialidad de la información y como se salvaguarda el resto de la documentación de protección].

[Añadir información según criterio del Oficial de Protección]

[Crear una tabla con la identificación de la distribución de ejemplares del plan de protección aprobado por la Dirección de Navegación y Seguridad]

IDENTIFICACIÓN DE LA DISTRIBUCIÓN DE EJEMPLARES			
No. Ejemplar	**Responsable**	**Ubicación**	**Firma**
	(Nombre y Cargo)	(Lugar especifico)	

[3] En adelante lo indicado en corchetes ([ ]) y en cursiva se refiere a instrucciones que se dan a quien elaborará el PPIP a fin de que se especifique o desarrolle lo que se le solicita.

8.3.2.4. Documento de Control para las revisiones, correcciones y cambios en el Plan de Protección.

Se incorporará el siguiente cuadro de control.

CONTROL DE REVISIONES, CORRECCIONES Y CAMBIOS EN EL PLAN DE PROTECCIÓN					
No.	**Fecha**	**Ref. PPIP**	**Cambios /Actualización**	**Nombre y Firma del OPIP**	**Revisado y Aprobado por el DMP/DNS Nombre y Firma**
01					
02					
03					
04					
05					

8.3.2.5. Introducción

El plan de protección de la instalación portuaria <*insértese nombre de la instalación portuaria*>, es elaborado y actualizado, con base a la evaluación de protección de la instalación portuaria, adecuado para la interfaz buque-puerto, el cual deberá actuar con arreglo a los niveles de protección y otras medidas establecidas por la Dirección de Navegación y Seguridad. Entre los factores que se tienen en cuenta para establecer el nivel de protección adecuado se encuentran los siguientes:

- En qué medida es creíble la información de la amenaza;
- En qué medida se puede corroborar la información sobre la amenaza;
- En qué medida la información sobre la amenaza es específica o inminente; y
- Las posibles consecuencias del suceso que afecte a la protección marítima.

Las disposiciones específicas contempladas en el plan de protección, propone y contribuye a la prevención de actos ilegales contra la instalación portuaria o algún suceso que pueda afectar a la protección marítima, de modo que se reduzcan al mínimo los inconvenientes o demoras para los pasajeros, los buques, el personal y los visitantes de los buques, las mercancías y los servicios.

El propósito del Plan de Protección de la Instalación Portuaria es el de tomar las medidas de protección necesarias para reducir al mínimo el riesgo de que suceda un fallo de protección y las consecuencias de los posibles riesgos.

[Añadir información adicional: objetivo del plan de protección de acuerdo a la actividad de la Instalación Portuaria]

8.3.2.6. Definiciones

Para la interpretación de los términos que no se encuentran listados aquí, se aplicarán para los fines de este documento, las contenidas en el Capítulo XI-2 del Convenio SOLAS y los acotados en el Código PBIP.

Accesibilidad: Grado de dificultad para acceder a la instalación portuaria. El término se relaciona con las barreras físicas y geográficas que pueden disuadir una amenaza, sin necesidad de protección.

Actividad buque a buque: Toda actividad no relacionada con una instalación portuaria que suponga el traslado de mercancías o personas de un buque a otro.

Amenaza: Posibilidad de que un incidente de protección ocurra.

Código Internacional para la Protección de los Buques y de las Instalaciones Portuarias (Código PBIP): Consiste en una serie de disposiciones atinentes a la protección de los buques y las instalaciones portuarias, adoptado el 12 de diciembre de 2002 mediante la resolución 2 de la Conferencia de los Gobiernos Contratantes del Convenio internacional para la seguridad de la vida humana en el mar, 1974, según sea enmendado por la Organización Marítima Internacional.

Comité de Protección Portuaria (CPP): El Comité está conformado por autoridades de alto mando de jurisdicción, entidades gubernamentales y privadas que están ubicadas en las cercanías del puerto y que de una forma u otra sus funciones están ligadas a la protección nacional y del puerto. En este comité participan DNS, Dirección de Inteligencia y Seguridad (DIS),

Organismos de Investigación Judicial (OIJ), Cruz Roja, Bomberos, Ministerio de Seguridad Pública (MSP), Dirección de Migración y Extranjería, Servicio Nacional de Guardacostas, K9.

Capitanía de Puerto: Oficinas Regionales marítimas a cargo de un capitán de puerto, creada para el desarrollo de las competencias de la DNS.

Declaración de Cumplimiento de la IP (DCIP): Documento expedido por la DNS, mediante el cual avala que una IP cumple satisfactoriamente con lo establecido en el Código PBIP.

Declaración de Protección Marítima (DPM): Acuerdo alcanzado entre un buque y una instalación portuaria u otro buque con el que se realiza operaciones de interfaz, en el que se especifican las medidas de protección que aplicará cada uno.

Dirección de Navegación y Seguridad (DNS): Dirección de la División Marítimo Portuaria del Ministerio de Obras Públicas y Transportes que tiene a cargo la Administración Marítima Nacional y por ende la ejecución de la rectoría en materia marítima. Responsable de la implantación de las disposiciones relativas a la protección de la IP y la interfase buque-puerto.

Equipaje no acompañado: Todo equipaje, incluido los efectos personales, que no esté con el pasajero o el miembro del personal del buque en el lugar de la inspección o registro.

Incidente de protección de la IP: Cualquier circunstancia, activa, pasiva o sospechosa, en la cual elementos humanos intenten o concreten actos ilícitos contra la instalación portuaria, sus facilidades, las cargas, las personas o los buques que operen en ella, o que concreten dichas acciones contra terceros utilizando la instalación o al buque, su carga o su tripulación, como intermediario de estos actos ilícitos. Comprende asimismo la utilización de la instalación portuaria, como objeto o intermediario para llevar a cabo actos de piratería, hurto, terrorismo, contrabando, tráfico de drogas o precursores, tráfico de armas, esclavitud, inmigración ilegal, etc.

Instalación Portuaria (IP): Lugar determinado donde tiene lugar la interfaz buque-puerto. Esta incluirá, según sea necesario, zonas como los fondeaderos, atracaderos de espera y accesos desde el mar.

Interfaz Buque-Puerto: Interacción que tiene lugar cuando un buque se ve afectado directa e inmediatamente por actividades que entrañan el movimiento de personas o mercancías o la provisión de servicios portuarios al buque o desde éste.

Mitigar: Cualquier medida tendiente a reducir el nivel de riesgo. En el proceso de evaluación de protección, significa que necesariamente deben implementarse medidas para reducir el riesgo (mitigación). Estas estrategias pueden incluir medidas y/o procedimientos de protección, a fin de reducir el riesgo para dicho incidente de protección.

Nivel de Protección (NP): Graduación del riesgo de que ocurra o se intente provocar un suceso que afecte a la protección marítima. La Dirección de Navegación y Seguridad determinará los niveles de protección para las instalaciones portuarias e impartirá, según sea necesario, las instrucciones oportunas y facilitará información sobre los aspectos de protección a los buques y las instalaciones portuarias que puedan verse afectados.

Nivel de Protección 1 (NP1): El nivel en el cual deberán mantenerse medidas mínimas adecuadas de protección en todo momento.

Nivel de Protección 2 (NP2): El nivel en el cual deberán mantenerse medidas adecuadas de protección adicionales durante un periodo de tiempo, como resultado de un aumento del riesgo de que ocurra un suceso que afecte a la protección marítima.

Nivel de Protección 3 (NP3): El nivel en el cual deberán mantenerse más medidas concretas de protección durante un periodo de tiempo limitado cuando sea probable o inminente un suceso que afecte a la protección marítima.

Oficial de Protección del Buque (OPB): Persona a borde del buque, responsable ante el capitán, designada por la compañía para responder de la protección del buque, incluidos la implantación y el mantenimiento del PPB, y para la coordinación con el oficial de la compañía para la protección marítima y con los oficiales de protección de las instalaciones portuarias.

Oficial de la Compañía para la Protección Marítima (OCPM): Persona designada por la compañía para asegurar que se lleve a cabo una evaluación sobre la protección del buque y que el plan de protección del buque se desarrolla, se presenta para su aprobación, y posteriormente se implanta y mantiene, y para la coordinación con los oficiales de protección de las instalaciones portuarias y con el oficial de protección del buque.

Oficial de Protección de la Instalación Portuaria (OPIP): Persona designada para asumir la responsabilidad de la elaboración, implantación, revisión y actualización del plan de protección de la instalación portuaria, y

para la coordinación con los oficiales de protección de los buques y con los oficiales de protección de las compañías para la protección marítima.

Plan de Protección del Buque (PPB): Plan elaborado para asegurar la aplicación a bordo del buque de medidas destinadas a proteger a las personas que se encuentren a bordo, la carga, las unidades de transporte, las provisiones de a bordo o el buque de los riesgos de un suceso que afecte a la protección marítima.

Plan de Protección de la Instalación Portuaria (PPIP): plan elaborado para asegurar la aplicación de medidas destinadas a proteger la instalación portuaria y los buques, las personas, la carga, las unidades de transporte y las provisiones de los buques en la instalación portuaria de los riesgos de un suceso que afecte a la protección marítima.

Riesgo: Efecto combinado de la gravedad de un incidente, la amenaza de ocurrencia del mismo y la vulnerabilidad del elemento

Suceso que Afecta a la Protección Marítima: Todo acto o circunstancia que levante sospechas y que constituya una amenaza para la protección de un buque, incluidas las unidades móviles de perforación mar adentro y las naves de gran velocidad, de una instalación portuaria, de una interfaz buque-puerto o de una actividad buque-buque.

Vulnerabilidad: Predisposición o susceptibilidad que tiene un elemento a ser afectado por un incidente de protección. Consta de 4 (cuatro) elementos que se deben considerar y se detallan a continuación:

- **Disponibilidad:** La presencia y predicción en relación a la habilidad de planear un ataque.
- **Accesibilidad:** Facilidad de producir el incidente, en relación a las barreras físicas y geográficas que determinan la amenaza sin seguridad orgánica.
- **Protección orgánica:** La habilidad del personal de seguridad para detener un incidente, esto incluye los planes de seguridad, capacidad de comunicación, guardia, detección de intrusos y tiempo de reacción de las fuerzas externas para prevenir el incidente.
- **Estructura de la instalación**: La capacidad de la instalación de soportar un incidente específico basado en la complejidad del diseño y los materiales de construcción.

[Inclúyase definiciones adicionales]

8.3.2.7. Responsabilidad de la Instalación Portuaria

< Inclúyase nombre de la IP >, siendo una instalación portuaria sujeta a cumplir las prescripciones del Capítulo XI-2 del convenio SOLAS referente al Código PBIP, habrá de disponer de un plan de protección de la instalación portuaria aprobado por la DNS y operar con arreglo a los niveles de protección establecidos.

El OPIP debe implantar las disposiciones del plan y vigilar que éste siga siendo correcto y eficaz en todo momento, ocupándose entre otras cosas, de encargar auditorías internas de la aplicación del plan, adoptar medidas y procedimientos de protección para reducir al mínimo inconvenientes o demora para los pasajeros, los buques, el personal y los visitantes de los buques, las mercancías y los servicios.

[Inclúyase consideraciones adicionales]

8.3.2.7.1. Comité de Protección Portuaria (CPP)

El Comité de Protección Portuaria está conformado por miembros de *(Nombre del Puerto, con alto mando de jurisdicción),* por miembros de entidades gubernamentales y privadas que están ubicadas en las cercanías del puerto (un representante por cada entidad), y que de una forma u otra sus funciones estén ligadas a la protección nacional y del puerto. Por ejemplo: Aduanas, Migración, Salud, Cruz Roja, Bomberos, Servicio Nacional de Guardacostas, Seguridad Pública, Policía de Control de Drogas (PCD), Capitanía de Puerto, entre otras.

- El CPP tiene un objetivo, misión y funciones enmarcadas en la protección del puerto.
- El CPP realiza reuniones periódicas y el Plan de Protección debe estipular cada cuanto tiempo se reúnen. Si ocurre un suceso que amerite su convocatoria antes de la reunión prevista el PPIP debe estar abierto a reuniones no programadas.
- Se debe llevar un registro de cada reunión que se realice, con sus integrantes, enmarcando los temas, el propósito, los avances, entre otros puntos de importancia para la protección del puerto.

8.3.2.8. Procedimientos de Protección

Todos los procedimientos se elaboran en presente y los puntos a desarrollar van enumerados y/o viñetas para un mejor entendimiento.

1. Hacer frente a las amenazas para la protección o a un fallo de las medidas de protección. (Agregar con que protección física cuenta la I.P y especificar un procedimiento general para reaccionar ante las amenazas, según los sucesos que puedan afectar a la protección marítima y detallar los posibles casos bajo una evaluación técnica). Incluir disposiciones necesarias para mantener las operaciones esenciales de la instalación portuaria o de la interfaz buque-puerto.
2. Responder a cualquier instrucción que se dé, en los Niveles de Protección 1-2-3, por la DNS. (Establecer como es la comunicación y coordinación de la I.P, a nivel interno en el accionar sobre la protección y con la DNS cuando hay cambios en los niveles de protección).
3. Evacuación en caso de amenaza para la protección o de fallo de las medidas de protección. (Detallar el plan de evacuación, quien lo coordina, especificar el alcance del personal con funciones de protección, ubicación de las señalizaciones de evacuación, puntos de encuentro o reunión y como se le alerta al personal administrativo, operativo y visitante de la forma de evacuar la I.P, y medidas a tomar con los buques atracados).
4. La interfaz con las actividades buque-puerto. Dividir en tres puntos:
   - Arribo: Tiempo de anticipación para recibo de toda la documentación del buque, especificar la comunicación entre naviera/ IP y qué medidas se toman en materia de protección para el área de atraque.
   - Estadía: Cómo es la coordinación con entidades de seguridad /naviera/ depto. de protección o similar de la IP y vigilancia durante las estadía del buque en la IP (marítimo /terrestre).
   - Salida: Cómo es la coordinación con entidades de seguridad /naviera/ depto. de protección o similar de la IP y durante la salida del buque.
5. La revisión periódica del plan y su actualización. (Especificar cada cuanto tiempo es revisado el PPIP, quién o quiénes son los responsables del proceso y detallar los casos que lo ameriten, además añadir el siguiente punto: Toda actualización debe hacerse y someterse al conocimiento, revisión y aprobación de la Dirección de Navegación y Seguridad. Se incluyen todas las correcciones y se mantienen registrados en el Documento de Control de este plan aprobado).
6. Informar y alertar de los sucesos que afecten la protección marítima a la DNS y al Comité de Protección Portuaria de la Instalación Portuaria. (Especificar quién es el responsable de informar al CPP, medios de comunicación con las entidades, listado de puntos de

contactos, tiempo de notificación y describir como se informa a la DNS).

7. Presentar y evaluar sucesos de protección e informes relativos a posibles fallos. (Especificar si tienen un comité de protección, registros de los sucesos y describir quién es el responsable de evaluar lo ocurrido durante el suceso, y todo el proceso general que conlleve un análisis completo).
8. En caso de activación del sistema de alerta de protección de un buque en la IP (Detallar coordinación OPIP-OPB-Naviera-Marina Mercante, medidas a tomar, comunicación interna y con autoridades competentes).
9. Facilitar el permiso a tierra del personal del buque o los cambios del personal, así como el acceso a los visitantes al buque, incluidos los representantes de las organizaciones para el bienestar de la gente de mar y los sindicatos.
   Se recomienda separar este procedimiento de la siguiente manera:

   - **Facilitar el permiso a Tierra del Personal del buque**
   - **Facilitar los cambios del personal del buque**
   - **Facilitar el acceso a los visitantes del buque**

   Explique en cada uno cual será el procedimiento de identificación, medidas de seguridad y la facilitación que dará el puerto en cada uno de estos permisos al personal.

   Cómo es custodiado el traslado de los tripulantes desde y hacia al buque, medidas para verificar la identificación de los tripulantes, agentes navieros, cambio de tripulación, y otras visitas.
10. Los procedimientos necesarios para evaluar la eficacia en todo momento de las medidas, procedimientos y equipos de protección.
    Dividir en los siguientes puntos:
    - Auditoría interna: metodología, quien es responsable, tiempo, criterios a auditar.
    - Ejercicios y prácticas: frecuencia, comunicación, ejecución, cronograma anual.
    - Calibración y prueba de equipos de protección: nombre del armero, especificar mediante una tabla o listado los equipos de protección contemplados por la IP, el personal o departamento responsable del mantenimiento y la frecuencia. Garantizar que los sistemas de comunicación que se dispone, se mantengan continuas y eficaces entre el puerto, buque y autoridades locales en los tres niveles de protección.

    Nota: Todo formato de mantenimiento y prueba de equipo de protección debe quedar debidamente documentado en el Anexo I denominado “Registros” (Anexos del PPIP).
11. Mantener y actualizar un inventario de mercancías peligrosas y su control de entrada y salida. *[Especificar qué productos manejan,*

almacenamiento, trasiego, quién o quiénes son responsables de llevar un inventario actualizado de las mercancías, describir área designada en la IP, con qué tiempo de anticipación es notificada la operación, en el caso de explosivos establecer las medidas a seguir y la coordinación con otros departamentos de la IP].

12. Ayudar a los oficiales de protección del buque a confirmar la identidad de las personas que deseen subir a bordo. *[Tiempo de anticipación, tipo de identificación que se le entrega a las visitas del buque y medidas para custodiar, de no haber notificación previa de visitantes qué medidas se toman].*
13. Cuando el nivel de protección de la IP, es inferior al de un buque. Coordinación de OPIP-OPB-Naviera, comunicación con Capitanía de Puerto, describir posible área restringidas para este proceso, en caso de que no se deja atracar los buques especificar las medidas o procedimientos tomadas por la IP, referirse a la Declaración de Protección Marítima *[Identificar claramente el proceso antes del arribo de la nave al puerto].*
14. Capacitaciones y entrenamientos al personal con y sin funciones de protección de la IP *[Detallar los diferentes adiestramientos para el personal con tareas específicas de protección y el personal sin funciones de protección, quién o quiénes son responsables de este proceso, cronograma de capacitación, plan de seguimiento. En cuanto a la seguridad subcontratada mantienen registros de idas al Polígono, Manejo de armas, Generalidades del código PBIP, entre otras capacitaciones].* Parte A/17.2.7 PBIP.
15. Procedimiento para la evaluación y supervisión al personal de protección antes de ser contratado y su verificación periódica. Dividir en dos:
    - Seguridad Subcontratada: como se evalúa al personal, información que se le exige, tipo de exámenes, frecuencia, toda esta información es revisada por el OPIP, quien lo supervisa
    - Personal de Protección: requisitos, como se evalúan, tipo de exámenes y su frecuencia.
16. Procedimiento para la emisión de la Declaración de Protección Marítima (DPM). *[Quiénes están autorizados para firmar, en que situaciones se debe actualizar o generar una nueva y como se lleva a cabo dicho procedimiento].*
17. Medidas previstas para evitar que se introduzcan a bordo de un buque o en la instalación portuaria armas, sustancias peligrosas y dispositivos destinados a ser utilizados contra personas, buques o puertos y cuyo transporte no esté autorizado.
18. Medidas destinadas a prevenir el acceso no autorizado a la instalación portuaria, a los buques amarrados en ella y a las zonas restringidas de la instalación portuaria.

8.3.2.9. Medidas de carácter físico operacional para los niveles de protección portuaria.

A. Nivel de Protección 1

A.1. Acceso a la Instalación Portuaria

Establecer los puntos de control en los que se podrán aplicar las siguientes medidas:

1. Delimitar las zonas restringidas, debe especificar el tipo de restricción que se impondrá y los medios para garantizar su observancia.
2. Comprobar la identidad de todas las personas que deseen entrar en la IP para acceder a un buque, incluido los pasajeros, el personal del buque y los visitantes, y confirmar los motivos que tienen para hacerlo, mediante la comprobación, por ejemplo, de las instrucciones de embarco, los billetes de los pasajeros, las tarjetas de embarco, ordenes de trabajo, etc.
3. Los pasajeros deben poder demostrar su identidad con documento de identificación oficial y su ingreso mediante su tarjeta de embarco, billete, etc., pero no se les permitirá acceder a las zonas restringidas a menos que estén supervisados.
4. Controlar los vehículos utilizados por quienes deseen entrar en la IP para acceder a un buque.
5. Verificar la identidad del personal de la IP, de las personas que trabajen dentro de la IP y los visitantes, así como de sus vehículos.
6. Limitar el acceso para excluir a las personas que no trabajen para la IP o dentro de ella si no pueden identificarse debidamente.
7. Registrar a las personas, sus efectos personales, los vehículos y el contenido de estos.
8. Identificar todo punto de acceso que no se utilice regularmente y que convendría cerrar de forma permanente.
9. El PPIP debe indicar la frecuencia con que se aplicarán los controles de acceso, y si se aplicarán al azar o de vez en cuando.

A.2. Zonas Restringidas dentro de la Instalación Portuaria:

Debe especificar la extensión y las medidas que habrán de adoptarse para controlar, por un lado, el acceso a esas zonas y por otro, las actividades que se realicen en ellas. Entre las medidas que debe observar están las siguientes:

1. Instalar barreras permanentes o temporales que rodeen la zona restringida.
2. Establecer puntos de acceso que puedan estar controlados por guardias de seguridad cuando se utilicen, y que puedan cerrarse o bloquearse eficazmente si no se utilizan.
3. Expedir pases que deberán llevar visibles quienes tengan derecho a encontrarse dentro de la zona restringida.

4. Todo registro que se realice, debe llevarse a cabo de manera tal que se respete plenamente los derechos humanos y la dignidad de las personas.
5. Identificar claramente los vehículos autorizados a entrar en las zonas restringidas.
6. Organizar patrullas y guardias.
7. Instalar sistemas automáticos de detección de intrusos o equipos o sistemas de vigilancia, para detectar el acceso no autorizado a las zonas restringidas y los movimientos en éstas.
8. Controlar el movimiento de naves en las proximidades de los buques que utilicen la instalación portuaria.
9. En el PPIP se debe establecer que todas las zonas restringidas estarán claramente marcadas, indicándose que el acceso a la zona queda restringido y que la presencia no autorizada dentro de la zona constituye una violación de las normas de protección.
10. Las zonas restringidas pueden ser, entre otras, las siguientes:
    - las zonas de tierra y las aguas contiguas al buque;
    - las zonas de embarco, desembarco, zonas de espera, tramitación para los pasajeros y el personal de los buques, incluidos los puntos de registro;
    - las zonas de embarque, desembarque y almacenamiento de la carga y las provisiones de los buques;
    - los lugares en los que se guarde información importante desde el punto de vista de la protección, como la relativa a la carga;
    - las zonas en las que se guarden mercancías peligrosas y sustancias potencialmente peligrosas;
    - las salas de control de los sistemas de ordenación del tráfico marítimo, las ayudas a la navegación y los edificios de control del puerto, incluidas las salas de control de los sistemas de protección y vigilancia;
    - las zonas en las que se almacene o está situado el equipo de protección y vigilancia;
    - las instalaciones esenciales radioeléctricas, de telecomunicaciones, de electricidad, de agua y de otros servicios públicos;
    - otros lugares de la instalación portuaria a los que deba restringirse el acceso de buques, vehículos y personas.

A.3 Manipulación de la Carga

Establecer las medidas de protección aplicables a la manipulación de la carga y al equipo para la manipulación de la carga en la IP:

1. Evitar la manipulación indebida.
2. Evitar que se reciban y almacenen en la instalación portuaria cargas que no estén destinadas a ser transportadas.

3. Inspeccionar la carga, las unidades de transporte y las zonas para almacenar la carga dentro de la IP antes y durante las operaciones de manipulación de la carga.
4. Efectuar comprobaciones para asegurarse de que la carga que se embarca coincide con lo indicado en la nota de entrega o equivalente.
5. Registrar los vehículos.
6. Comprobar el estado de los precintos u otros medios utilizados para evitar la manipulación indebida de la carga a la entrada de esta en la instalación portuaria, y en el momento de proceder a su almacenamiento en la instalación.
7. Las inspecciones de la carga pueden realizarse mediante examen visual y físico; mediante la utilización de equipos de exploración / detección, dispositivos mecánicos o perros adiestrados para estos fines.
8. Cuando haya un movimiento de carga regular, o repetido, el OCPM o el OPB, tras consultar a la IP, podrán llegar a un acuerdo con el expedidor o con otras partes responsables de la carga sobre la inspección de ésta fuera de las instalaciones, el precintado, la programación de los movimientos, los comprobantes, etc. Estos acuerdos deben notificarse al OPIP interesado, para obtener su conformidad.

A.4. Entrega de Provisiones al Buque

Establecer las medidas de protección aplicables a la entrega de las provisiones del buque.

1. Inspeccionar las provisiones.
2. Notificar por adelantado la composición de la remesa, los datos del conductor y la matrícula del vehículo.
3. Registrar el vehículo utilizado para la entrega.
4. Las inspecciones de las provisiones de los buques pueden realizarse mediante examen visual y físico; mediante la utilización de equipos de exploración, detección, dispositivos mecánicos o perros adiestrados para tales fines.
5. Siempre debe ser posible confirmar que las provisiones que se entregan van siempre acompañadas de alguna prueba que han sido pedidas por el buque.

A.5. Equipaje No Acompañado

Establecer las medidas de protección aplicables a los equipajes no acompañados para garantizar que hasta el 100% de dichos equipajes se somete a un examen o registro, lo que puede incluir la utilización de equipo de rayos X.

A.6. Vigilancia de la Instalación Portuaria

Establecer las medidas de protección aplicables que pueden incluir una combinación de alumbrado, oficiales de seguridad (a pie/motorizados/en

embarcaciones), dispositivos automáticos de detección de intrusos y equipo de vigilancia; el cual debe funcionar de manera continua y permita que el personal encargado de la protección de la instalación portuaria pueda:

1. Vigilar en todo momento, incluso en la oscuridad y con visibilidad limitada, toda la instalación portuaria, los accesos por mar y tierra, las zonas restringidas dentro de la instalación, los buques que se encuentren en ella y los alrededores de esos buques.
2. Cuando se utilicen dispositivos automáticos de detección de intrusos, éstos deben dar una alarma visual y/o audible en un espacio con dotación o vigilancia permanente.
3. En el PPIP deben especificarse los procedimientos y el equipo necesario para cada nivel de protección, así como los medios para garantizar que tal equipo de vigilancia funcione continuamente, teniendo en cuenta los posibles efectos de las condiciones meteorológicas o de las interrupciones del suministro eléctrico.

B. Nivel de Protección 2

B.1 Acceso a la Instalación Portuaria

Especificar las medidas de protección adicionales que habrá de tomar y que pueden ser, entre otras.

1. Destinar más personal a la vigilancia de los puntos de acceso y el patrullaje de las barreras del perímetro de la instalación.
2. Limitar el número de puntos de acceso a la IP e identificar los que conviene cerrar, habilitando medios para protegerlos adecuadamente.
3. Habilitar medios para obstaculizar el movimiento por los demás puntos de acceso, por ejemplo instalando barreras de seguridad.
4. Aumentar la frecuencia de los registros de personas, efectos personales y vehículos.
5. Denegar el acceso a los visitantes que no puedan aportar una justificación verificable de la razón por la que deseen acceder a la IP. Tomar nota de ellos e informar a las autoridades competentes.
6. Realizar patrullaje con embarcaciones para incrementar la protección de las aguas de la IP.

B.2. Zonas Restringidas dentro de la Instalación Portuaria

Indicar como se va a incrementar la frecuencia e intensidad de la vigilancia y el control de acceso a las zonas restringidas. Especificar las medidas de protección adicionales que habrá que tomar, y que pueden ser entre otras:

1. Reforzar la eficacia de las barreras o vallas que delimiten las zonas restringidas, utilizando, por ejemplo, sistemas automáticos de detección de intrusos o patrullas.

2. Reducir el número de puntos de acceso a las zonas restringidas y reforzar los controles aplicables en los demás accesos.
3. Restringir el estacionamiento en las zonas adyacentes a los buques amarrados.
4. Limitar aun más el acceso a las zonas restringidas, así como los movimientos y el almacenamiento en esas zonas.
5. Utilizar equipo de vigilancia supervisado de forma continua y con grabación.
6. Reforzar el número y la frecuencia de las patrullas, incluidas las patrullas marítimas, en los límites de las zonas restringidas y dentro de dichas zonas.
7. Controlar y restringir el acceso a las zonas adyacentes a las zonas restringidas.
8. Impedir el acceso de naves no autorizadas a las aguas adyacentes a los buques que se encuentren en la instalación portuaria.

B.3. Manipulación de la Carga

Establecer las medidas de protección adicionales aplicables para la manipulación de la carga.

1. Efectuar inspecciones pormenorizadas de la carga, las unidades de transporte y las zonas para almacenar la carga dentro de la instalación portuaria.
2. Intensificar las comprobaciones para garantizar que solo entra en la IP carga debidamente documentada para su almacenamiento temporal y posterior embarque en un buque.
3. Intensificar los registros de vehículos.
4. Aumentar la frecuencia y la minuciosidad de las comprobaciones de los precintos y otros medios utilizados para evitar la manipulación indebida.

Una inspección pormenorizada de la carga puede lograrse por los siguientes medios*:*

- Aumentar la frecuencia y la minuciosidad de las inspecciones de la carga, las unidades de transporte y las zonas para almacenar la carga dentro de la IP (visuales y físicos).
- Usar con más frecuencia equipos de exploración/ detección, dispositivos mecánicos o perros.
- Coordinar las medidas de protección reforzadas con el expedidor u otras partes responsables, además de los acuerdos y procedimientos ya concertados.

B.4. Entrega de Provisiones al Buque:

Establecer las medidas de protección adicionales aplicables a la entrega de las provisiones de los buques, que pueden ser, entre otras:

1. Efectuar inspecciones pormenorizadas de las provisiones de los buques.

2. Efectuar registros pormenorizados de los vehículos utilizados para las entregas.
3. Coordinar con el personal de los buques para comprobar que la remesa coincide con la nota de entrega antes de autorizar su entrada en la instalación portuaria.
4. Acompañar al vehículo utilizado para la entrega dentro de la instalación portuaria.

Una inspección pormenorizada de las provisiones de los buques puede lograrse por los siguientes medios:

- Aumentar la frecuencia y la minuciosidad de los registros de los vehículos utilizados para las entregas.
- Usar con más frecuencia equipos de exploración/detección, dispositivos mecánicos o perros adiestrados para tales fines.
- Restringir o prohibir la entrada de provisiones que no vayan a salir de la instalación portuaria en un determinado plazo.

B.5. Equipaje No Acompañado

Establecer las medidas de protección adicionales aplicables a los equipajes no acompañados las cuales deben prever que se someta a un examen con equipo de rayos X el 100% de los equipajes.

B.6. Vigilancia de la Instalación Portuaria

Establecer las medidas de protección adicionales necesarias para incrementar la capacidad de observación y vigilancia.

1. Aumentar la intensidad del alumbrado y la cobertura del equipo de vigilancia, incluida la instalación de alumbrado y equipo de vigilancia adicional.
2. Aumentar la frecuencia de las patrullas de a pie, motorizadas o en embarcaciones.
3. Destinar más personal de protección a las tareas de observación y patrullaje.

C. Nivel de Protección 3

C.1. Acceso a la Instalación Portuaria

La IP debe cumplir las instrucciones de los encargados de hacer frente al suceso. El PPIP debe especificar las medidas de protección que puede adoptar la IP, en estrecha colaboración con los encargados de hacer frente a un suceso y con los buques que se encuentren en ella, medidas que pueden ser, entre otras, las siguientes:

1. Suspender el acceso a la IP, o a partes de ella.
2. Autorizar únicamente el acceso de los encargados de hacer frente al suceso que afecte a la protección o a la amenaza de este.

3. Suspender los movimientos de personas o vehículos en la instalación portuaria o en partes de ella.
4. Incrementar las patrullas de protección en la IP.
5. Suspender las operaciones portuarias en toda la IP o en algunas de sus partes.
6. Dirigir los movimientos de los buques en toda la IP o en algunas de sus partes.
7. Evacuar total o parcialmente la instalación portuaria.

C.2. Zonas Restringidas a la Instalación Portuaria

La IP debe cumplir las instrucciones de los encargados de hacer frente al suceso. El PPIP debe especificar las medidas de protección que puede adoptar la IP, en estrecha colaboración con los encargados de hacer frente a un suceso y con los buques que se encuentren en ella.

1. Establecer zonas restringidas adicionales, dentro de la instalación, en las proximidades del suceso que afecte a la protección marítima o del lugar en el que se sospecha que está la amenaza para la protección, en las que se prohibirá el acceso.
2. Preparar el registro de las zonas restringidas como parte del registro total o parcial de la IP.

C.3. Manipulación de la Carga

La IP debe cumplir las instrucciones de los encargados de hacer frente al suceso. El PPIP debe especificar las medidas de protección que puede adoptar la IP, en estrecha colaboración con los encargados de hacer frente al suceso y con los buques que se encuentren en ella, las cuales pueden ser, entre otras:

1. Limitar o suspender los movimientos u operaciones de carga en toda la instalación portuaria o en partes de ella, o en determinados buques.
2. Verificar el inventario de mercancías peligrosas, sustancias potencialmente peligrosas que se encuentren en la instalación portuaria y comprobar su ubicación.

C.4. Entrega de Provisiones al Buque

La IP debe cumplir las instrucciones de los encargados de hacer frente al suceso. El PPIP debe especificar las medidas de protección que puede adoptar la IP, en estrecha colaboración con los encargados de hacer frente al suceso y con los buques que se encuentren en ella, medidas que pueden incluir preparar la restricción o suspensión de la entrega de provisiones para los buques en toda la instalación portuaria, o en partes de ella.

C.5. Equipaje No Acompañado

La IP debe cumplir las instrucciones de los encargados de hacer frente al suceso. La PPIP debe especificar las medidas de protección que puede adoptar la IP, en estrecha colaboración con los encargados de hacer frente un suceso y con los buques que se encuentren en ella.

1. Someter los equipajes a un examen más extenso, por ejemplo, viéndolos por rayos X desde al menos dos ángulos distintos.
2. Preparar la restricción o suspensión del tratamiento de equipajes no acompañados.
3. Negarse a aceptar la entrada de equipajes no acompañados en la instalación portuaria.

C.6. Vigilancia de la protección de la Instalación Portuaria

La IP debe cumplir las instrucciones de los encargados de hacer frente al suceso. El PPIP debe especificar las medidas de protección que puede adoptar la IP, en estrecha colaboración con los encargados de hacer frente al suceso y con los buques que se encuentren en ella.

1. Encender todo el alumbrado de la instalación portuaria y el que ilumine sus inmediaciones.
2. Encender todo el equipo de vigilancia de la instalación portuaria que pueda grabar las actividades en la instalación y en sus inmediaciones.
3. Prolongar al máximo el período de tiempo que pueda grabar el equipo de vigilancia.

D. Niveles de protección diferentes entre el buque y la IP

Establecer los procedimientos y las medidas de protección que puede aplicar la instalación portuaria si su nivel de protección es inferior al de un buque.

E. Actividades no reguladas por el Código

Establecer los procedimientos y las medidas de protección que debe aplicar la IP cuando:

1. Realice una operación de interfaz con un buque que haya hecho escala en un puerto de un Estado que no sea un Gobierno Contratante.
2. Realice una operación de interfaz con un buque al que no se aplique el presente Código.
3. Realice una operación de interfaz con una plataforma fija o flotante o con unidades móviles de perforación emplazadas mar adentro.

F. Declaraciones de protección marítima

Indicar los procedimientos que habrán de seguirse cuando el OPIP, atendiendo a las instrucciones de la DNS, solicite una declaración de protección marítima, o cuando tal declaración la solicite un buque.

G. Auditorías, revisiones y enmiendas

Indicar el método de auditoría que tiene previsto utilizar el OPIP para verificar que el plan sigue siendo eficaz y el procedimiento que habrá de seguirse para la revisión, actualización o enmienda del plan. El PPIP debe revisarse a discreción del OPIP. Además, debe revisarse en los casos siguientes:

1. Si se modifica la evaluación de la instalación portuaria.
2. Si una auditoría independiente del PPIP o las pruebas que realice el Gobierno de Costa Rica, de la organización de la protección de la instalación portuaria ponen de manifiesto fallos organizativos o plantean la duda de que ciertos elementos importantes del PPIP aprobado sigan siendo válidos.
3. Después de haberse producido un suceso que afecte a la protección marítima o una amenaza para ésta relacionados con la instalación portuaria.
4. Cuando se produzca un cambio en la propiedad de la instalación portuaria o en el control de su explotación.

El OPIP puede recomendar las enmiendas oportunas al plan aprobado tras una revisión de éste. Se deben presentar a la DNS para su examen y aprobación, las enmiendas al PPIP que supongan:

1. Cambios que puedan alterar fundamentalmente el enfoque adoptado para mantener la protección de la instalación portuaria.
2. La eliminación, alteración o sustitución de barreras permanentes, equipo y sistemas de protección y vigilancia u otros elementos que se consideraban anteriormente esenciales para garantizar la protección de la instalación portuaria.
3. La DNS podrá aprobar las enmiendas propuestas, con o sin cambios. Al aprobarse el PPIP, la DNS debe indicar los cambios físicos o de procedimiento que requerirán su aprobación.

8.3.2.10. Referencias:

- Acceso a la Instalación Portuaria. *[Inclúyase: consideraciones adicionales, B/16.10 PBIP].*
- Zonas restringidas de la instalación portuaria. *[Inclúyase: consideraciones adicionales, B/16.21 PBIP].*
- Manipulación de la carga. *[Inclúyase: consideraciones adicionales, B/16.30 PBIP].*

- Entrega de provisiones al buque. *[Inclúyase: consideraciones adicionales, B/16.38 PBIP].*
- Equipajes no acompañados. *[Inclúyase: consideraciones adicionales, B/16.45 PBIP].*
- Vigilancia de la protección de la instalación portuaria. *[Inclúyase: consideraciones adicionales, B/16.49 PBIP].*

8.3.2.11. Anexos del PPIP

I. Anexo A. Descripción de las amenazas y vulnerabilidades de la instalación portuaria

[El Anexo A conceptúa la información relevante para el desarrollo, administración y operación de un puerto y/o una instalación portuaria, y el extracto de lo enunciado de acuerdo con la Evaluación de Protección y su actualización previamente aprobada por la Dirección de Navegación y Seguridad.]

- Información Interna de la Instalación Portuaria.
- Descripción física de las instalaciones: Características, categoría, ubicación geográfica (coordenadas), mareas y calados, características del suelo, estructura portuaria incluyendo rompeolas, perímetro, estructura de servicios que ofrece, superficie, topografía, clima, áreas administrativas y aquellas destinadas al bienestar del tripulante de un buque.
- Incluir plano que contenga información de la instalación.
- Amenazas.
- Vulnerabilidades.
- Blancos Potenciales.
- Áreas restringidas en la Instalación Portuaria.
- Anillos de protección.

II. Anexo B. Identificación de la Instalación Portuaria

B.1 – La Empresa, Ejecutivos y Propiedad.

- Nombre completo de la empresa, datos de contactos (teléfonos, celulares, correos electrónicos), representantes legales;
- Concesión marítima portuaria (cuando aplique);
- Propiedad y Ejecutivos;
- Tipo de administración;
- Identificación y modo para ubicar al OPIP;
- Localización y dirección específica, detallando provincia, distrito, cantón, área Pacífica o Atlántica.

B.2 – Información Interna y Actividad de la Instalación Portuaria.

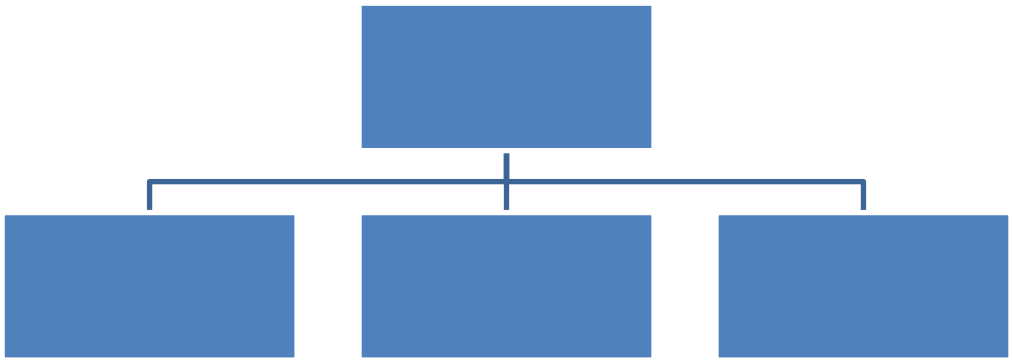
III. Anexo C. Organización y administración de protección de la instalación portuaria.

C.1 – Función y estructura de la organización y administración de protección de la instalación portuaria

Información del Gerente de Protección / OPIP / Oficial de Protección Suplente (s) / Supervisores de Seguridad o Protección / Secretaria de Protección / Empresa de Seguridad Sub. Contratada.

- Nombre
- Cargo(s)
- Teléfono Oficina
- Teléfono Móvil
- E-mail

Se presentarán un gráfico con la estructura de la Organización General de la Instalación Portuaria y otro de la Organización General de Protección de la Instalación Portuaria:



C.2 – Requisitos, responsabilidades y tareas del personal de protección.

Requisitos Mínimos de:

- Oficial de Protección Portuaria
- Oficial de Protección Suplentes
- Guardias de Seguridad
- Recepcionistas
- Otros

Responsabilidades y tareas de:

- Oficial de Protección Portuaria
- Oficial de Protección Suplentes

- Guardias de Seguridad
- Recepcionistas
- Otros

Capacitación, programa e instrucción de protección y evaluación.

Personal que eventualmente desempeña funciones especificas de protección y aquellos sin funciones específicas de protección.

Agencias de Seguridad Subcontratada.

IV. Anexo D. Enlaces internos en la instalación portuaria y con entidades nacionales cuya responsabilidad enmarca la Seguridad / Protección.

- Departamentos, secciones en la Instalación Portuaria
  - Gerentes de Protección
  - Personal de Protección
  - Personal de Seguridad
  - Cuarto de CCTV
  - Otros
- Entidades Gubernamentales
- Otros.

[Presentar plano de ubicación geográfica en que se demarquen los límites físicos de la instalación portuaria, vías de aproximación y acceso, estaciones de policías, bomberos, servicios médicos, servicios marítimos portuarios, entidades gubernamentales ubicadas en la zona y todas aquellas que correlacionan con los puertos]

[Características del entorno con énfasis en las que resultan ser un riesgo para sus operaciones, detallando las distancias de las entidades, dirección, teléfonos y tiempo estimado de concurrencia en situaciones de emergencia, resumiéndolo en un cuadro]

Enlaces internos en la instalación portuaria y con entidades nacionales cuya responsabilidad enmarca la Seguridad / Protección				
Entidad	**Nombre del Responsable**	**Dirección**	**Teléfonos** **Oficina/Móvil**	**Tiempo y Distancia Estimado de Concurrencia**

V. Anexo E. Listado de Contacto de los Oficiales de Protección de las Instalaciones Portuarias.

[*La Dirección de Navegación y Seguridad recopilará los datos pertinentes y los informará oportunamente a los Oficiales de Protección de las Instalaciones Portuarias.]*

Es responsabilidad de cada OPIP informar cualquier cambio de contacto a la DNS, a efecto de mantener el listado actualizado.

VI. Anexo F. Notificación–Cambio en Niveles de Protección (DNS)

El OPIP debe informar oportunamente a la DNS, sobre la existencia de indicios, actos o circunstancias que levante sospechas y que constituyan una amenaza para la protección del buque o a la instalación portuaria y que pueda justificar un cambio de nivel.

El Director de la DNS analizará con las autoridades superiores competentes la situación que se le presente y se valorará la posibilidad de realizar un cambio de nivel. En caso de un cambio de nivel, se informará en primer lugar al OPIP para que proceda según lo exijan las circunstancias y en concordancia con el PPIP.

VII. Anexo G. Planes de contingencias

[Inclúyase, planes y/o procedimientos alternos que identifique la seguridad o protección de la instalación portuaria: Guías, Manuales, Instrucciones de trabajo, sistema de calidad].

VIII. Anexo H. Formularios

Formularios:

- Modelo de la Declaración de Protección Marítima.
- Notificación y recepción del cambio en niveles de protección.
- Reporte de sucesos de protección.
- Formato de mantenimiento y prueba de equipos de protección.
- Entrenamiento de seguridad y/o protección.

- Ejercicios y prácticas de protección.
- Planos de la instalación portuaria con información de protección (acceso, vigilancia, áreas restringidas, punto de reunión, infraestructura física y operacional).
- Otros.

IX. Anexo I. Registros

[Se llevará registros de todas las actividades previstas en el plan las que serán mantenidas por un periodo no menor a 5 años].

- Ejercicios y Prácticas.
- Entrenamientos y capacitaciones.
- Reportes de sucesos e incidentes de protección.
- Declaración de Protección Marítima.
- Cambio de Nivel de Protección.
- Mantenimiento, calibración y prueba del equipo de protección.
- Revisión periódica de la evaluación de protección.
- Auditorias de protección.
- Control de acceso y salida de la instalación portuaria.
- Comunicaciones internas en la instalación portuaria.
- Comunicaciones externas.
- Otros.

9. PROCEDIMIENTO PARA REALIZAR LAS AUDITORÍAS EXTERNAS A LAS INSTALACIONES PORTUARIAS

La auditoría es un proceso sistemático, independiente y profesional para obtener y evaluar objetivamente evidencia, en relación con hechos y eventos de diferente naturaleza; con el propósito de comprobar su grado de correspondencia con un marco de referencia de criterios aplicables y; comunicar los asuntos determinados, así como las conclusiones y disposiciones o recomendaciones con el fin de impulsar mejoras en la gestión y facilitar la toma de decisiones.

En la aplicación del Código PBIP los procedimientos de auditorías externas de protección constituyen el medio para aprobar los planes de protección o verificar que el PPIP sigue siendo válido, en cuyo caso se podrá expedir una declaración de cumplimiento de la instalación portuaria.

Este apartado abarca dos temas importantes que son el marco general que contiene principios generales para las auditorías y los procedimientos que se deberán seguir para la realización de las mismas.

9.1. Marco general para la auditoria de protección

El Marco constituye el conjunto de principios generales dentro de las cuales se deben realizar las auditorias de protección.

9.1.1. Finalidad

La finalidad del presente es describir el objetivo, principios y alcance, de la auditoria de protección

9.1.2. Aplicación

El presente Marco se aplicará a todos los participantes en la auditoría de un sistema de protección.

9.1.3. Definiciones

Auditoría: Proceso sistemático, independiente y documentado para obtener pruebas de auditoría y evaluarlas objetivamente con el fin de determinar en qué medida se cumplen los criterios de auditoría.

Criterios de auditoría: Conjunto de políticas, prácticas, procedimientos, principios, prescripciones o requisitos frente a los cuales el auditor compara las evidencias recogidas.

Pruebas de auditoría: Registros, exposiciones de hechos u otra información que guarden relación con los criterios de auditoría y se puedan verificar.

Cumplimiento: Observancia de una prescripción.

Medidas correctivas: Medidas para eliminar la causa de un incumplimiento detectado u otra situación no deseada.

Documento: Información y su soporte.

Conclusión: Observación o incumplimiento.

Información: Datos significativos.

Incumplimiento: Situación observada en la que hay pruebas objetivas que indican que no se ha cumplido una determinada prescripción.

Observación: Exposición de hechos formulada durante una auditoría y justificada con pruebas objetivas.

Pruebas objetivas: Información cuantitativa o cualitativa, registros o exposiciones de hechos, basados en observaciones, medidas o análisis y que puedan verificarse.

Medidas preventivas: Medidas para eliminar la causa de un posible incumplimiento u otra posible situación no deseada.

Procedimiento: Manera específica de llevar a cabo una actividad o un proceso.

Proceso: Serie de actividades interrelacionadas o interactivas que transforman los aportes en resultados.

Registros: Documentos que exponen los resultados alcanzados o que dan prueba de las actividades realizadas.

Prescripciones: Necesidad o expectativa formulada, generalmente implícita u obligatoria.

Verificación: Confirmación, mediante la aportación de pruebas objetivas, de que determinadas prescripciones se han cumplido.

9.1.4. Norma de la auditoria

La norma de la auditoría será el Código de Protección de Buques e Instalaciones Portuarias (Código PBIP).

9.1.5. Propósito de la Auditoría Externa a las Instalaciones Portuarias

Fomentar la implantación uniforme y eficaz del Código PBIP y contribuir de esa manera a la mejora de la actuación de todos los involucrados para dar cumplimiento a las prescripciones del Código PBIP.

9.1.6. Objetivo y alcance de la Auditoría Externa a las Instalaciones Portuarias

El objetivo de la auditoria es determinar la medida en que se implantan y ejecutan los Planes de Protección aprobados, y demás directrices o normas, que se emitan para la mejora de los sistemas de protección.

Al tomar medidas para mejorar la protección se actuará de manera que, ni directa ni indirectamente, se transfieran daños o peligros de un área a otra o se transformen en un tipo de peligro mayor.

9.1.7. Principios

- **Coherencia, imparcialidad, objetividad e independencia**

Las auditorías deberán tener un enfoque constructivo, ser pragmáticas e imparciales y ajustarse a un plazo determinado. Reconociendo y apreciando el hecho que se pueden cumplir las responsabilidades de formas distintas, pero igualmente válidas. Se debe garantizar que la calidad de las auditorías responde a un nivel adecuado de coherencia y uniformidad.

- **Transparencia y divulgación**

Los informes provisionales y finales de auditoría deberán ser confidenciales y accesibles exclusivamente a las partes involucradas.

La DNS podrá dar a conocer cuando lo estime pertinente, algunas de las buenas prácticas encontradas para mejorar otros sistemas de protección.

- **Mejora constante**

Las auditorias deben tener como resultado, la mejora constante de la implantación y ejecución por parte de los Auditados, de los Planes de Protección y otras medidas adoptadas para el cumplimiento del Código PBIP.

9.1.8. Responsabilidades

El Director de la DNS tiene la responsabilidad de:

- Implantar un sistema de auditorías de protección incluyendo las actividades de seguimiento.
- Constituir un equipo auditor para cada auditoria y nombrar los jefes y miembros de estos equipos, quienes deben contar con la competencia necesaria.
- Establecer el alcance y objetivo de las auditorias de protección.
- Garantizar la formación y capacitación de los auditores y la cooperación técnica para estos fines.
- Procurar la homogeneidad de las auditorías.

- Asegurarse de que las auditorías se planifican según un calendario establecido.
- Cuando se considere necesario, podrá facilitar una reunión previa del jefe del equipo auditor y el auditado antes de la auditoría, a fin de ampliar la información sobre los pormenores de la misma para un mejor entendimiento y cooperación entre las partes.
- Avalar el informe Provisional y Final que se deriven de la auditoría.

El Auditado tiene la responsabilidad de:

- Facilitar al máximo la auditoría. Entre otros, se debe brindar acceso a las instalaciones, a los registros y archivos, y de ser necesario se debe brindar espacio para trabajar preferiblemente en privado, además de facilitar acceso a ordenadores, fotocopiadoras, facsímiles, internet.
- Facilitar acceso al personal seleccionado para las entrevistas.
- Responder a las conclusiones del equipo auditor mediante la preparación de un plan de medidas.
- Implantar el programa de medidas para abordar las conclusiones.

El Jefe del equipo auditor tiene la responsabilidad de:

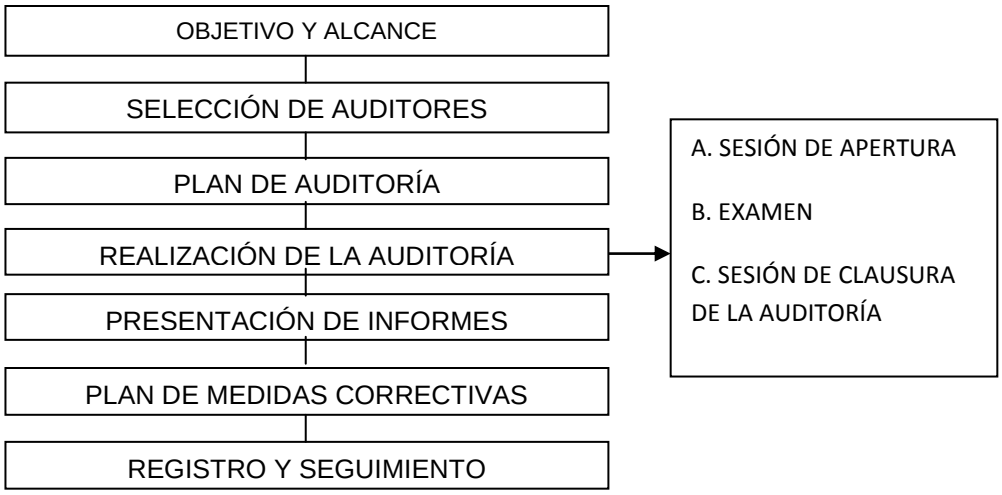
- Representar al equipo auditor.
- Dirigir y supervisar al equipo auditor.

9.2. Procedimiento para la Auditoría Externa a las Instalaciones Portuarias

El procedimiento que se presenta a continuación contiene los pasos a seguir para realizar las auditorías externas de protección, estas constituyen el medio para aprobar los planes de protección y verificar que siguen siendo válidos.

El proceso de la auditoria de protección

El proceso detallado de auditoría de protección se ilustra mediante el esquema siguiente:



Finalidad

La finalidad de la presente es describir los procedimientos para la auditoría de un sistema de protección, en términos generales los siguientes aspectos:

- Plan de auditoría;
- Realización de la auditoría;
- Presentación de informes;
- Plan de medidas correctivas;
- Registro y seguimiento.

Aplicación

Los presentes procedimientos serán de aplicación a todos los participantes en la auditoría de un sistema de protección.

9.2.1. Etapas del proceso de auditoría

I. Objetivo y Alcance de la auditoria

El Director de la DNS establecerá el objetivo y alcance de cada auditoría en particular, dentro del contexto del Marco general.

II. Selección de los auditores

Para la selección de los candidatos a auditor, el Director de la DNS tomará en cuenta, entre otras, las siguientes competencias y aptitudes personales:

- Iniciativa, juicio, tacto, sensibilidad y la capacidad de mantener unas relaciones laborales armoniosas al enfrentarse con obstáculos intencionados o no intencionados durante la auditoría y al trabajar en un entorno interdisciplinario;
- Capacidad para ejercer funciones a nivel directivo y/o superior;

- Motivación demostrada y capacidad para escribir de manera clara y concisa;
- Conocimiento profundo del código PBIP;
- Conocimiento profundo del marco y los procedimientos para la auditoría de protección; y
- Conocimiento básico de los principales Convenios Internacionales promovidos por la Organización Marítima Internacional (SOLAS 74/78, MARPOL 73/78, Convenio de Formación 1978, Convenio Internacional sobre líneas de Carga 66/88, Convenio Internacional de Arqueo 1969, Convenio sobre el Reglamento Internacional para prevenir abordajes 1972);
- Conocimientos de los paquetes informáticos básicos.

El Director de la DNS, entre otras, podrá tener en cuenta para formar un equipo de auditores la necesidad de que:

- Se nombre un jefe del equipo auditor.
- El equipo auditor aspire al mayor nivel de calidad en el desempeño de su tarea.
- El equipo auditor esté compuesto por un número suficiente de auditores para que la auditoría se lleve a cabo y se concluya satisfactoriamente según lo planificado. En algunas situaciones, cabrá la posibilidad de que el equipo se subdivida para realizar actividades paralelas en el transcurso de la auditoría;
- El equipo auditor trabaje en total independencia.

III. Plan de auditoría

El equipo auditor debe definir las actividades a realizar de manera que permita que se logren los objetivos y alcances establecidos por el Director de la DNS. Así mismo debe considerar las coordinaciones necesarias y los recursos disponibles para el desarrollo del trabajo.

El equipo auditor podrá solicitar la información previa que se considere necesaria, la cual deberá ser examinada. Esta información podrá ser utilizada para ultimar el plan pormenorizado de la auditoría.

Cuando se haya solicitado una reunión previa por parte del auditado, se deberán hacer las gestiones necesarias para celebrarla.

Cuando se estime conveniente se debe valorar de manera oportuna la posibilidad de gestionar la utilización asesores externos.

Se deberá elaborar un programa general de las actividades de la auditoria el cual podrá incluir:

- Lugar o lugares donde se vaya a llevar a cabo la auditoría;
- Objetivos y alcance de la auditoría;
- Fechas de inicio y finalización de la auditoría, incluidas las fechas y lugar de las sesiones de apertura y clausura;

- Los nombres de los participantes en la auditoría, tanto los de los auditores como de parte de los auditados.
- Nombre de la persona designada por parte de los auditados, que será el punto de contacto entre estos y el equipo auditor;
- Recursos para el desarrollo del trabajo.

Se valorará la utilización de listas de comprobación o prontuarios para puntualizar los aspectos a auditar.

IV. Realización de la auditoría

El equipo auditor deberá regirse por las pautas generales descritas en el Marco general para la auditoria de protección.

Los miembros del equipo auditor deberán esforzarse por conseguir el mayor grado de objetividad, imparcialidad y confidencialidad posible. Un comportamiento correcto es vital para evitar cualquier impresión de parcialidad a favor o en contra del Auditado.

Se debe reconocer que el resultado final de la auditoría, es decir, los informes de auditoría, incluidas sus conclusiones, son documentos muy delicados, ya que indican al Auditado cómo funcionan algunos componentes del sistema de protección.

Las auditorías pueden suscitar la sensibilización y el interés de algunos sectores, medios de comunicación, organizaciones de empleadores, sindicatos, etc., que quizá soliciten entrevistarse con el equipo auditor. Debido a la naturaleza confidencial que el Código PBIP le brinda al tema, las entrevistas con el equipo auditor sólo tendrán lugar con el consentimiento tanto del Director de la DNS como del Auditado mismo, el cual estará presente en ellas. En todo caso, el equipo auditor se limitará a explicar su mandato y sus objetivos.

La auditoría se deberá realizar siguiendo los plazos establecidos en el programa general.

A. Sesión de apertura

Deberá celebrarse una sesión de apertura entre los auditores y los representantes del Auditado para confirmar los preparativos antes del comienzo de la auditoría. El jefe del equipo auditor deberá aprovechar la sesión para presentar el objetivo y el alcance de la auditoría.

Se deberá considerar que en esa reunión, el Auditado tal vez desee ofrecer información e instrucciones respecto a la instalación portuaria al equipo auditor. El orden del día podrá abarcar al menos los siguientes puntos:

- Presentación de los participantes.

- Información general y explicación de la finalidad de ésta.
- Revisión y confirmación del programa de auditoría por si acaso debe efectuarse algún cambio de horarios.
- Medios y disposiciones de carácter administrativo.
- Coordinar el personal guía que acompañará al equipo durante la auditoría.
- Confirmación que el personal de las áreas a ser auditadas esté disponible.
- Un breve resumen de los métodos y procedimientos que se emplearán en la realización de la auditoría.
- Asegurar al auditado la confidencialidad de la información.
- Dar la oportunidad para que se realicen preguntas de cualquier tipo.

B. Examen

En esta etapa se realizan exámenes, pruebas, entrevistas, observaciones, inspecciones, se evalúan controles, procedimientos y protocolos, etc. para alcanzar los objetivos de la auditoría, determinando si las actividades y los resultados relacionados satisfacen las disposiciones preestablecidas y si estas disposiciones son aplicadas en forma efectiva y son apropiadas.

Este examen conlleva la recopilación de pruebas o evidencia para obtener, justificar y presentar apropiadamente los hallazgos de auditoría.

Conforme se requiera por el equipo auditor, el auditado deberá facilitar la presencia del OPIP, o personal competente, quien deberá acompañar al auditor.

El auditor deberá anotar los pormenores de los incumplimientos detectados y el lugar dónde se observaron. Para ayudar a que el Auditado solucione pronto cualquier caso de incumplimiento detectado, el equipo auditor podrá facilitarle información periódicamente antes de la sesión de clausura.

C. Sesión de clausura de la auditoría

En esta sesión, el Director de la DNS y el equipo auditor, tendrá la oportunidad de presentar a los auditados, una breve reseña de todas las conclusiones que figurarán en el informe provisional de auditoría. Deberá procurarse que los auditados entiendan claramente cuál es la situación según el equipo auditor, y que puedan empezar a trabajar en el plan de medidas correctivas si es necesario.

Al final de la auditoría, durante la sesión de clausura y de ser posible, el Director de la DNS hará entrega al auditado del informe provisional de auditoría.

En esta sesión se podrá tratar con el Auditado las actividades de seguimiento, inclusive propuestas sobre la necesidad y el contenido de un plan de medidas correctivas que elaborará el Auditado. Además se podrá informar al Auditado de las

fechas importantes como lo son la entrega del informe final, y la presentación del plan de medidas correctivas.

La estructura de la sesión de clausura de la auditoría podrá ser la siguiente:

- ✓ Finalidad, alcance y objetivos de la auditoría;
- ✓ Resumen de los procedimientos de la auditoría;
- ✓ Presentación de las observaciones e incumplimientos detectados;
- ✓ Según proceda, información sobre las visitas a los centros pertinentes;
- ✓ Cuando proceda, medidas adoptadas por el Auditado tras la auditoría; y
- ✓ Plazo para el informe final y para el plan de medidas correctivas.

V. Presentación de informes

El informe provisional y el definitivo deberán ser remitidos por el equipo auditor al Director de la DNS para su correspondiente aval.

Una vez avalados, el Director de DNS remitirá al Auditado en el momento oportuno el informe provisional o definitivo correspondiente.

Los informes de auditoría de protección deberán tener en cuenta los siguientes principios:

- Las conclusiones indicadas en la sesión de clausura de la auditoría, del informe provisional y del informe final han de ser coherentes entre sí;
- Las conclusiones han de estar respaldadas por pruebas objetivas;
- Las conclusiones han de exponerse de forma clara y concisa;
- Han de evitarse las generalidades y las expresiones vagas;
- Las conclusiones de la auditoría han de presentarse de forma objetiva;
- Ha de evitarse la crítica de personas o puestos.
- El equipo auditor tratará confidencialmente toda la información recopilada, los materiales, notas e informes obtenidos o elaborados durante la auditoría.

A. Informe provisional de auditoría

Este informe es un mecanismo de fortalecimiento de la calidad de los informes finales y no constituye un acto formal de la DNS. El informe provisional establece la base para la preparación del informe final de auditoría, que lo sustituirá cuando esté listo.

El Auditado deberá realizar las observaciones que considere pertinentes sobre el contenido del informe provisional, en un plazo no mayor a cinco días hábiles, aportando el sustento documental pertinente.

El contenido del informe provisional deberá ser el siguiente:

- Resumen ejecutivo
- Introducción
- Objetivo y alcance de la auditoría
- Generalidades acerca de la auditoría
- Metodología aplicada
- Cuando aplique, fecha y participantes en la sesión de clausura
- Resultados (Observaciones e incumplimientos)
- Conclusiones
- Posibles recomendaciones para medidas de seguimiento
- Apéndices y Anexos.

Tanto el Auditado como el equipo auditor harán lo posible para evitar cualquier desacuerdo acerca de las conclusiones de la auditoría. En cualquier fase, el Auditado debe notificar al equipo auditor cualquier preocupación respecto de la validez y/o interpretación de las conclusiones de la auditoría. Las divergencias sobre las conclusiones de la auditoría entre el equipo auditor y el Auditado deberán analizarse y, de ser posible, resolverse.

B. **Informe final de auditoría**

El informe final de auditoría constituye el pronunciamiento oficial de la auditoría. Su estructura y contenido deberán ser similares a los del informe provisional.

VI. Plan de medidas correctivas

El plan de medidas correctivas que debe presentar el Auditado deberá estar basado en el informe final de auditoría.

Deberán adoptarse las medidas correctivas que sean necesarias y en plazos definidos para cada una de las conclusiones de la auditoría. El conjunto de estas medidas constituye el plan de medidas correctivas.

Dicho plan deberá proporcionar información pormenorizada de las medidas que haya que adoptar, incluido el plazo de tiempo para el comienzo y la finalización de cada medida.

El plan de medidas correctivas deberá presentarse al Director de la DNS para su revisión y aprobación. El Auditado tendrá un plazo de 10 días hábiles a partir de la fecha de recepción del informe final de auditoría para la presentación del plan de medidas correctivas. En casos excepcionales mediante solicitud formal del Auditado ante el Director de la DNS, se podrá conceder una prórroga.

VII. Registro y seguimiento

La DNS deberá mantener registros de todas las auditorías realizadas. Tales registros deberán incluir, entre otras cosas, lo siguiente:

- los informes provisionales;
- los informes finales de auditoría; y
- Formularios de registro de auditoría (Anexo 1).

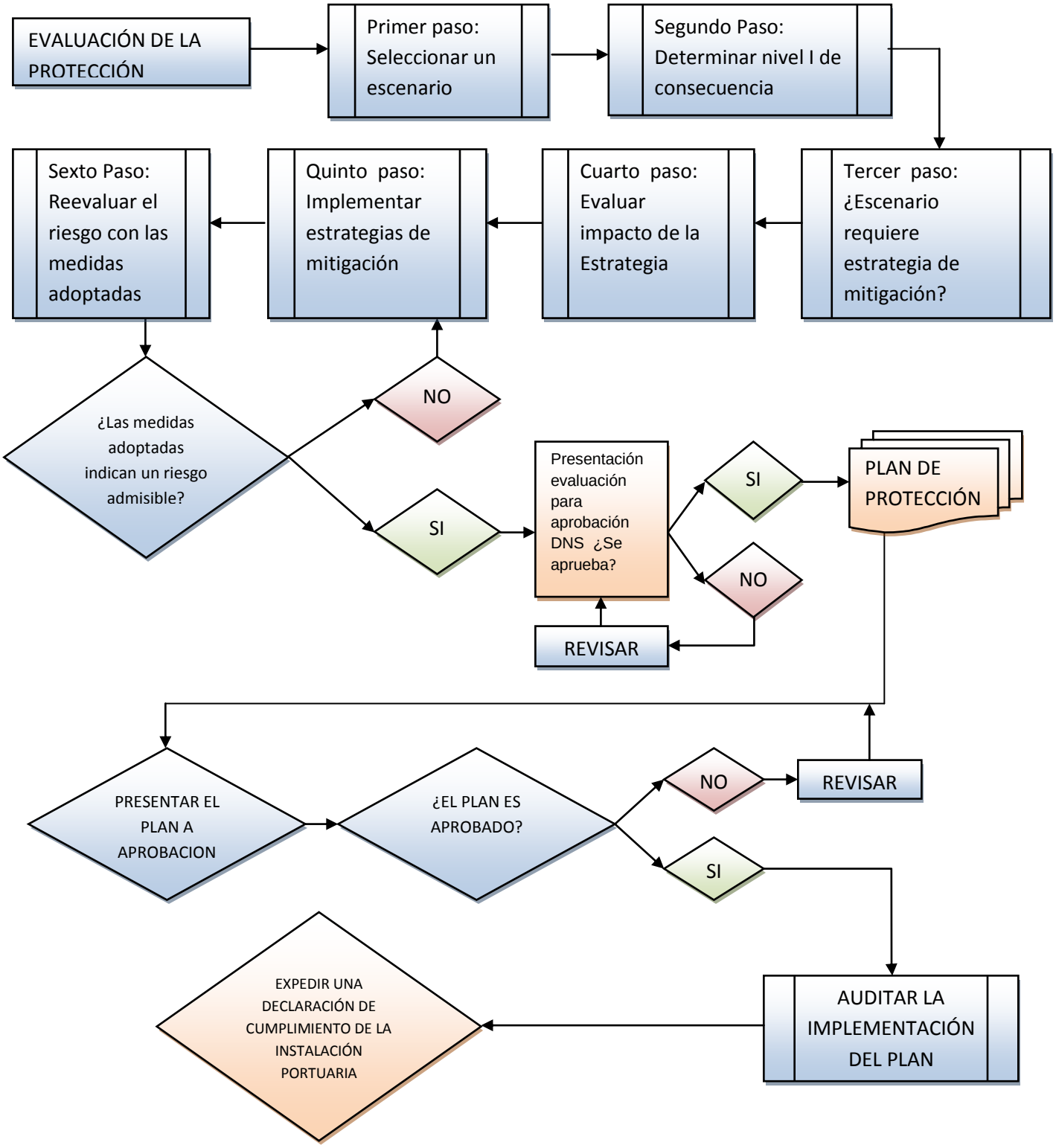
Si procede, después de haberse realizado la auditoría de una Instalación Portuaria, deberá efectuarse un seguimiento de la misma para así determinar el grado de implantación del plan de medidas correctivas.

Los procedimientos normalizados de auditoría que han de aplicarse a la labor de seguimiento son los mismos que los de las auditorías normales que se describen en el presente documento. La única excepción es la diferencia que existe en el alcance, ya que el seguimiento de una auditoría deberá estar limitado a los aspectos que se determine durante la auditoría inicial que deberán mejorarse o seguir supervisándose.

El equipo de seguimiento de una auditoría estará formado normalmente por un jefe del equipo auditor y otros auditores en un número que variará, dependiendo del alcance de la auditoría. De ser posible, como mínimo, uno de los miembros del equipo auditor para el seguimiento de una auditoría deberá haber pertenecido al equipo auditor original.

DIAGRAMA DE FLUJO DEL PROCESO DE CERTIFICACIÓN

El presente diagrama es solo una guía, en todos los casos se deberá de referenciar a la norma, SOLAS XI-2, Código PBIP o el presente manual.



10. DECLARACIÓN DE CUMPLIMIENTO DE LA INSTALACIÓN PORTUARIA

1. Cumplido con el proceso de Certificación previsto en el DIAGRAMA DE FLUJO DEL PROCESO DE CERTIFICACIÓN, la DNS expedirá una Declaración del Cumplimiento de la Instalación Portuaria, acorde al MODELO DE DECLARACIÓN DE CUMPLIMIENTO DE INSTALACIÓN PORTUARIA.

2. Otorgada una Declaración del Cumplimiento de una Instalación Portuaria, la DNS, asentará dicha información en la página que, a sus efectos posee la Organización Marítima Internacional (OMI).

3. La Declaración del Cumplimiento de la Instalación Portuaria expida por la DNS, podrá tener una validez hasta por 5 (cinco) años, pero no excederá este plazo. La validez de la misma estará sujeta a una verificación obligatoria anual o las verificaciones no anunciadas.

4. Una vez aprobada la verificación anula obligatoria o las verificaciones no anunciadas, la DNS procederá a refrendar la Declaración de Cumplimento, en los espacios que para tal efecto están en la parte posterior de la Declaración misma.

MODELO DE DECLARACIÓN DE CUMPLIMIENTO DE INSTALACIÓN PORTUARIA

MINISTERIO DE OBRAS PÚBLICAS Y TRANSPORTES
DIRECCIÓN DE NAVEGACIÓN Y SEGURIDAD
REPÚBLICA DE COSTA RICA

DECLARACIÓN DE CUMPLIMIENTO DE INSTALACIÓN PORTUARIA

Nº de la declaración**:** *<insertar número>*

Expedida en virtud de las disposiciones de la Parte B del
CÓDIGO INTERNACIONAL PARA LA PROTECCIÓN DE LOS BUQUES Y DE LAS INSTALACIONES PORTUARIAS (CÓDIGO PBIP)

El Gobierno de la **REPÚBLICA DE COSTA RICA**

Nombre de la instalación portuaria	Puerto Número, IMO	Código Localización	Dirección de la instalación portuaria
<insertar nombre de la instalación>	*<insertar número IMO o UN>*	*<insertar código de localización>*	*<incluir costa o litoral>*
			<incluir Provincia>
			<incluir Cantón>
			<incluir Coordenada geográfica latitud>
			<incluir Coordenada geográfica longitud>

CERTIFICA: que se ha efectuado la verificación del cumplimiento de las disposiciones del Capítulo XI-2 y de la parte A del Código internacional para la protección de los buques y de las instalaciones portuarias (Código PBIP) por parte de esta instalación portuaria y que satisfactoriamente se observa el Plan de Protección de la Instalación Portuaria que le ha sido **APROBADO** para lo siguiente:

Buque de pasaje
Granelero
Petrolero
Quimiquero
Gasero
Buques de carga distintos de los anteriores

<tachar lo que no corresponde>

Nota: El Código PBIP implementado mediante el Decreto Ejecutivo N° 31845-MOPT de fecha 18 de junio del 2004 (Reglamento para la Protección de los Buques y de las Instalaciones Portuarias). La adhesión de la República de Costa Rica al Convenio Internacional para la Seguridad de la Vida Humana en el Mar, 1974, sus protocolos y sus enmiendas (SOLAS 74), fue ratificada mediante la Ley N° 8708 del 23 de diciembre de 2010.

La presente Declaración de Cumplimiento es válida hasta el <*incluir fecha*>, a reserva lo indicado en el oficio <*incluir número de oficio*> de la Dirección de Navegación y Seguridad y de las pertinentes verificaciones (indicadas al dorso).

Expedida en *San José, Costa Rica***,** <*incluir fecha*>

<*incluir firma*> <*incluir sello*>

Ing. Jorge Hernández Chavarría
Director
Dirección de Navegación y Seguridad

REFRENDO DE LAS VERIFICACIONES

El Gobierno de *Costa Rica* ha establecido que la validez de la presente declaración de cumplimiento este´ sujeta a *<insertar los datos pertinentes de las verificaciones (por ejemplo, una verificación obligatoria anual o una verificación no programada)>.*

SE CERTIFICA que durante una verificación efectuada de conformidad con el párrafo B/16.62.4 del Código PBIP se ha comprobado que la instalación portuaria cumple las prescripciones pertinentes del capítulo XI-2 del Convenio y de la parte A del Código PBIP.

1a VERIFICACIÓN Firmado: . . . . . .

(firma del funcionario autorizado)

Lugar: . . . . . .

Fecha: . . . . . .

2a VERIFICACIÓN Firmado: . . . . . .

(firma del funcionario autorizado)

Lugar: . . . . . .

Fecha: . . . . . .

3a VERIFICACIÓN Firmado: . . . . . .

(firma del funcionario autorizado)

Lugar: . . . . . .

Fecha: . . . . . .

4a VERIFICACIÓN Firmado: . . . . . .

(firma del funcionario autorizado)

Lugar: . . . . . .

Fecha: . . . . . .

MINISTERIO DE OBRAS PÚBLICAS Y TRANSPORTES
DIRECCION DE NAVEGACIÓN Y SEGURIDAD
REPÚBLICA DE COSTA RICA

STATEMENT OF COMPLIANCE OF PORT FACILITY

Statement Number: *<insertar número>*

Issued under the provisions of Part B of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES (ISPS CODE)

The Government of **REPUBLIC OF COSTA RICA**

Name of the port facility	Port ID Number, IMO	Locator Code	Address of the port facility
<insertar nombre de la instalación>	*<insertar número IMO o UN>*	*<insertar código de localización>*	*<incluir costa o litoral>*
			<incluir Provincia>
			<incluir Cantón>
			<incluir Coordenada geográfica latitud>
			<incluir Coordenada geográfica longitud>

THIS IS THE CERTIFY that the compliance of this port facilities with the provisions of chapter XI-2 and part A of the International Code for the Security of Ships and Port Facilities (ISPS CODE) has been verified and that this port facility operates in accordance with the **APPROVED** Port Facility Security Plan. This plan has been **APPROVED** for the following.

Passenger ship
Bulk carrier
Oil tanker
Chemical tanker
Gas carrier
Cargo ships other than those referred to above

<tachar lo que no corresponde>

Note: The ISPS Code was implemented by Executive Decree No. 31 845-MOPT dated June 18, 2004 (Regulations for the Protection of Ships and Port Facilities). The accession of the Republic of Costa Rica to the International Convention for the Safety of Life at Sea, 1974, its protocols, as amended (SOLAS 74), was ratified by Law No. 8708 of December 23, 2010.

THIS STATEMENT OF COMPLIANCE applies from <*incluir fecha*>, and is valid until <*incluir fecha*>*,* to reservation of the indicated in the office <*incluir número de oficio*> of the Direction of Navigation and Safety and subject to the pertinent checks.

Issued at San José, Costa Rica**,** <*incluir fecha*>

<*incluir firma*> <*incluir sello*>

Ing. Jorge Hernández Chavarría
General Manager
Direction of Navigation and Safety

ENDORSEMENT FOR VERIFICATIONS

The Government of *Costa Rica* has established that the validity of this Statement of Compliance is subject to *<insertar los datos pertinentes de las verificaciones (por ejemplo, una verificación obligatoria anual o una verificación no programada)>*.

THIS IS TO CERTIFY that, during a verification carried out in accordance with paragraph B/16.62.4 of the ISPS Code, the port facility was found to comply with the relevant provisions of chapter XI-2 of the Convention and Part A of the ISPS Code.

1st VERIFICATION

Signed: .....

(Signature of authorized official)

Place: .....

Date: .....

2nd VERIFICATION

Signed: .....

(Signature of authorized official)

Place: .....

Date: .....

3rd VERIFICATION

Signed: .....

(Signature of authorized official)

Place: .....

Date: .....

4th VERIFICATION

Signed: .....

(Signature of authorized official)

Place: .....

Date: …….

11. DECLARACIÓN DE PROTECCIÓN MARÍTIMA

El DNS determinará cuándo se requiere una Declaración de Protección Marítima (DPM), generalmente situaciones de alto riesgo, mediante la evaluación del riesgo que una operación de interfaz buque-puerto o una actividad de buque a buque supongan para las personas, los bienes o el medio ambiente. Esto con el objetivo de garantizar que el buque y la IP, u otros buques con los que realice operaciones de interfaz, lleguen a un acuerdo sobre las medidas de protección y responsabilidades que cada uno de ellos va adoptar, de conformidad con las disposiciones de sus respectivos planes de protección aprobados.

La necesidad de una DPM puede desprenderse de los resultados de una EPIP. Por otro lado, la práctica con respecto a la solicitud, o la respuesta a solicitudes de la misma, además de las razones y las circunstancias en las que se requiere una DPM, debe figurar en el PPIP.

La DPM acordada debe ir firmada y fechada tanto por la IP como por el buque o los buques, según sea el caso, y en ellas debe quedar constancia del cumplimiento de lo dispuesto en el capítulo XI-2 y en la Parte A del Código PBIP. Se debe especificar el periodo de vigencia de la DPM y el nivel o niveles de protección pertinentes, así como los datos de contacto correspondientes.

En lo que respecta a la firma, a petición del buque, de una DPM cuando se establezca contacto con una IP o el buque no esté cubierto por un plan de protección, se debe considerar que en lo que respecta a la IP no cubiertas por las reglas, el estado tendrá que asegurar que se disponga de un punto de contacto en tierra con el que el buque pueda comunicarse y que tenga autoridad para firmar la DPM, en tanto que para el buque no cubierto por el plan de protección debería haber igualmente un punto de contacto designado en tierra o en el buque autorizado para firmar dicha declaración.

En caso de que el nivel de protección cambie, puede ser necesario revisar la DPM o elaborar una nueva.

La DPM debe redactarse en español o inglés, o en un idioma común a la IP y al buque o buques, según sea el caso.

En virtud de la sección A/5.2 del Código PBIP, los buques pueden solicitar que se cumplimente una declaración de protección marítima cuando:

1.1 El buque funcione a un nivel de protección más elevado que la instalación portuaria u otro buque con el que esté realizando una operación interfaz.

1.2 Exista un acuerdo sobre la DPM entre los Gobiernos Contratantes que regule determinados viajes internacionales o buques específicos en dichos viajes.

1.3 Se haya producido una amenaza o un suceso que afecte a la protección marítima relacionado con el buque o con la instalación portuaria, según sea el caso.

1.4 El buque se encuentre en un puerto en el que no esté obligado a tener e implantar un plan de protección de la instalación portuaria aprobado.

1.5 El buque esté llevando a cabo actividades de buque a buque con otro buque que no esté obligado a tener e implantar un plan de protección del buque aprobado.

La DNS especificará, teniendo en cuenta las disposiciones de la regla XI-2/9.2.3m, el período mínimo por el que las IP situadas dentro de su territorio deberán conservar las DPM.

Las Administraciones especificarán, teniendo en cuenta las disposiciones de la regla XI-2/9.2.3m, el período mínimo por el que los buques con derecho a enarbolar su pabellón deberán conservar las DPM.

Solicitud de una DPM

- La solicitud o la respuesta a solicitudes de la misma, debe figurar en el plan de protección de la instalación portuaria (PPIP) y la correspondiente a la solicitud de una DPM, en el plan de protección del buque (PPB).
- Toda DMP tendrán el acuse de recibo de la correspondiente IP o buque.
- En el caso de que un buque o una Administración, en representación de los buques con derecho a enarbolar su pabellón, soliciten una DPM, el OPIP o el OPB son los llamados a dar acuso recibo de la solicitud y examinar las medidas de protección oportunas.
- Si bien un buque debe dar cumplimiento a la solicitud cursada por una IP de cumplimentar una DPM, una IP no tiene por qué dar cumplimiento a la solicitud cursada por un buque de que se cumplimente una DPM. De igual manera, otro buque no tiene que dar cumplimiento a una solicitud de DPM.

Incumbirá Cumplimentar la DPM

- En el caso de los buques, al capitán o al OPB, y si procede
- En caso de la IP, al OPIP o si la DNS determina otra cosa, a cualquier otro organismo responsable de la protección en tierra.

Orientaciones para el llenado de la DPM

A efectos de brindar una orientación para el llenado de la DPM se deberá tener en cuenta los siguientes parámetros:
(1) Se anotará los nombres de los buques que operarán en la actividad buque – buque o eventualmente el nombre de la Instalación portuaria (IP) cuando se efectúen operaciones de interfaz buque – puerto.
(2) Se anotará el puerto de matrícula de cada uno de los buques.
(3) Sea notará el número IMO asignado a cada uno de los buques.
(4) Se anotará la fecha de inicio y finalización de las operaciones de actividad buque – buque /interfaz buque – puerto.
(5) Se detallarán las operaciones a llevar a cabo (embarque de contenedores, embarque de pasajeros, top off, operaciones de alijo, etc.).
(6) Se anotarán los niveles de protección en que operan cada uno de los buques o en su defecto buque e instalación portuaria.
(7) Se anotarán las iniciales del OPB u OPIP bajo estas columnas indicando al responsable de las instrucciones o procedimientos desarrollados al efecto.
(8) Se anotarán el lugar (puerto / rada / etc.) y fecha en que se confecciona la DPM.
(9) Los responsables de la protección tanto a bordo, como en la Instalación portuaria, deberán insertar su firma como responsables directos del cumplimiento de las actividades a desarrollar.

(10) Se insertarán los nombres y cargos de los firmantes en (9).
(11) Se establecerá la información de contacto necesaria para garantizar la ubicación del personal relevante en protección durante las actividades de protección.
(12) En este campo “Observaciones” se hará referencia a la identificación de las instrucciones / procedimientos que respaldan las actividades relacionadas con la protección que se desarrollan.

MODELO No. 1 DE DECLARACIÓN DE PROTECCIÓN MARÍTIMA (DPM)

Nombre del buque 1 (1):	
Puerto de matrícula (2):	
Número IMO (3):	
Nombre del buque 2 (1):	
Puerto de matrícula (2):	
Número IMO (3):	

La presente declaración de protección marítima es válida del……..…..al……., para las siguientes actividades: (5)

.....

(enumerar las actividades, con los datos pertinentes)

Con arreglo a los siguientes niveles de protección

Nivel(es) de protección del buque (1):	(6)
Nivel(es) de protección del buque (2):	(6)

La instalación portuaria y el buque acuerdan las siguientes medidas y responsabilidades en la esfera de la protección con el fin de garantizar el cumplimiento de lo prescrito en la Parte A del Código internacional para la protección de los buques y de las instalaciones portuarias.

	La inclusión de las iniciales del OPB bajo estas columnas indica que la actividad será realizada, de conformidad con el pertinente plan aprobado, por:	
Actividad	Buque 1 (7)	Buque 2 (7)
Garantías de que se realizan todas las tareas de protección		
Vigilancia de las zonas restringidas para garantizar que sólo tiene acceso a ellas personal autorizado		
Control de los accesos al buque 1		

Control de los accesos al buque 2		
Vigilancia del buque, incluidas las zonas de atraque y los alrededores del buque 1		
Vigilancia del buque, incluidas las zonas de atraque y los alrededores del buque 2		
Manipulación de la carga		
Entrega de las provisiones del buque		
Control del embarco de personas y sus efectos		
Aseguramiento que se pueden establecer con facilidad comunicaciones de protección entre los buques		

Los firmantes del presente acuerdo certifican que las medidas de protección de los buques, durante las actividades especificadas, se ajustan a lo dispuesto en el capítulo XI-2 y en la Parte A del Código que se implantarán de conformidad con las disposiciones ya estipuladas en su plan aprobado o en las medidas específicas acordadas y establecidas en el anexo adjunto.

Lugar (8) y
Fecha:.....(8).....

Firmado en Nombre de (09):	
Buque 1:	Buque 2:
(Firma del Capitán o del oficial de protección del buque)	(Firma del Capitán o del oficial de protección del buque)

Nombre y cargo de los firmantes (10)	
Nombre:	Nombre:
Cargo:	Cargo:

Datos de contacto (11) ***(Cumpliméntese según corresponda)*** ***(indíquese los números de teléfono o los canales o frecuencias que se deben utilizar)***	
Buque 1:	**Buque 2:**
Capitán	Capitán
Oficial de protección del buque	Oficial de protección del buque
Compañía	Compañía
Oficial de la Compañía para la protección marítima	Oficial de la Compañía para la protección marítima

OBSERVACIONES (12)

MODELO N° 2 DECLARACIÓN DE PROTECCIÓN MARÍTIMA

Nombre del buque:	
Puerto de matrícula:	
Número IMO:	
Nombre de la Instalación Portuaria:	

La presente declaración de protección marítima es válida del……..…..al……., para las siguientes actividades:

.....

(enumerar las actividades, con los datos pertinentes)

Con arreglo a los siguientes niveles de protección

Nivel(es) de protección del buque:	
Nivel(es) de protección de la Instalación Portuaria:	

La instalación portuaria y el buque acuerdan las siguientes medidas y responsabilidades en la esfera de la protección con el fin de garantizar el cumplimiento de lo prescrito en la Parte A del Código internacional para la protección de los buques y de las instalaciones portuarias.

	La inclusión de las iniciales del OPB o del OPIP bajo estas columnas indica que la actividad será realizada, de conformidad con el pertinente plan aprobado, por:	
Actividad	La Instalación Portuaria	Buque
Garantías de que se realizan todas las tareas de protección		
Vigilancia de las zonas restringidas para garantizar que sólo tiene acceso a ellas personal autorizado		
Control de los accesos a la Instalación Portuaria		
Control de los accesos al buque		

Vigilancia de la Instalación Portuaria, incluidas las zonas de atraque y las adyacentes al buque		
Vigilancia del buque, incluidas las zonas de atraque y los alrededores del buque		
Manipulación de la carga		
Entrega de las provisiones del buque		
Control del embarco de personas y sus efectos		
Aseguramiento que se pueden establecer con facilidad comunicaciones de protección entre los buques		

Los firmantes del presente acuerdo certifican que las medidas de protección de la Instalación Portuaria y del buque, durante las actividades especificadas, se ajustan a lo dispuesto en el capítulo XI-2 y en la Parte A del Código que se implantarán de conformidad con las disposiciones ya estipuladas en su plan aprobado o en las medidas específicas acordadas y establecidas en el anexo adjunto.

Lugar (8) y Fecha:.....

Firmado en Nombre de:	
La instalación portuaria	El buque
(Firma del oficial de protección de la Instalación Portuaria)	(Firma del Capitán o del oficial de protección del buque)

Nombre y cargo de los firmantes	
Nombre:	Nombre:
Cargo:	Cargo:

Datos de contacto
(Cumpliméntese según corresponda)

(indíquese los números de teléfono o los canales o frecuencias que se deben utilizar)	
Instalación Portuaria	**Buque:**
Instalación Portuaria	Capitán
Oficial de protección de la instalación portuaria	Oficial de protección del buque
	Compañía
	Oficial de la Compañía para la protección marítima

OBSERVACIONES

12. FUNCIONES, OBLIGACIONES Y REQUISITOS PARA LA INSCRIPCIÓN Y HABILITACIÓN DEL OFICIAL DE PROTECCIÓN DE LA INSTALACIÓN PORTUARIA (OPIP)

El OPIP es la persona designada para asumir la responsabilidad de la elaboración, implantación, revisión y actualización del plan de protección de la instalación portuaria, y para la coordinación con los oficiales de protección de los buques y con los oficiales de protección de las compañías para la protección marítima.

La instalación portuaria debe designar un oficial de protección para cada instalación portuaria. Una misma persona podrá ser designada OPIP de más de una instalación siempre y cuando la distancia entre las mismas no sea superior a 10 km, el mismo tendrá el apoyo necesario para que pueda desempeñar las funciones y responsabilidades que se le imponen.

12.1. Obligaciones y responsabilidades

Las obligaciones y responsabilidades del OPIP incluirán las siguientes tareas, sin que esta enumeración sea exhaustiva.

1- Llevar a cabo una evaluación inicial y general de la instalación portuaria, tomando en consideración la oportuna evaluación de la protección de la instalación portuaria, a fin de elaborar un plan de protección de la instalación portuaria.

2- Elaborar, implantar y perfeccionar el plan de protección de la instalación portuaria.

3- Inspeccionar periódicamente el estado de protección de la instalación portuaria y realizar prácticas para asegurarse que se han tomado las medidas de protección adecuadas.

4- Recomendar, e incluir, según proceda, modificaciones en el plan de protección de la instalación portuaria a fin de subsanar deficiencias y actualizarlo, tomando en consideración los cambios que haya habido en la instalación portuaria.

5- Fomentar la toma de conciencia en cuanto a la protección y la vigilancia entre el personal de la instalación portuaria.

6- Garantizar la formación adecuada del personal responsable de la protección de la instalación portuaria.

7- Notificar a las autoridades pertinentes y llevar registros de los sucesos que suponen una amenaza para la protección de la instalación portuaria.

8- Coordinar la implantación del plan de protección de la instalación portuaria con los oficiales de protección del buque y de la compañía.

9- Establecer los mecanismos de coordinación con la DNS y otras autoridades gubernamentales pertinentes.

10- Garantizar que se cumplen las normas relativas al personal responsable de la protección de la instalación portuaria.

11- Garantizar el funcionamiento, prueba, ajuste y mantenimiento adecuados del equipo de protección, si lo hay.

12 -Ayudar a los oficiales de protección del buque a confirmar la identidad de las personas que tratan de subir a bordo, cuando así se requiera.

Se ha de dar al OPIP el apoyo necesario para que pueda desempeñar las funciones y responsabilidades que se le imponen en el capítulo XI-2 SOLAS y parte A código PBIP.

12.2. Requisitos de inscripción

Los requisitos para inscribirse como OPIP y los suplentes son los siguientes:

1. Presentar la solicitud de inscripción como OPIP ante la DNS;
2. Ser ciudadano costarricense, con dos años de residencia efectiva en el país, mayor de treinta años;
3. Poseer título universitario expedido por una institución de educación reconocida por CONESUP o CONARE, y experiencia comprobada en el desempeño de tareas desarrolladas en ámbitos portuarios que avalen su idoneidad para el ejercicio de la función (presentar constancias laborales);
4. Estar incorporado y al día en los pagos por concepto de colegiatura del colegio profesional respectivo;
5. Acreditar mínimo 3 años de experiencia en cargos relacionados con la operación de puertos y/o gestión de la seguridad de los mismos o título de especialización o posgrado en gerencia o manejo de sistemas de gestión o en seguridad;
6. Aprobar los cursos modelo OMI 3.19, 3.20 y 3.21 en protección marítima y demás cursos y conocimientos que estime oportuno la DNS;
7. Deseable, acreditar conocimientos del idioma inglés técnico normalizado OMI;
8. No poseer ningún impedimento o inhabilidad constitucional o legal y/o sanción profesional;
9. Estar exentos de impedimentos o inhabilitaciones dispuestos por autoridad judicial competente, debiendo el interesado adjuntar informe de antecedentes penales, expedido por el Poder Judicial, no mayor a quince días a la fecha de presentación;
10. Conocer el uso de las comunicaciones para operaciones mínimas de seguridad acorde equipos de la terminal;
11. Acreditar aptitud psíquica (psicológica) para el desempeño de la función, mediante la correspondiente certificación médica otorgada por un profesional de la especialidad.

12.3. Habilitación

1. Cumplida las exigencias reglamentarias correspondientes la DNS emitirá la disposición para la habilitación del OPIP.
2. La validez del certificado de habilitación será anual, a partir de la fecha de emisión y sujeta al mantenimiento de las condiciones de otorgamiento.

12.4. Registro

La DNS mantendrá un registro de los OPIP habilitados.

12.5. Revalidación de la Habilitación

1. Las renovaciones anuales se efectuarán dentro de los 30 días hábiles antes de la fecha del vencimiento.
2. Los OPIP registrados que no soliciten en término la renovación anual de su habilitación quedarán automáticamente eliminados del registro.
3. La habilitación es intransferible.

12.6. Inhabilitación

1. Será motivo de inhabilitación y eliminación del registro correspondiente:
    - No mantener las condiciones exigidas para la habilitación.
    - No contar con los cursos recomendados por la DNS para mantener vigente la habilitación.
    - No renovar anualmente la inscripción.

Para designar a un OPIP, la empresa interesada deberá constatar previamente que dicha persona cuenta con el perfil y los atestados pertinentes, y solo después de ello, con la documentación que lo compruebe se procederá a solicitar ante la DNS que sea acreditado como OPIP.

La DNS revisará que el aspirante efectivamente cumpla con los requisitos para fungir como OPIP del operador portuario, conforme a lo señalado en el Reglamento de esta materia, de ser procedente o autorizado, dentro de un plazo de quince días hábiles lo acreditará como OPIP.

13. MANEJO DE DOCUMENTACIÓN

Garantizar la protección de la información confidencial contenida en la evaluación y en el plan sea en papel o en formato electrónico. El EPIP y el PPIP podrá mantenerse en formato electrónico, en tal caso estará protegido mediante procedimientos destinados a evitar que se borre, destruya o altere sin autorización. Al mismo tiempo, se protegerá contra acceso o divulgación no autorizados.

El presente instructivo tiene por objeto señalar pautas para la confección de las evaluaciones y los planes de protección de las instalaciones portuarias, con el propósito de estandarizar su clasificación y cantidad de ejemplares, evitando reproducción no autorizada:

a) Clasificación de la documentación:
   i) Evaluaciones de Protección: Secreto
   ii) Planes de Protección: Reservado

b) Cantidad de ejemplares:
   i) Evaluaciones de Protección: 3 ejemplares
   ii) Planes de Protección: 3 ejemplares

c) Distribución de ejemplares relativos a las instalaciones portuarias:
   i) Evaluaciones de Protección:

      - Ejemplar N° 1: Administración Marítima
      - Ejemplar N° 2: Operador portuario
      - Ejemplar N° 3: OPIP

   ii) Planes de Protección:

      - Ejemplar N° 1: Administración Marítima
      - Ejemplar N° 2: Operador portuario
      - Ejemplar N° 3: OPIP

d) De la documentación:

   i) La correspondencia Secreta y Reservada podrá ser abierta únicamente por aquellas personas que tengan “Autorización escrita” para ello.

   ii) Las Evaluaciones y Planes de Protección, que por su naturaleza deben ser conocidos solamente por el remitente y el destinatario, se clasificarán como “Personal” además de la clasificación indicada anteriormente.

   iii) Todo documento Secreto o Reservado deberá tener además del número de ejemplar y de hoja en el margen superior derecho, el número del ejemplar

estampado en el centro de la página, mediante el empleo de marcas de agua de color rojo (10 cm de alto por 5 cm de ancho).

iv) Toda la documentación Secreta o Reservada deberá llevar un membrete en la parte superior izquierda, timbrado o sello blanco de quien realizó la Evaluación y/o Plan de Protección.

e) Envío de la documentación.

i) La documentación “Secreta” y “Reservada” que será tramitada, y remitida a la Dirección de Navegación Seguridad y deberá ser entregada y recibida mano a mano por personal autorizado.

ii) Se deberá usar doble sobre para la correspondencia Secreta y Reservada. En el sobre interior se indicará la clasificación, ejemplar y número de hojas.

iii) En el sobre exterior no se hará mención del documento sino que, se mencionará solamente el “Acuse de Recibo” que debe ir entre ambos sobres.

iv) De toda la documentación “Secreta” deberá darse “Acuse de Recibo”, el cual consistirá en una hoja de clasificación Ordinaria y se despachará junto con la documentación, en dos copias (una de las cuales deberá ser devuelta firmada al remitente, una vez reciba la documentación).

v) De no recibir el emisor el acuse de recibo dentro de un plazo de 15 días posterior al envío del documento, dicho emisor deberá cerciorarse que éste no se haya extraviado.

13.1. MANEJO DE DOCUMENTACIÒN DIGITAL

La DNS contará con un espacio específico como por ejemplo un gabinete seguro e incombustible para guardar la documentación en formato digital y encriptado, la información digital podrá estar contenida en discos compactos (CD), disco versátil digital (DVD), dispositivos de memoria USB u otros; al cual solamente tendrán acceso las personas autorizadas.

Políticas para salvaguardar la información:

Los funcionarios con acceso a la información digital, podrán hacer uso del equipo de cómputo necesario para poder visualizar el contenido siempre y cuando sigan las políticas para salvaguardar la información.

Políticas de escritorios y pantallas limpios

1. Se debe guardar bajo llave los EPIP y PPIP y documentación anexa en un gabinete incombustible.

2. Al utilizar una notebook, tablet o laptop se deberá mantener en un lugar seguro para evitar hurtos o robos.

3. Los dispositivos de almacenamiento masivo externos y removibles con información reservada o secreta como lo son de los EPIP y PPIP no deben dejarse en lugares visibles y accesibles.

4. No se debe dejar accesibles documentos impresos que contengan datos confidenciales.

5. Deje su lugar de trabajo en orden, apague los equipos y guarde los documentos al finalizar la jornada laboral.

6. Cierre la sesión al ausentarse o dejar de utilizar un sistema informático.

7. Si debe abandonar, aunque sea momentáneamente, su puesto de trabajo, bloquee su terminal con un protector de pantalla que solicite el ingreso de una clave.

8. Carpetas compartidas

   •Establezca contraseñas robustas en las carpetas compartidas a través de la red y cámbielas periódicamente.

   •No comparta todo el disco de la computadora.

   •Distribuya la información a compartir en distintas carpetas.

9. Traslado de información crítica

   Todo traslado de información crítica debe realizarse de manera que se preserve la seguridad de la información:

   •Uso de sobres cerrados y firmados.

   •Entrega en mano al personal autorizado.

   •En caso de ser medios digitales, proteger los archivos con contraseña.

10. Eliminación segura

    La eliminación de los documentos constituye la fase final del ciclo de vida de un registro.

Los registros que contienen información privada o confidencial (por ejemplo, números de documento, EPIP, PPIP, etc.) requieren procedimientos de destrucción segura, que resguardan la privacidad y protegen contra el robo de identidad. Entre estos procedimientos se recomienda la eliminación utilizando equipamiento de destrucción de documentos.

La eliminación segura de la información crítica, ya sea que resida en un medio digital o en papel, impide obtener información mediante *trashing*, que es la práctica de recuperar información técnica o confidencial a partir de material descartado, y suele ser la manera de obtener datos para posteriormente cometer otros delitos (robo, intrusión en los sistemas de información u otros incidentes).

Las Personas Autorizadas que hayan tenido acceso a Información Privilegiada deberán destruir cualquier soporte que contenga esta información en el momento en el que haya dejado de ser útil, salvo que exista algún requisito, legal o de negocio, que justifique su mantenimiento. En este sentido, se deberá tener en cuenta no solo que han de destruirse versiones definitivas de los documentos confidenciales, sino también todos los borradores, copias, extractos y demás documentos de trabajo que contengan Información Privilegiada. Cuando resulte proporcionado y factible a criterio de la unidad o departamento de informática, los documentos confidenciales en formato electrónico deberán eliminarse utilizando una herramienta de borrado que garantice que la información eliminada es irrecuperable.

- *Trashing* físico: papeles o impresos descartados, diskettes, discos compactos, etc.

- *Trashing* lógico: contenido de la papelera de reciclaje, historial de sitios visitados, contraseñas almacenadas, etc.

11. Ingeniería social

•No responda preguntas sobre características de los sistemas. De ser necesario, derive la consulta a los responsables que tengan competencia para dar dicha información.

•Cerciórese de la identidad del interlocutor antes de brindar información sobre un sistema.

•Utilice el servicio técnico de confianza.

12. Resguardo de la información

El resguardo permite tener disponible e íntegra la información ante una contingencia.

•Realice copias periódicas de la información crítica y de trabajo diario.

•Guarde las copias en lugar seguro.

•Verifique la integridad física y lógica de los respaldos.

•Garantice la confidencialidad de los datos respaldados.

•Practique la reutilización segura de los medios.

13. Navegación en Internet

•Utilice un navegador seguro y con la configuración recomendada por el departamento de informática correspondiente.

•Evite acceder a sitios desconocidos o no confiables.

•No acepte la instalación automática de software.

•No descargue archivos de sitios web no confiables.

•Siempre descargue los archivos en una carpeta y analícelos con un antivirus actualizado antes de abrirlos.

•No ingrese información crítica o personal en formularios, páginas o foros.

•Si un sitio requiere que ingrese información crítica o personal sólo hágalo en sitios seguros (la dirección debe comenzar por https).

14. Código malicioso

El código malicioso o malware es software diseñado para infiltrarse en una computadora sin el conocimiento de su dueño con el fin de robar, dañar o eliminar el software y la información almacenada, o aprovechar los recursos de la misma para efectuar otras acciones maliciosas. El término código malicioso es una expresión general que engloba una variedad de formas de software o código hostil e intrusivo: virus informáticos, gusanos, troyanos, la mayoría de los rootkits y programas espía

•Utilice un antivirus reconocido, con la configuración recomendada por el departamento de informática correspondiente.

•Verifique que siempre esté activo y actualizado a la fecha.

•Analice siempre los medios removibles (discos, disquettes, pen-drives, mp3, celulares, cámaras digitales) que se conecten a la computadora.

•Ejecute un análisis completo (análisis en profundidad) del equipo al menos una vez por semana.

Envío y recepción de información secreta o reservada en formato digital

La información en formato digital seguirá las pautas enunciadas anteriormente para el envío de la documentación secreta o reservada, esta información previo al envío, será encriptada usando el software de encriptación suministrado o aprobado por la

Dirección de Informática del MOPT. La clave necesaria para desencriptar el archivo deberá ser conocida por las partes.

La clave utilizada para encriptar los archivos, no será enviada en el mismo sobre en el que se envía la información digital, deberá ser enviada previamente siguiendo las pautas para el envió y resguardo de la documentación secreta, la clave deberá ser cambiada periódicamente.

La documentación tal como oficios en formato digital que no se acompaña de su correspondiente documento físico con las firmas que le dan su validez, deberán ser remitidos con la firma digital correspondiente.

Anexo 1. Formulario de Registro de Auditoría

Registro de Auditoría
Confidencial una vez completado
Ver al reverso para obtener ayuda. Se pueden usar fotocopias de este documento. POR FAVOR, USE LETRA MAYUSCULA (cuando sea aplicable)

Auditado _____ página _____ de _____ Certificación N° _____ [4]

1. **Fecha** (día/mes/año)	2. **Duración de la auditoría (días)**		3. **Detalles de contacto de la Instalación Portuaria auditada** • nombre • dirección • persona de contacto • firma • teléfono/fax • email • tamaño de la organización (por ejemplo, cantidad de empleados)	4. **Nombre de los Auditores que participaron**	5. **Tipo de auditoría** Ver al reverso.	6. **Datos sobre el auditor líder que actuó como guía y supervisor:** • nombre • firma • teléfono/fax • email
	En sitio	Fuera del sitio				

[4] Anotar cuando sea asignado.

Registro de Auditoría
Confidencial una vez completado
Ver al reverso para obtener ayuda. Se pueden usar fotocopias de este documento. POR FAVOR, USE LETRA MAYUSCULA (cuando sea aplicable)

Columna 1	**Fecha:** Día, mes y año del primer día de la auditoría, comenzando con la reunión de apertura.
Columna 2	**Duración:** tiempo total de la auditoría en días (calculado al ½ día). Tiempo en el sitio: Tiempo transcurrido desde el inicio al fin de las actividades de examen en la instalación portuaria. Tiempo fuera del sitio: Tiempo utilizado en la preparación, planificación, análisis de documentos y elaboración del informe. Estas actividades pueden ser realizadas en el sito o fuera del sitio, pero en ambos casos son consideradas "fuera del sitio".
Columna 3	**Instalación Portuaria Auditada:** Esta sección debe responderse en su totalidad para permitirnos realizar la evaluación y verificación que corresponda. Si faltara alguna información, le pediremos que nos provea evidencias adicionales.
Columna 4	**Nombre de los Auditores que participaron:** Nombre de los auditores que participaron activamente en el equipo de auditoría.
Columna 5	**Tipo de auditoría:** De pre-certificación, certificación, de seguimiento o control, re-certificación, etc.
Columna 6	**Datos del auditor líder:** Los datos necesarios para contactar al auditor líder bajo cuya dirección y guía[1] se realizó la auditoría. El auditor líder debe ser competente[2]. [1]Dirección y guía no significa que Ud. debió estar bajo supervisión constante ni que haya habido una persona designada solamente para esta tarea. [2]Por competencia se entiende que tiene los atributos personales, descritos en el punto 8.2.1. "*Etapas del proceso de auditoría*" parte II del Manual para la aplicación del código PBIP en instalaciones y experiencia laboral, formación y experiencia en auditorías.