

**FORMATO GUÍA PARA LA EVALUACIÓN DE PROTECCIÓN DE
UNA INSTALACIÓN PORTUARIA DE ACUERDO AL CÓDIGO
I.S.P.S.**

I.	IDENTIFICACIÓN Y ANTECEDENTES DE LA INSTALACIÓN PORTUARIA	
A.	<u>IDENTIFICACIÓN:</u>	
1	Nombre Empresa	
2	Nombre Instalación Portuaria	
3	Rut	
4	Dirección	
5	Ciudad	
6	Latitud/Longitud Instalación Portuaria	
7	Teléfono	
8	Correo electrónico	
9	Concesión Marítima	

B.- INFORMACIÓN GENERAL DE LA INSTALACIÓN PORTUARIA

PROPIEDAD Y EJECUTIVOS.

Identificación y modo para ubicar a representante legal de la Instalación Portuaria y al Oficial de Protección de la Instalación Portuaria, en caso de urgencia.

ACTIVIDAD DE LA INSTALACIÓN PORTUARIA

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.

C.- INFORMACIÓN EXTERNA DE LA INSTALACIÓN PORTUARIA

ENTORNO.

1. Presentar plano de ubicación geográfica en que se demarquen los límites físicos de la instalación, vías de aproximación y acceso, ubicación de la Autoridad Marítima, cuarteles policiales, bomberos y servicios médicos. El plano debe ser confeccionado de manera de poder identificar de manera

clara y a simple vista lo requerido.

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

D.- INFORMACIÓN INTERNA DE LA ENTIDAD

INSTALACIONES.

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

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. Ramal de agua de bebida;
 - d. 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;
 - 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 ser: agua, electricidad, gas, teléfono, alcantarillado u otros, y su incidencia en las operaciones normales de la entidad.

II. GENERALIDADES

En la evaluación de protección de la instalación portuaria debe considerarse a lo 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 instalación portuaria.

III. IDENTIFICACIÓN Y EVALUACIÓN DE LOS BIENES E INFRAESTRUCTURAS QUE ES IMPORTANTE PROTEGER.

Establecer la importancia relativa de las distintas estructuras e instalaciones para el funcionamiento de la instalación portuaria.

En esta evaluación considerar el impacto que pueda causar una emergencia o atentado con consecuencia de pérdidas de vidas, paralización de actividades y daños de las zonas de importancia económica del puerto. Capacidades para restablecer los servicios que pudieren resultar dañados.

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, sistema de informática y redes de computadores;
4. Señalización Marítima dentro de las instalaciones portuarias.
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 instalación portuaria.

IV. 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.

Identificar 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. Habiendo determinado la vulnerabilidad, queda en evidencia las falencias 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 que para cada Instalación Portuaria en particular determine la Autoridad Marítima.

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

1. Daños o destrucción de una instalación portuaria 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.

V. 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 instalación portuaria 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

VI. 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;
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, en los informes sobre aspectos de protección preocupantes, al ejercer las medidas de control, al realizar una auditoria, etc.

VII. CONFECCIÓN DE TABLAS DE ANÁLISIS DE RIESGOS.

Con los antecedentes anteriores y de acuerdo a las indicaciones que se sugiere seguir en base al Anexo " A " adjunto, 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.

VIII. ANTECEDENTES QUE ACOMPAÑAN LA EVALUACIÓN:

IDENTIFICACIÓN DEL EVALUADOR.

Nombre:.....
RUT:.....
Cargo:.....
Empresa:.....
Fecha Evaluación:.....

IX. ANEXOS

ANEXO “ A “ : Guía para el Análisis de Riesgos en la Evaluación de la Protección en una Instalación Portuaria.

VALPARAÍSO,

**ÁREA DE PROTECCIÓN DE
INSTALACIONES PORTUARIAS
Servicio de Inspecciones Marítimas
Dirección de Seguridad y Operaciones
Marítimas**

ANEXO “A”

GUIA 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) de fecha 13 de Enero 2003 del Servicio de Guarda Costas de los Estados Unidos de Norte América.

La Toma de Decisiones Basada en Riesgo (RBDM) es una de las mejores herramientas para desarrollar y determinar las medidas apropiadas de Protección para una Instalación.

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

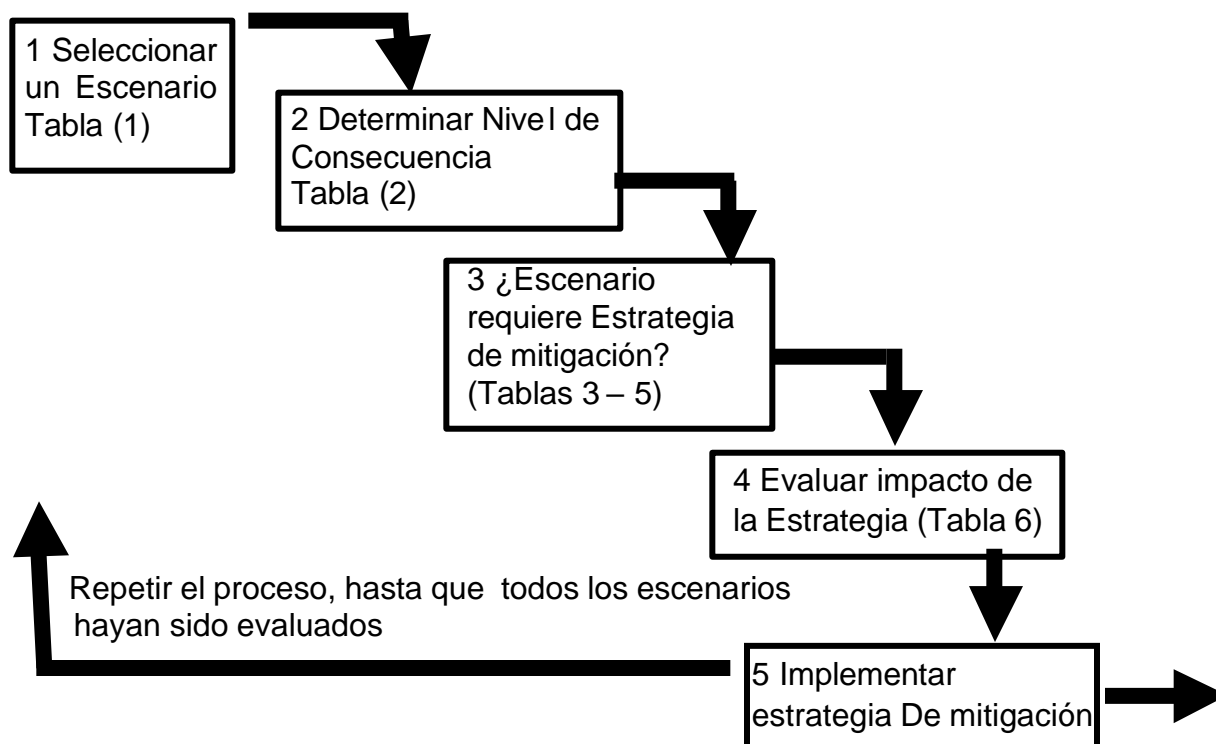
Una evaluación de protección es un proceso que identifica las debilidades en estructuras fijas, sistemas de protección personal, procesos u otras áreas que puedan conducir a una violación de protección y puede sugerir opciones para eliminar o mitigar esas debilidades.

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

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.

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

Diagrama de Flujo de una Evaluación de Protección Basada en Riesgo



Paso 1 – Amenazas Potenciales

Para comenzar una evaluación se necesita considerar escenario(s) de ataque que consiste en una amenaza potencial bajo circunstancia 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 1 entrega 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. Los escenarios típicos deben ser descritos en base a las probabilidades de ocurrencia y antecedentes previos y presentes, ajustados lo más posible a la realidad.

Tabla 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	Abre válvulas para derramar materiales tóxicos, o los ha traído consigo.
Toma rehenes / mata	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: <ul style="list-style-type: none"> - 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 protección Durante el transporte.

El número de escenarios se deja a juicio del equipo evaluador. Una evaluación inicial completa debe a lo menos considerar los escenarios expuestos en la **Tabla 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. Variaciones menores en escenarios similares no necesitan ser evaluados separadamente a no ser que haya diferencias sustanciales en las consecuencias o las vulnerabilidades.

Paso 2 – Estimación de Consecuencias

Se debe determinar el Nivel de Consecuencia apropiado para la Instalación (3, 2, 1), determinado de la Tabla 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 2 – Nivel de Consecuencias

Nivel de Consecuencia	Descripción
3	Instalaciones que transfieren, almacenan o manipulan “cargamentos peligrosos”
2	Instalaciones que 1 Están sujetas al 33 CFR Partes 126 y 154 (pero que no son “cargamentos peligrosos”) 2 Reciben naves certificadas para más de 150 pasajeros, o 3 Reciben naves en viajes internacionales
1	Instalaciones que no son las arriba indicadas

Nota: CFR (Code Federal Regulations) (www.gpo.gov/nara/cfr/index.html)

Paso 3 – Estimación de Vulnerabilidad

Cada escenario debiera ser evaluado en términos de la vulnerabilidad de la Instalación a un ataque. Cuatro elementos de vulnerabilidad pueden ser considerados en la determinación del puntaje: disponibilidad, accesibilidad, seguridad orgánica y dificultad del objetivo.

Disponibilidad: Presencia de la Instalación y la predicción de cómo se relaciona con la capacidad de planificar un ataque.

Accesibilidad: Accesibilidad de la Instalación al escenario de ataque. Esto se relaciona con las barreras físicas y geográficas que disuaden la amenaza sin protección/ protección orgánica.

Seguridad Orgánica: La habilidad del personal de protección de disuadir un ataque. Esto incluye los Planes de Protección/ 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.

Dificultad del Objetivo: La habilidad de 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 Oficial de Protección de la Instalación Portuaria, 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 protección ya adoptadas.

La evaluación de la vulnerabilidad sin estrategias proporcionará una ponderación base mas 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, dando un mejor entendimiento del riesgo general asociado con el escenario y como las nuevas estrategias y medidas de protección 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 entregados por la Tabla 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 en tabla 5). Este puntaje deberá ser usado como puntaje de vulnerabilidad cuando se evalúe cada escenario en el próximo paso.

Tabla 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 plan, 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 protección mínimo, algunas comunicaciones, fuerza de protección 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 que disuada el ataque (plan detallado de protección, comunicaciones efectivas de emergencia, equipo de personal de protección bien entrenado, sistema de detección múltiples (Rayos X, cámaras, etc) Fuerza externa para prevenir oportunamente..

Paso 4 – Mitigación

A continuación se debe determinar qué escenarios requieren de una estrategia de mitigación. Esto se logra determinando donde se posiciona el escenario en la Tabla 4, basado en el Nivel de Consecuencia y Puntuación de Vulnerabilidad

La Tabla 4 es una herramienta relativa y amplia para ayudar en el desarrollo del Plan de Protección.

Mitigar: significa que se deben desarrollar estrategias de mitigación, tales como medidas protectoras de protección, para reducir el riesgo del escenario. Un Apéndice del Plan de 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 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, medidas que tengan un bajo costo pueden ser consideradas. El Plan de

Protección debe contener los escenarios evaluados y los resultados de la evaluación.

Tabla 4 – Matriz de Vulnerabilidad y Consecuencia

		Puntuación Total de Vulnerabilidad (Tabla)		
		2	3-4	5-6
Nivel de Consecuencia (Tabla 2)	3	Considerar	Mitigar	Mitigar
	2	Documentar	Considerar	Mitigar
	1	Documentar	Documentar	Considerar

Paso 5 – Métodos de Implementación

Para determinar qué escenarios requieren medidas de mitigación, puede ser útil usar la Tabla 5. La instalación portuaria, puede registrar los escenarios considerados, el nivel de consecuencias (Tabla 2), el puntaje de vulnerabilidad de cada elemento (Tabla 3), el puntaje total de vulnerabilidad y la categoría de mitigación (Tabla 4). El efecto deseado es reducir el riesgo asociado con las combinaciones objetivo/escenario que se 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 5 – Determinación de Mitigación

HOJA DE TRABAJO DE DETERMINACIÓN DE MITIGACIÓN					
Paso 1	Paso 2	Paso 3			Paso 4
Descripción/ Escenario	Nivel de Consecuencia (Tabla 2)	Puntaje de Vulnerabilidad (Tabla 3)			Mitigar, Considerar, o Documentar (Tabla 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 6

Tabla 6 – Implementación Mitigación

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 5)	Nivel de Consecuencia (Tabla 2)	Puntaje de Vulnerabilidad (Tabla 3)			Nuevos Resultados de Mitigación (Tabla 4)
			Accesibilidad +	Orgánica =	Puntaje Seguridad Total	
1.	1.					
	2.					
	3.					
2.	1.					
	2.					
	3.					

Los pasos siguientes corresponden a cada columna de la Tabla 6.

- 1.- Para aquellos escenarios puntuados como **considerar** o **mitigar**, se deben idear estrategias de mitigación (Medidas de Protección) y registrarlas en la primera columna de la tabla 6.
- 2.- Usando el escenario (s) de la tabla 5, hacer un listado de todas los escenarios que serán afectados por la estrategia de mitigación seleccionada.
- 3.- El nivel de consecuencia permanece igual que el determinado en la tabla 2 para cada escenario.
- 4.- Reevaluar los puntajes de accesibilidad y seguridad orgánica (Tabla 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.

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.

Considerar las estrategias como un todo, 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 que en general, el nivel de riesgo de una instalación permanece constante en relación con el incremento de la amenaza.

Las Tablas 7 y 8 , dan un ejemplo abreviado de cómo las tablas 5 y 6 , pueden completarse para una instalación que esta afecta al 33 CFR 154 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 7 – Determinación Mitigación

EJEMPLO DE HOJA DE TRABAJO DE DETERMINACIÓN DE MITIGACIÓN					
Paso 1	Paso 2	Paso 3			Paso 4
Descripción/ Escenario	Nivel de Consecuencia (Tabla 2)	Puntaje de Vulnerabilidad (Tabla 3)			Mitigar, Considerar, o Documentar (Tabla 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. Usar la instalación como un medio para transferir gente desde un buque a un vehículo para ingreso ilegal al país.		3	2	5	Mitigar

Tabla 8 – Implementación Mitigación

EJEMPLO 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 5)	Nivel de Consecuencia (Tabla 2)	Puntaje de Vulnerabilidad (Tabla 3)			Nuevos Resultados de Mitigación (Tabla 4)
			Accesibilidad +	Orgánica =	Puntaje Seguridad Total	
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

**ÁREA DE PROTECCIÓN DE
INSTALACIONES PORTUARIAS**
Servicio de Inspecciones Marítimas
Dirección de Seguridad y Operaciones
Marítimas