



FACULTAD DE CIENCIAS ECONOMICAS Y EMPRESARIALES

TRABAJO DE DIPLOMA

Título: Análisis y evaluación del sistema de protección física a partir de modelos numéricos.
Estudio de un caso. En la Empresa Servicios Portuarios Tricontinental.

Autor: Rogelio Miguel López Pérez.

Tutores: Ing. Rafael Oviedo Casanova.
Ing. Aneyrelis Casanova Reyes.

Curso: 2006-2007

“Año 49 del Triunfo de la Revolución”

HAGO CONSTAR

Hago constar que el presente trabajo fue realizado en la Empresa Servicios Portuarios Tricontinental como parte de la culminación de los estudios de Ingeniería Industrial; autorizando a que el mismo sea utilizado por la Universidad y la empresa donde fue realizado para los fines que estime convenientes, tanto de forma parcial como total y que además no podrá ser presentado en eventos ni publicado, sin la aprobación de los antes mencionados.

El autor

Los abajo firmantes certifican que el presente trabajo ha sido revisado según acuerdos de la dirección de nuestro centro y el mismo cumple los requisitos que debe tener un trabajo de esta envergadura, referido a la temática señalada.

Computación

Información Científico-técnico

Firma del tutor

Firma del tutor

DEDICATORIA

A mi padre, principal motivación para que yo haya llegado hasta aquí,

A mi madre, en quien siempre encontré apoyo para enfrentar las dificultades del camino,

A mi hermano, quien me ayudó a resolver mis problemas,

A mi esposa, quien comprendió mis alegrías y tristezas,

A mis hijitas, quienes deberán ser mejores que yo

AGRADECIMIENTOS

A Fidel, la Revolución y sus Mártires, pues sin la obra que se ha creado un hijo de familia humilde como yo no hubiese tenido la oportunidad y el privilegio de realizar estudios universitarios y mucho menos intentar hacer ciencia.

A la dirección de la Gerencia territorial de SEPSA Cienfuegos, a mis compañeros de trabajo Lorgio, Albuerne, Ariel, Marrero, Luís Alberto, Alexey y demás que me han brindado su ayuda y amistad sincera.

A mis tutores, motores impulsores, Rafael Oviedo Casanova y Aneyrelis Casanova Reyes, por la sabiduría y apoyo ofrecido, por su disposición incondicional para atender todos mis reclamos. Sin su firme y, tierna exigencia de compañeros, este trabajo no hubiese existido.

A todos mis compañeros de estudio, en especial a Vladimir y Jorge Raúl por su amistad y ayuda a través de todos los años de estudio.

Al colectivo de profesores que durante la carrera de quienes recibí los conocimientos que llevaré siempre.

A mi familia, en especial a mi Madre, Hijas y Esposa, por estar siempre a mi lado y por esas horas de compañía que la tesis y mi trabajo, sin querer, le han arrebatado.

“El problema es que la gente no es perfecta ni mucho menos, y hay que perfeccionar los sistemas de control para detectar la primera infracción que se produzca, porque esta es la que conduce a todas las demás”

Ché

RESUMEN

Para analizar el diseño de un Sistema de Protección Física para Instalaciones Sensibles, surge como una buena herramienta alternativa de evaluación, el uso de Modelos Analíticos de Simulación. En tal sentido el uso de estos modelos, insertos en la metodología empleada por países de avanzada tecnología, dan al estudio del tema un marco interesante. Conceptos modernos en el campo de la seguridad de instalaciones, tales como, Sistemas Efectivos de Protección Física, elementos de retardo y de detección, controles de acceso, estimación y evaluación de amenazas, junto a tiempos de respuestas y probabilidades de interrupción, entre otros, son analizados en detalle en el desarrollo de este tema. Finalmente se concreta la presente investigación con la proposición de implementar un Sistema de Protección Física en una Instalación aplicando los conceptos más avanzados y la tecnología de punta en el área, aprovechando la experiencia y asesoría de empresas internacionales y nacionales dedicadas al tema.

INTRODUCCIÓN.....	8
CAPITULO 1: MARCO TEÓRICO	12
Seguridad integrada en los sistemas de protección física.....	12
Sistemas de Protección Física.....	15
La Seguridad Portuaria	24
El desarrollo de la Protección Física en Cuba	25
Descripción del modelo	29
El modelo SAVI (Systematic Analysis of Vulnerability to Intrusion).....	31
Conclusiones del capítulo	37
CAPITULO 2: EL OBJETO Y SU SISTEMA DE PROTECCIÓN ACTUAL.....	38
Presentación del objeto de estudio.....	38
Caracterización de la seguridad y protección actual	40
Identificación de blancos	41
Diagrama de Secuencia del Adversario.....	43
Características de la Amenaza.....	44
Las acciones de la Fuerza de Respuesta	45
La detección y el retardo	45
Análisis de sensibilidad del SPF actual	47
Conclusiones del Capítulo	53
CAPÍTULO 3: RESULTADOS Y DISCUSIÓN.	54
Alternativas de mejoras del sistema de protección física	54
Proceso de análisis y selección de las mejoras del sistema de protección física.....	55
Demostración de la validez de la solución	56
Formas de implementación de la solución	66
Conclusiones del Capítulo	66
CONCLUSIONES GENERALES	67
RECOMENDACIONES	68
BIBLIOGRAFÍA	
ANEXOS	

INTRODUCCIÓN

Una de las principales necesidades del ser humano es la de sentir y tener seguridad, tal como bien lo define Abraham Maslow (1902-1971). El hombre requiere proteger su integridad física como también la de sus bienes y para ello hace uso de los medios y técnicas que estén a su disposición, creando y organizando sistemas de seguridad, y a la vez, requiriendo y exigiendo día a día una mayor eficiencia de ellos.

La definición del concepto de seguridad es una materia compleja, ya que ésta no se refiere a un específico y único problema, sino que está afectada por un conjunto de factores interrelacionados, muy diversos entre sí.

Hoy no es posible analizar la problemática de seguridad a través de soluciones aisladas o independientes, sino que resulta necesario el diseño de sistemas más complejos que, partiendo de posiciones genéricas y mediante el análisis y valoración de aspectos muy diversos, vayan definiendo una solución integrada y coherente, que se extiende desde el mero cambio de procedimientos, hasta el uso de soluciones técnicas avanzadas.

Dentro del campo global de la seguridad, ocupa un lugar de preeminencia el importante grupo denominado "Seguridad Física de Instalaciones" o "Protección Física", que comúnmente se presenta como el grupo de más complejidad y que menos se ha abordado. Este grupo comprende: elementos físicos, funciones o protocolos a desarrollar y personas.

En la actualidad y particularmente el Ejército contempla, en sus sistemas de protección física de las instalaciones dependientes, básicamente un sistema de protección apoyado casi en su totalidad en medios humanos, los cuales cumplen las funciones de prevención, vigilancia, detección y reacción. Esta tendencia se observa también en las instalaciones no civiles de países poco desarrollados y conlleva a un gran desgaste de personal y al poco aprovechamiento de recursos que pueden ser empleados en otras funciones.

ANTECEDENTES

En Cienfuegos existen un grupo de objetivos que resultan estratégicos para el país y toda la provincia, todos los cuales resultan de un gran atractivo para los adversarios con motivaciones político-ideológicas, económicas y personales.

El estado cubano ha reconocido públicamente y ha hecho denuncias de los planes de EEUU a fin de dañar la actividad de objetivos estratégicos ubicados en Cienfuegos y otras partes del país.

Las entidades del territorio han reportado en diferentes momentos, magnitudes preocupantes de daños producidos en su gran mayoría por el actuar de adversarios locales que impactan sobre objetivos estratégicos y otros que no lo son pero que al final repercuten negativamente sobre el desempeño de la actividad de toda la provincia.

SITUACIÓN PROBLÉMICA

La situación problemática identificada se fundamenta en la necesidad que tienen las organizaciones estratégicas de garantizar los sistemas de protección física óptimos que le permitan homologarse ante las exigencias de la Organización Marítima Internacional (OMI) y el estado cubano, incrementando, con ello, su capacidad defensiva, la seguridad de sus operaciones e incrementar su cultura de seguridad.

DEFINICIÓN DEL PROBLEMA

Inexistencia de un sistema de protección física adecuado en la empresa Servicios Portuarios Tricontinental que le permita disponer de una capacidad defensiva para poder enfrentar los riesgos y amenazas a que está expuesta.

HIPÓTESIS

A partir de la utilización del software SAVI a la Empresa Servicios Portuarios Tricontinental se podrán identificar los puntos vulnerables que atentan contra la protección física y establecer un conjunto de medidas preventivas que conlleven a fortalecer la protección de la organización.

OBJETIVO GENERAL

Analizar y evaluar el sistema de protección física de la Empresa Servicios Portuarios Tricontinental a partir de la utilización de herramientas informáticas para identificar los puntos vulnerables.

OBJETIVOS ESPECÍFICOS

1. Elaborar una base teórico conceptual que permita abordar y conocer las principales consideraciones teóricas sobre sistemas de protección física.
2. Hacer un diagnóstico de la protección física de la instalación a partir del procedimiento establecido por seguridad portuaria.
3. Comprobar la capacidad del modelo SAVI para el análisis y diseño de instalaciones no nucleares.
4. Obtener las variantes que permitan mejorar razonablemente la eficacia del sistema de protección física de la instalación.

En primera instancia se hace necesario hacer un estudio detallado de lo que se conoce actualmente por un Sistema de Protección Física “efectivo” para determinar los modelos de simulación de sistemas de protección física que existen y están disponibles. Seguidamente es necesario realizar un estudio sobre la tecnología de diagnóstico de seguridad portuaria establecida tanto a nivel internacional como nacional, así como de las proyecciones de la Organización Marítima Internacional en tal sentido, también es necesario estudiar lo establecido por el Estado cubano en cuanto a la protección física. Posteriormente se procederá a realizar un diagnóstico de la seguridad actual de la instalación y finalmente se realizará la confección de los modelos de Diagrama de Secuencia del Adversario de la misma y a la simulación del sistema de seguridad mediante el modelo seleccionado, concluyendo con los principales resultados obtenidos, concluyendo con las recomendaciones para trabajos futuros.

BREVE DESCRIPCIÓN DE LAS PARTES FUNDAMENTALES

El trabajo se desarrolla en tres capítulos, el primero de ellos está dedicado a ofrecer la tendencia actual de la seguridad, explicando los conceptos básicos de la protección física y la seguridad

portuaria, una panorámica del tema en nuestro país, así como la descripción del modelo utilizado; en el segundo se hace una caracterización del objeto de estudio, analizando la situación actual que en materia de protección física posee la entidad determinando los puntos vitales de la misma; y en el tercer capítulo se desarrolla la propuesta de las medidas a tomar por parte de la empresa, validadas mediante el software SAVI.

CAPITULO 1: MARCO TEÓRICO

SEGURIDAD INTEGRADA EN LOS SISTEMAS DE PROTECCIÓN FÍSICA

Hoy no es posible analizar la problemática de seguridad a través de soluciones aisladas o independientes, sino que resulta necesario el diseño de sistemas más complejos que, partiendo de posiciones genéricas y mediante el análisis y valoración de aspectos muy diversos, vayan definiendo una solución integrada y coherente, que se extiende desde el mero cambio de procedimientos, hasta el uso de soluciones técnicas avanzadas, que permiten - como objetivo común a casi todos los sistemas - la disminución del personal empleado en tareas de vigilancia, sin que se disminuya el grado de seguridad que la situación amerite.

Pero es necesario antes de adentrarnos en las especificidades de esta integración es necesario definir a la seguridad, la que según Abraham Maslow (1902 –1971), es un *“conjunto de necesidades, impulsoras del comportamiento, que aparecen una vez que han sido satisfechas las necesidades de orden fisiológico y ocupan el segundo escalón entre las necesidades del ser humano que es la representación básica de la empresa”*.

La integración es un fenómeno propio de las organizaciones de éxito, a las que le es necesario no ya anticiparse al futuro, sino crearlo, diseñar el futuro deseable y los medios para alcanzarlo. De esta forma se habrá logrado minimizar el número de sorpresas estratégicas y maximizar la rentabilidad de la empresa.

La seguridad debe ser integradora de toda la organización sobre la base de un estilo de planificación interactiva que movilice todos los recursos que integran su estrategia en la formulación de la misma, a la vez que facilite los procesos de integración de la organización en dicha estrategia, con una flexibilidad tal que le permita adaptarse a los cambios previstos, y suficiente pro actividad que le permita anticiparse al futuro.

La seguridad integrada se caracteriza por la incorporación de los objetivos y tareas de seguridad en cada área y miembros de la organización, según su responsabilidad y esfera de competencia.

La seguridad integrada resulta más efectiva y rentable precisamente por estar integrada a la actividad empresarial y no descansar en la existencia de un gran aparato de seguridad.

La seguridad integral va dirigida a suprimir el riesgo en sus diversas manifestaciones, no solo a lo que concierne a los riesgos y daños para el hombre, sino también lo concerniente a las instalaciones, el producto, el entorno y otros aspectos de la actividad de la empresa. La integración de la seguridad en contenidos y responsabilidades, en este tema la responsabilidad tanto de las áreas, como de los directivos, jefes y trabajadores se refiere a:

1. Introducir los requisitos de seguridad en la preparación, el desarrollo y el control de la actividad productiva o de servicio, previo análisis de los procesos, métodos y medios de trabajo.
2. Introducir los requisitos de seguridad en las reglas, órdenes e instrucciones de trabajo, las normas de operación de los equipos y otros procedimientos previstos en la producción y los servicios, tanto como la documentación técnica que elabore la empresa.
3. Incluir los aspectos organizativos relativos a la seguridad en los reglamentos, sistemas de información y control.
4. Desarrollar el papel de los jefes directos, asumiendo la responsabilidad en esta labor, facultándolo para detener un equipo, o un proceso en caso de peligrar la seguridad del trabajador, del patrimonio o del entorno.
5. Orientar a los técnicos y especialistas de seguridad una labor básica de asesoría y fiscalización en esta materia.

Acciones que garantizan la seguridad en la empresa.

1. Análisis de la seguridad del trabajo.
2. Selección del personal para puestos riesgosos.
3. Formación e información en materia de seguridad.
4. Participación de los trabajadores.
5. Actividad de proyectos y el proceso inversionista de la empresa.
6. Organización de la producción y el trabajo.
7. Actividad técnica de la empresa.
8. Actividad comercial.
9. Evaluación y estimulación de los trabajadores.

10. Seguridad contra incendios.
11. Seguridad del transporte.
12. Seguridad del entorno.
13. Seguridad del producto.
14. Seguridad del patrimonio. (es tener en cuenta las medidas que garanticen la seguridad de los bienes, frente a los riesgos derivados de la intrusión, robos y otros actos delictivos, así como de incendio, explosiones, derrumbes, etc.)

Las acciones de seguridad su control y ajuste para comprobar la eficacia de las acciones de seguridad necesita un adecuado control de esta actividad en la empresa mediante indicadores apropiados, comparando los resultados obtenidos con los objetivos, las normas y los parámetros de referencia, tanto interno como externo, para establecer las medidas correctivas necesarias.

Un indicador en la evaluación y el control de la seguridad de la empresa es: La capacidad de respuesta ante averías y otras emergencias.

Hoy puede verse como se integran los circuitos cerrados de televisión (CCTV) con los sistemas automáticos contra intrusos (SACI) y estos con los sistemas automáticos de detección de incendios (SADI); de la misma manera en que se integran sistemas y procedimientos de “inteligencia” a sistemas técnico – mecánicos para llegar a tecnologías de edificación inteligente.

La integración presupone la estructuración de niveles superiores de desempeño de la seguridad corporativa buscando que la seguridad tenga un mayor desempeño y aporte mayor valor a la empresa.

A los efectos de la presente investigación se ha considerado como Integración a “la acción y efecto de funcionar en aras del cumplimiento de objetivos generales de un sistema sin afectar los fundamentos de funcionamiento de cada uno de sus elementos”; pues el hecho de que todas las acciones de seguridad estén funcionando de manera integrada no puede significar que el funcionamiento del sistema que protegen se subordine a ello, sino todo lo contrario, que uno y otros accionen mancomunadamente para lograr la eficacia del sistema en general.

La Seguridad Preventiva no ha constituido jamás en ninguna esfera un gasto superfluo y fondo perdido, sino una inversión, que de hecho y derecho constituye una vacuna contra las acciones delictivas diversas e incluso un instrumento valioso para la protección y salvaguarda de vidas humanas, sensibles y bienes que integran su patrimonio

SISTEMAS DE PROTECCIÓN FÍSICA

Como se plantea en el epígrafe 1.1 una de las acciones que garantizan la seguridad de la empresa es la seguridad del patrimonio, este tipo de seguridad es conocido también como protección física.

En epígrafes anteriores nos referimos a la necesidad de la integración en materia de seguridad, la seguridad física es un factor importante a la hora de lograr una óptima integración en la empresa, es por ello que la utilización de esta terminología en los SPF es imprescindible.

Hoy la gran mayoría de nuestros empresarios se encuentran convencidos e interesados por mejorar su SPF (Sistema de Protección Física) para eliminar o reducir los daños que producen un grupo de contingencias que amenazan sus acciones; pero muchos no tienen conocimiento de cómo diseñar un SPF o de cómo realizar un análisis del mismo. Esto no es tarea fácil por cuanto es necesario organizar y ejecutar un grupo de procedimientos para que los resultados finales realmente apoyen y permitan el máximo cumplimiento de los objetivos de seguridad de las empresas.

En la sociedad actual, el tema de la seguridad es tratado de disímiles formas y con cierta importancia que se traduce en los enormes presupuestos que los gobiernos asignan a la Seguridad Nacional, la Seguridad Pública, la Prevención de Desastres, Combate al Crimen y otras de las llamadas seguridades, aunque en la realidad, el creciente interés por la Seguridad se ha desarrollado paralelamente a los grandes daños que han ocurrido y al uso y empleo de modernas tecnologías; siendo bien tangibles los resultados alcanzados; puesto que la industrialización unido a todos sus beneficios ha traído también efectos muy perjudiciales sobre el entorno, las personas y las cosas, véase tan sólo que la actividad delictiva manifiesta una tendencia internacional creciente y los daños que la misma genera son cada vez mayores. Los gobiernos han comprendido que la protección física posee una importancia estratégica: los atracos a bancos, los asaltos a instalaciones co-

merciales, los incendios y otras manifestaciones amenazan la seguridad pública que deben garantizar los estados. También las empresas comprendieron que todo no podía quedar en manos de los estados y comenzaron a adoptar medidas de protección para defender sus patrimonios y para garantizar una mayor eficiencia y efectividad; comprendiendo que la protección física requiere un método integrado que cubra todas las causas y posibles resultados de los eventos dañinos y que este método tiene que ser visto como una estrategia.

En la década de los 60 era comprensible que para los SPF la comparación cuantitativa de riesgo / consecuencia entre diferentes entidades puede no ser correcta pues esta está muy ligada a otros factores de carácter económico, político, social, ético y moral entre otros; y de esta forma sólo es viable y muy recomendada la realización de estas comparaciones entre entidades de similares características pertenecientes a la misma rama con lo cual podemos definir estrategias ramales aunque la tendencia mundial actual es dirigir estos trabajos hacia la gestión de riesgos específicos y no hacia las evaluaciones comparativas ínter entidades.

Según estudios internacionales, los efectos más destacables de la falta de adecuación de la dirección de seguridad de las empresas se puede resumir en:

1. Las técnicas de gestión y los modos de dirección de protección física convencionales, se muestran ineficaces para orientar a la organización en el entorno en que viene actuando.
2. La dirección de la empresa persigue soluciones a corto plazo en cuanto a su seguridad.
3. Como los problemas anteriores no se resuelven o se resuelven con lentitud y los problemas administrativos de cada día no desaparecen y se van acumulando, surgen los conflictos en los grupos humanos y comienzan las crisis internas de las organizaciones, produciéndose pérdidas en la moral laboral que redundan en reducción del valor de los activos de las organizaciones.

A pesar de todo el desarrollo que en materia de seguridad se ha alcanzado no ha cristalizado todo lo necesario para que la seguridad se conforme como una disciplina del conocimiento con sus propias categorías. De hecho existe una cierta confusión entre los grupos sociales o profesionales en cuanto a la conformación de categorías, unas veces por falta de preparación, otras por falta de análisis y otras por la afectación que ello tendría en los intereses que se encuentran en juego; pero en la definición de seguridad es común que se confundan los fines y los medios y se mezcle en el

diálogo cuando se habla de uno u otro caso. Por ejemplo, el Estado Mexicano establece en el Manual de Seguridad a Instalaciones Vitales (DNM3107) la siguiente definición de seguridad, donde pueden verse las confusiones abordadas. Se define la “Seguridad Física sobre la base de las acciones y no del resultado como: “...las medidas que se adoptan para evitar lesión o pérdida de una vida, daño o desorganización, ruina o destrucción de una propiedad, así como hacer todo lo necesario para que existan, se desarrollen y cumplan los propósitos fijados, por lo tanto se debe adoptar en toda situación, en todo lugar y en todo tiempo. Esta seguridad depende en gran parte del adiestramiento individual y del conjunto de la organización de que se trate.”

Todos los estudiosos del tema concuerdan que la seguridad total no existe por la naturaleza de los factores que en ella participan de forma dinámica modificando los estándares definidos en un momento dado y las formas en que se manifiestan las contingencias, así como por el impacto que en ella tiene el error humano. No puede eliminarse la participación del hombre como elemento de acción y recepción de la seguridad en las organizaciones.

Con todo lo anterior es posible definir a los efectos de este trabajo a la Seguridad Corporativa como” una sensación de confianza de la empresa ante las contingencias indeseables que le permite un mayor rendimiento al sentirse protegida por un grupo de fuerzas, medios y procedimientos, contra los daños potenciales que puede tener por la materialización de los riesgos a los que está sometida”.

En nuestro trabajo entenderemos por Seguridad al “resultado de la protección, a un sentimiento relacionado con el nivel de vulnerabilidad y las amenazas que posea la empresa” mientras que Protección son las “acciones que se realizan para lograr la seguridad”. La protección es la acción consciente de la empresa para reducir el daño que puede recibir sobre sus bienes y no se considera sólo bienes de la organización al dinero, los ingresos, los inventarios y los activos fijos tangibles, sino que se considera también el capital humano, el conocimiento y otros valores intangibles; es decir que por Protección es entendido el “esfuerzo que realiza la organización para reducir los daños que pueden sufrir sus bienes por la ocurrencia de contingencias indeseables”.

Un Sistema de Protección Física es un conjunto de medios y medidas que se establecen para detectar la presencia de intrusos en las zonas a proteger, disuadirles o impedirles su penetración en las mismas y neutralizar sus acciones ofensivas, antes de que puedan consumir sus propósitos.

Con los sistemas de protección física se pretende lograr una delimitación física de zonas que además de facilitar la protección de materiales y personas, permita a su vez ganar tiempo para la intervención reactiva de los núcleos de seguridad o para adoptar las oportunas medidas evasivas. Consta de estructuras, sistemas y componentes muy variados, entre otros: barreras, detectores de intrusos, alarmas comunicaciones y medios para reaccionar, tanto activos como pasivos. A la vez un Plan de Seguridad de Instalaciones, es un conjunto armónico de sistemas de protección física y medidas reactivas en estrecha e íntima relación, para conformarlo es necesario tener en cuenta algunas consideraciones que pueden verse en el anexo #1.

Para establecer una seguridad y protección aceptables se debe comenzar por formularse las interrogantes siguientes:

1. ¿A quién brindamos seguridad o protegemos?
2. ¿De quién debemos asegurarnos o protegernos?
3. ¿Por qué lo debemos hacer?
4. ¿De qué debemos asegurarnos o protegernos?
5. ¿Con qué lograremos nuestro objetivo?
6. ¿Cuándo debemos hacerlo?
7. ¿Dónde debemos asegurarnos o protegernos?

En el pensamiento y actuar de los especialistas que en el mundo se desarrollan en esta especialidad existe la consideración de que en sistema de seguridad y protección debe estar encaminado a cumplir con objetivos definidos, entre los que se encuentran:

1. DISUADIR: Acción evidentemente preventiva y racional ya que predispone, a la vista de las medidas de seguridad adoptadas, a no cometer la acción autorizada.
2. DEMORAR: Función que tiene como objetivo el obstaculizar, dificultar, o retardar físicamente la entrada por puntos no autorizados, al tiempo que obliga violentar la instrucción establecida legalmente.
3. DETECTAR – ALERTAR: Detectar el tipo de acción no autorizada y alertar a la fuerza encargada de reconocer y corregir la alarma en el tiempo más breve posible y con la suficiente antelación para que su acción de respuesta sea eficaz.

4. IDENTIFICAR: Conocer el tipo de acción no autorizada, de forma rápida y fiable, porque esta información va a resultar determinante del tipo de respuesta a poner en marcha.
5. CANALIZAR: Esta función permite dirigir indirectamente a las personas por la vías deseables, de este modo, se puede mantener la vigilancia de manera permanente y ejercer control de las situaciones.
6. REACCIONAR: Es la función que realiza generalmente por el factor humano, tiene como objeto poder enmarcar acciones de respuesta, acordes con cada uno de los incidentes, para la corrección de los mismos y recuperación de la normalidad perdida.

Habitualmente pensamos que son bienes el dinero, los ingresos, la propiedad física y otros. Sin embargo, también se deben considerar especialmente los trabajadores de la empresa. Sin la experimentada fuerza laboral, los demás bienes pueden ser inútiles para lograr los propósitos de la entidad.

Existen dos factores fundamentales determinantes en la calidad de un programa de protección:

1. Primero, un buen plan de medidas para prevenir y limitar las pérdidas.
2. Segundo, la dirección principal debe apoyar el programa.

El sistema de seguridad y protección óptimo es aquel que además de prevenir los riesgos generales y particulares y adoptar el programa de medidas preventivas, por su efectividad, estimula el convencimiento en las diversas categorías de personas a los que va dirigido, que no deben cometer hechos delictivos de ninguna clase, no solo porque su escala de valores y principios se lo impida, sino también por poseer el convencimiento que si lo hiciera sería descubierto oportunamente y atraído a la responsabilidad que sus actos conllevaran.

Las medidas en los actuales Sistemas se orientan hacia tres vertientes principales, en las personas, los soportes y el programa. Las personas son lo mas importante y generalmente lo mas costoso de los tres elementos de medidas.

Se considera como protección física efectiva el conjunto integral de medidas ejecutivas, políticas, legislativas, económicas, organizativas, técnicas y de control, destinadas a garantizar el régimen de máxima seguridad, en correspondencia con las características propias de los órganos y entida-

des que lo integran, mediante la prevención y erradicación de todas las posibilidades y riesgos de actividad enemiga, delictiva y situaciones de inseguridad que afecten la integridad de los bienes, personas e informaciones del organismo así como de sus órganos y entidades que la integra, como complemento de la seguridad del estado y el orden interior.

Definición de Amenaza

Uno de los principales puntos de partida para el proyecto del sistema es la definición de la amenaza, sus móviles y sus atributos. No se debe perder de vista la situación, en cierto modo ventajoso, en la que se va a encontrar cualquier adversario. La decisión de actuar va a estar siempre en sus manos y, por consiguiente, puede preparar sus medios y tomar la decisión de actuar de acuerdo con su percepción de la constitución del sistema de seguridad, de las fuerzas de protección y de sus vulnerabilidades.

Es fundamental para la definición y mantenimiento del sistema de protección física, un conocimiento previo detallado de las actividades que se desarrollan dentro de la instalación, unido a un conocimiento actualizado de los móviles, medios y atributos del posible adversario. (Inteligencia)

En cuanto a objetivos es posible distinguir dos fundamentales: el robo y el sabotaje. El robo puede ser de material, equipo o información, ésta generalmente orientada hacia acciones posteriores. El sabotaje, puede tener por objeto la inutilización de las instalaciones e impedir que sirvan para los fines a que están destinadas, o provocar una catástrofe con los consiguientes perjuicios y perturbaciones materiales o el aprovechamiento del efecto psicológico con fines políticos, o terroristas por la vía de la extorsión.

En cuanto al adversario, es necesario considerar un espectro amplio que va desde el individuo aislado, que puede ser parte del propio personal que por alguna razón desea producir un perjuicio a la institución, hasta la organización criminal que va buscando un beneficio económico con la amenaza de producir daños, cuya repercusión sería tan grave que los responsables de la instalación deberían estar dispuestos a pagar para evitarlas e incluso evitar la difusión de la noticia de la agresión.

Concepto de Adversario

Persona o grupo de ellas con motivación suficiente y capacidad real para atacar los bienes protegidos. Pueden ser internos, externos y combinados.

Caracterización del Adversario

Los adversarios o agresores son personas que desempeñan actos hostiles contra nuestras instalaciones, incluyendo el equipo, personal u operaciones. Otras características que se emplean en la caracterización del adversario potencial contemplan:

1. FINALIDAD: Objetivo del adversario o sea las acciones potenciales que con mayor probabilidad este intente desarrollar en sus ataques, los blancos que atacará y el momento en que realizará el ataque.
2. CANTIDAD: Promedio de adversarios que se espera atacarán a la empresa en cada agresión.
3. ARMAMENTO: Tipo de armamento que empleará el adversario en sus ataques a la empresa. Puede ser garrotes, armas blancas, armas de fuego.
4. HERRAMIENTAS: Herramientas y equipos que se estima utilizará el adversario en sus ataques a la empresa. Pueden ser herramientas de mano, de oxicorte, etc.
5. TRANSPORTE: Transporte que se estima utilice el adversario para los ataques a la empresa. Puede ser que no utilice transporte alguno, o puede ser vehículos de tracción animal, autos, camiones, etc.
6. EXPERIENCIA: Experiencia estimada del adversario en cuanto a la ejecución de ataques a empresas.
7. APOYO: Apoyo que puede tener el adversario en la realización de su ataque. Los adversarios internos pueden apoyar a los externos con la neutralización de los sistemas de detección, comunicación o retardo facilitándole el acceso a los blancos, etc.
8. INFORMACIÓN: Nivel de conocimiento que tiene el adversario sobre la empresa y su sistema defensivo.
9. ACCESIBILIDAD: Nivel de accesibilidad que se le atribuye al adversario a los diferentes blancos.
10. LA CONSPIRACIÓN: Se refiere al que pueda recibir ayuda por parte del personal de la instalación y si este auxilio ha de ser activo o pasivo. Los objetivos pueden ser como ya se mencionó, el robo y/o el sabotaje.

A partir del análisis de estos atributos y de la experiencia disponible se llega a definir en forma general cuatro niveles de amenaza.

1. **SIGILO:** Es la táctica que se basa en la utilización de los descuidos o brechas del sistema de seguridad para burlarlo.
2. **ENGANO:** Se basa en elementos de falsificación a través del cual tratan de enmascarar su actividad a fin de no ser detectado por el sistema de protección.
3. **FUERZA:** Táctica de los adversarios que se basa en el empleo de la misma sobre los medios de protección que conforman el sistema de seguridad procediendo con vistas a su neutralización y lograr así la consecución de sus objetivos.
4. **SOBORNO:** Se basa buscar el comprometimiento de las fuerzas de respuesta o de los demás elementos que inciden en la instalación desde un punto de vista legal y de esta forma garantizar la realización del daño.

La confrontación del sistema de seguridad con estos niveles de agresión u otros parecidos permite definir cuál es el máximo nivel que el sistema será capaz de contrarrestar por procedimientos propios. Al mismo tiempo se debe analizar el impacto de los cambios en el sistema de seguridad sobre su capacidad para resistir la actuación de un determinado adversario, lo que permitirá definir la conveniencia, desde un punto de vista sobre todo económico de introducir determinados cambios en el sistema de seguridad. También es interesante un análisis de la sensibilidad del sistema frente a los medios de que disponga el adversario.

Un procedimiento adecuado para estos análisis es la Simulación, que se efectúa, en general, por medio de modelos y programas de computador, que pueden ir desde sistemas sencillos a grandes computadores, en la que se incluyen complejos modelos determinísticos o aleatorios.

Objetivos del adversario

Los posibles objetivos del adversario incluyen:

1. Infligir daño o muerte sobre las personas
2. Destruir o dañar instalaciones, propiedad, equipo, o recursos

3. El robo de equipo, material o información (espionaje)
4. Crear publicidad adversa.

Diagrama de secuencia del adversario

La detección, demora, y los elementos de respuesta son todos importantes al análisis y evaluación de un blanco que resulta en robo o en sabotaje). El analista debe considerar las metas del adversario al completar la trayectoria. El tiempo de demora o la probabilidad del Sistema de Protección Física y su eficacia. Para la mayoría de los modelos de análisis, primero deben identificarse las trayectorias del adversario y los posibles blancos (serie de acciones contra acumulativa de detección a lo largo de una trayectoria específica) no es satisfactorio para evaluar la eficacia de un Sistema de Protección Física a lo largo de la trayectoria. Por lo tanto, la combinación de la dos debería ser usada como una medida de eficacia. Otra probabilidad de interrumpir al adversario es la detección oportuna, que es, detectar al adversario en la demora mientras queda todavía suficiente tiempo para que la fuerza de respuesta pueda responder. Pero, no toma en cuenta la real neutralización del adversario. Al inferir verdaderamente la eficacia de un sistema total de Protección Física se considera la trayectoria más crítica, que es la trayectoria con la probabilidad más baja de interrupción. El sistema de protección va a ser tan efectivo como la protección que le brinde a esta trayectoria.

Un sistema de protección física es una configuración compleja de detección, retardo, y elementos de respuesta. Las técnicas están disponibles para analizar un sistema de protección física y evaluar su eficacia. Tales técnicas identifican las deficiencias del sistema, evalúan su perfeccionamiento y realizan comparaciones costo versus eficacia. Estas técnicas son apropiadas para analizar los sistemas de protección física en sitios individuales. También, las técnicas pueden usarse para evaluar un sistema de protección existente o uno que se encuentre en la fase de diseño.

Es esencial que las medidas recomendadas se revisen y actualicen de vez en cuando, reflejando los adelantos que se han hecho en el estado del arte en sistemas físicos y equipos de protección o en la introducción de nuevos tipos de instalaciones. Además, en el diseño de un sistema de protección física para una instalación específica, se esperan varias de estas recomendaciones cuando predominan circunstancias que indican la necesidad de un diferente nivel de protección física.

Únicamente conduciendo periódicos reanálisis, pueden el efecto de esas condiciones de cambio ser vistas y cuantificadas.

LA SEGURIDAD PORTUARIA

La seguridad portuaria esta basada en el Convenio Internacional para la seguridad de la vida humana en el mar 1974 (Convenio SOLAS 1974) del cual Cuba es país miembro, este convenio en el capitulo XI-2 hace referencia al código internacional para la protección de los buques y las instalaciones portuarias (código PBIP) y exige a los buques, las compañías y las instalaciones portuarias que cumplan las prescripciones establecidas contribuyendo en gran medida a incrementar la seguridad y la protección marítimas y a salvaguardar a quienes se encuentren a bordo y en tierra.

La conferencia diplomática sobre protección marítima celebrada en Londres en diciembre del año 2002 adopto nuevas disposiciones del convenio internacional, para incrementar la protección marítima. Estas nuevas prescripciones constituyen el ordenamiento internacional que permitirá que 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. En el 2001 y 2002 fueron celebradas la XXII asamblea de la OMI y la conferencia diplomática sobre protección marítima respectivamente.

Donde aprobaron varias resoluciones, incluidas las relativas a la implementación y revisión del presente código, la cooperación técnica y la colaboración con la Organización Internacional del Trabajo y la organización Mundial de Aduanas.

Las disposiciones están redactadas de modo que se garanticen su compatibilidad con las del convenio Internacional sobre normas de formación, titulación y guardia para la gente de mar 1978, enmendado, el código Internacional de gestión de la seguridad (IGS) y el sistema armonizado de reconocimientos y certificación.

La implementación de las disposiciones requerirá una continua y eficaz cooperación y entendimiento entre todos los que tienen que ver con los buques y las instalaciones portuarias, o los que la utilizan, incluido el personal portuario, los pasajeros, los intereses de la carga, los gestores na-

vales, los administradores de puertos y las autoridades nacionales y locales que tengan responsabilidades en el ámbito de protección. Las autoridades Nacionales y las locales tendrán que asumir responsabilidades adicionales, estas orientaciones serán aplicables en mayor o menor medida según la naturaleza de la instalación portuarias y del buque, del servicio de que se trate y/o la carga.

EL DESARROLLO DE LA PROTECCIÓN FÍSICA EN CUBA

Como en todo el mundo, la Protección Física ha tenido un desarrollo gradual en Cuba; denotándose un punto de diferenciación en su desarrollo marcado por el triunfo de la revolución. Antes del triunfo de la revolución, la protección física tenía un carácter meramente privado que fue desarrollándose desde la época colonial y neocolonial; en estas épocas prerrevolucionarias no es menos cierto que el Estado tomaba partido en cuanto a medidas de seguridad; pero éstas tenían poco peso o demasiado en aquellos casos en que se intervenía en el sector con la policía o el ejército para defender los bienes de la clase dominante ante las acciones populares y revolucionarias, sin menospreciar las acciones de las lacras sociales de esta época.

Con el triunfo de la revolución, cambia el carácter de la protección física respondiendo a los intereses del Estado revolucionario. Comienza una aguda lucha de clases y el estado organiza formas circunstanciales de seguridad con estructuras paramilitares que defendieran las victorias alcanzadas. En esta lucha surgieron los Comités de Protección Física (CPF), los Cuerpos de Vigilancia y Protección (CVP), así como algunas legislaciones especiales.

La idea de la protección pública a la propiedad no personal apareció después de la revolución industrial y aún hoy es un concepto de aplicación limitada. El propietario de una empresa, es dueño de un recurso, en nuestro caso estatal como representación de los intereses de todo el pueblo, es y ha sido siempre, dependiente de su propia protección.

Al proyectar nuestro trabajo, si bien debemos tomar en cuenta toda la experiencia acumulada internacionalmente, debemos adecuarlas a nuestras necesidades y la concepción de que nuestra labor debe ser mas amplia y profunda, ya que al cumplir nuestra misiones debemos hacer frente a las acciones de los servicios especiales de los países imperialistas que tratan de destruir por todos

los medios posibles el proceso revolucionario, para lo cual tienen entre sus objetivos mas priorizados nuestra base económica.

Hemos introducido el estudio de modernas tecnologías que pueden ser aplicadas en tareas de obstaculización, y prevención.

El asimilar dichos conocimientos y trabajar en su constante actualización debe formar parte de la cultura del trabajo de protección, a pesar de las grandes limitaciones actuales a la hora de realizar inversiones, máxime cuando en este caso represente una fuerte erogación de divisas, en particular en aquellas entidades de alto valor estratégico en lo económico y lo científico.

A mediados de la década del 90 resultaron insuficientes estas estructuras ante la situación que existía en el país. Así surge el Decreto Ley 186 que propicia la mayor ruptura conceptual que ha existido en Cuba. Esta legislación de estado hecha por tierra toda la antigua estructura en que se organizaban los sistemas de protección física dando pie a la creación de empresas especializadas en la prestación de servicios de protección y la aparición de nuevas figuras en el espectro de servicios de protección todo lo cual sólo estaba anteriormente en manos de los cuerpos de seguridad y protección que poseían las empresas.

Los cambios que ocurrieron en la realidad económica – social de Cuba en la década del 90 exigieron cambios organizativos en los sistemas de protección física. Es el Estado, consciente de ésta necesidad, el que comienza a realizar un proceso de diagnóstico en cuanto a la protección física bajo la dirección de Carlos Lage en sus funciones de Secretario del Consejo de Estado y con la participación de las siguientes entidades del estado:

1. Ministerio del Trabajo y la Seguridad Social
2. Ministerio del Interior
3. Ministerio de Economía, Planificación, Finanzas y Precios
4. Organismos de la dirección Central del Estado
5. Organizaciones

En el diagnóstico realizado por esta comisión gubernamental se pudieron comprobar un conjunto de deficiencias que limitaban regularmente la aprobación del Decreto Ley 186 en las empresas. Ver anexo #2.

Luego de haber trabajado en estas deficiencias el Decreto fue firmado por el Presidente del Consejo de Estado el 17 de junio de 1998, con el objetivo de establecer y regular el Sistema de Seguridad y Protección Física y los servicios a prestar en esta materia.

El Decreto explica el papel rector del Ministerio del Interior como encargado de dirigir y controlar la política de Seguridad y Protección Física, en las instalaciones y demás bienes sociales asignados a los órganos, organismos y demás entidades de producción y servicios.

En el contexto nacional, existe el SNS (Sistema Nacional de Seguridad) el cual está conformado como sigue:

El Partido Comunista de Cuba

El Partido es el centro del SNS y al se subordinan: el MINFAR, el MININT, los órganos del Estado y el Gobierno; así como las Organizaciones Políticas, Sindicales y de Masas. En el anexo 3 encontramos la estructura que plantea las fuentes originales de información para el trabajo de identificación de la amenaza y los adversarios.

El Ministerio de las Fuerzas Armadas (MINFAR)

Cumple misiones combativas ante agresiones militares externas o internas, para lo cual realiza la preparación del teatro de operaciones y las fuerzas de defensa en la doctrina militar cubano; así como la búsqueda, obtención y análisis de información sobre el adversario (enemigo). También tiene la misión de brindar protección a las organizaciones del sector estratégico como Centrales Eléctricas, Refinerías y Complejos Fabriles entre otros, para ello resultan sumamente importantes las informaciones de las secciones de inteligencia y contrainteligencia del MINFAR.

Los Organismos del Estado

Todos los organismos del Estado están integrados al SNS y ellos a través de los departamentos de Protección y Seguridad realizan estudios de la amenaza y los adversarios que resultan interesantes a la organización. Los organismos del Estado también emiten proclamas de amenazas implícitas en las resoluciones, cartas directivas, etc. que deben ser utilizadas por las organizaciones constituyéndose todas en fuentes de información para la organización. Por ejemplo:

1. EL MINISTERIO DE JUSTICIA (MINJUS) emite legislaciones que apoyan el enfrentamiento a la delincuencia y la contrarrevolución.
2. LA FISCALÍA. En su función jurídica legal, obtiene conocimiento sobre las particularidades de la amenaza y los adversarios que son útiles a la empresa.
3. OFICINA NACIONAL DE AUDITORIA, poseen información sobre el comportamiento de la delincuencia y nos puede alertar sobre los riesgos que poseen las empresas.
4. EL SISTEMA BANCARIO, al igual que la Oficina Nacional de Auditoria, posee informaciones sobre riesgos que debe atender las empresas.
5. LA CÁMARA DE COMERCIO DE CUBA. Registra y controla todas las operaciones comerciales internacionales en las que participa nuestro país. Ello le permite obtener información útil para la empresa sobre acciones potenciales de carácter internacional como el lavado de dinero, la deslealtad de comerciantes, etc.
6. EL SISTEMA DEL SEGURO. Las entidades del seguro por sus funciones obtienen informaciones valiosas sobre el comportamiento delictivo y los riesgos generales que amenazan a las empresas.
7. LA ADUANA GENERAL DE LA REPÚBLICA. Tiene la función de controlar y fiscalizar la entrada y salida de bienes al país. Obtiene información sobre diferentes amenazas relacionadas con el contrabando de bienes, el narcotráfico, etc.
8. LA DEFENSA CIVIL. Su función es garantizar las medidas preventivas, de respuesta y recuperación de las empresas y la población ante situaciones de catástrofes, de allí lo importante que puede resultar su información.

El Ministerio del Interior (MININT)

Cumple misiones combativas contra los servicios especiales enemigos y la contrarrevolución interna y externa; así como contra la delincuencia común y otras. Puede ser fuente de información relacionada con los adversarios internos e intrusos a partir del trabajo de enfrentamiento que

realizan sus órganos especializados dentro de los cuales resultan de vital interés para las organizaciones los siguientes:

1. POLICÍA NACIONAL REVOLUCIONARIA, en particular los Jefes de Sectores y oficiales del DTI que forman parte de este órgano los cuales tienen información pública y secreta sobre la delincuencia común.
2. CONTRA INTELIGENCIA, en particular los oficiales de territorio y de las diferentes especialidades existentes. Obtiene información pública y secreta sobre la delincuencia contrarrevolucionaria.
3. SEGURIDAD Y PROTECCIÓN, poseen información sobre el adversario y la legislación vigente en cuanto a los Sistemas de Protección Física.

Las organizaciones políticas, sindicales y de masas.

Estas organizaciones tienen la función de nuclear a las personas alrededor de las tareas del Partido y del Estado; entre sus misiones específicas encontramos el enfrentamiento al delito como lo comprueban recientes proclamas de sus direcciones centrales. La experiencia acumulada por los trabajadores y la población general en el enfrentamiento al delito común y al delito contrarrevolucionario. Aquí podemos encontrar a:

1. Las organizaciones de base y comités del Partido Comunista de Cuba y la UJC.
2. Las secciones sindicales y sus buros.
3. Los CDR
4. Las FMC
5. La asociación de Combatientes de la Revolución.
6. Etc.

DESCRIPCIÓN DEL MODELO

El gran desarrollo tecnológico del sector de la seguridad hace razonable intentar incorporarle tecnología a los sistemas de protección física que se emplean, de manera que se aprovechen estas en beneficio de la operabilidad de las mismas; pero ello exige de una mayor preparación del perso-

nal encargado de tomar la decisión sobre la composición y estructura de los sistemas de protección física, en ayuda de lo cual han surgido los sistemas de simulación.

A finales de los años 60 tomo fuerza en muchos países desarrollados la idea de diseñar modelos numéricos orientados a describir la situación de seguridad de instalaciones sensibles del tipo militar o nuclear. Ya entre los 70 y 80 se desarrollaron modelos analíticos asistidos por computadoras para evaluar la eficacia de los sistemas de protección física. Algunos de estos modelos son muy buenos para el análisis de la amenaza interna, mientras otros son mejores para analizar amenazas externas. Entre los modelos desarrollados tenemos los siguientes:

ASSES	EASI
(Analytic System and software for Evaluating Safeguard and Security). Un modelo del estado del arte, en uso por el Ejército Norteamericano, que incorpora la amenaza interna en un modelo SAVI (System Analysis Of Vulnerability to Intrusion) de avanzada metodología. Los datos de salida que entrega el modelo son una ordenación de trayectorias de la amenaza de una instalación.	(Estimate of Adversary Sequence Interruption). Un simple y fácil método para evaluar el desempeño de un sistema de protección física a lo largo de una trayectoria específica y bajo condiciones específicas de amenaza y operación del sistema. Este modelo computa una probabilidad de interrupción desde el análisis de las interacciones de detección, demora, respuesta, y comunicación.
FESEM	ISEM
(Forcible Entry Safeguards Effectiveness Model). Un modelo para el análisis de la eficacia de una instalación cerrado contra una entrada que es forzada y atacada por un adversario. El modelo analiza una entrada forzada a lo largo de una trayectoria asumida por un adversario con un conjunto de atributos asumidos.	(Insider Safeguards Effectiveness Model). Un modelo que simula un grupo del interior intentando el robo de material o sabotaje a la instalación. Los datos de entrada relativos a la eficacia del sistema de control de personal, los sensores, detectores de puerta, y la táctica de la fuerza de resguardo son muy subjetivos.
MAIT	SAFE

(Matrix Analysis of the Insider threat). Este modelo está basado sobre matrices. Requiere aportes extensivos de entrada, sobre todo internos y cualquier aporte externo de interés, actuando en conjunto o solo. Lo que también requiere un conjunto amplio de planta y parámetros de protección física. El modelo analiza cada combinación posible de trayectoria, condición de amenaza y escenario de colusión y entonces imprime todas las trayectorias y condiciones en orden descendente.	(Safeguards Automated Facility Evaluation). SAFE toma los datos de entrada relativos a la instalación, los aspectos físicos de protección, las trayectorias del adversario, y la fuerza de respuesta y selecciona las trayectorias más vulnerables a través de una instalación.
SAVI	SNAP
(System Analysis of Vulnerability to Intrusion). Este modelo conduce un análisis comprensivo de diagramas de secuencia del adversario (DSA), en uso por la OIEA. Una vez ingresados los datos sobre la amenaza, objetivo, estado de la instalación, sitio específico del Sistema de Protección Física, distancia de transmisión y tiempo de la protección de la fuerza de respuesta, el SAVI calcula las diez trayectorias más vulnerables.	(Safeguards Network Analysis Procedure). EL SNAP emplea la red modelando acercamientos a la solución del problema. Requiere un analista para modelar la instalación, la fuerza de respuesta y la fuerza del adversario. SNAP es altamente dependiente del escenario y entrega una medida de eficacia del SPF contra un cierto escenario.

Esta no es de ninguna manera una lista completa, porque continuamente se están desarrollando nuevos modelos, pero nos da una idea de los tipos de modelos que están disponibles.

EL MODELO SAVI (SYSTEMATIC ANALYSIS OF VULNERABILITY TO INTRUSION)

En nuestro trabajo vamos a utilizar el modelo SAVI porque conduce a un análisis comprensivo de diagramas de secuencia del adversario para evaluar la efectividad del Sistema de Protección Física. El SAVI determina la trayectoria más vulnerable como una medida de la efectividad. Comienza con la identificación de un objetivo y la construcción de un diagrama de secuencia del sitio específico para el adversario de ese objetivo. A continuación, deben ser especificadas las características de la amenaza. Deberán también definirse el tiempo de respuesta del despliegue y los valores de retardo y detección para cada elemento de protección en el DSA.

El SAVI es un programa computarizado, desarrollado para el análisis y comprobación de la efectividad de los SPF utilizando DSA. Este programa ha sido utilizado y esta disponible en las insta-

laciones del Departamento de Energía Nuclear de los EU. Este modelo ha demostrado se valía en los sistemas de protección nuclear y ha sido recomendado por la Organización Internacional de Energía Atómica (OIEA) para su empleo en el análisis y diseño de los 'SPF.

La medida de evaluación utilizada por el SAVI para la efectividad de los SPF es la probabilidad de interrupción $P(I)$ que se define como la probabilidad de que la fuerza de respuesta detenga a los adversarios antes de que estos completen su tarea, por lo tanto provee solamente una medida parcial de la efectividad. Existe otro factor necesario para evaluar adecuadamente la efectividad general del SPF que es la capacidad de neutralización del adversario. La capacidad de neutralización es una medida de la probabilidad de que la fuerza de respuesta neutralice con éxito el ataque del adversario luego que estas realizan la interrupción de su ataque. No obstante, SAVI posee una estimación de la misma.

El algoritmo del modelo SAVI

El algoritmo para el cálculo de $P(I)$ asume, conservadoramente que:

Los adversarios poseen conocimiento acerca de las características del sistema de protección. Ellos emplean una estrategia de penetración óptima.

Para que ocurra una interrupción deben existir las condiciones:

1. Los adversarios deberán ser detectados.
2. Deberán ser detectados en un punto de la "ruta del adversario" a partir del cual el tiempo que le quede al mismo para alcanzar su objetivo, tiempo de demora restante (TR), sea menor que el tiempo requerido por las fuerzas de respuesta para proceder a su interrupción (RFT).

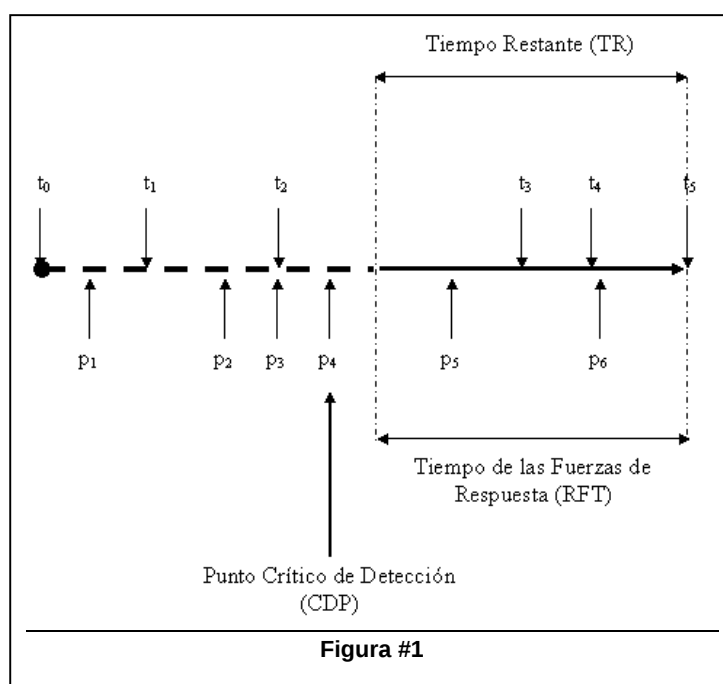
Por tanto la estrategia de penetración óptima estará dirigida a tratar de evitar la detección hasta que se alcance un punto en "camino del adversario" donde la demora restante no sea suficiente para permitir que las fuerzas de respuesta realicen la interrupción, y logrado esto proceder a minimizar la demora durante el resto del "camino del adversario".

En el DSA, una trayectoria (camino del adversario) consiste en una secuencia ordenada de elementos de protección a través de la instalación hasta el blanco, aunque también puede ser representada por una línea que representa los eventos en el camino del adversario desde el exterior de la instalación hasta el blanco. Estos eventos mostrados en la línea son:

1. Los componentes de detección $p_1, p_2, \dots, p_n$
2. El retardo acumulado ($t_0, t_1, \dots, t_n$) que producen las barreas y los componentes de retardo, el tiempo de tarea (tiempo utilizado por el adversario para vencer los elementos del SPF), y el tiempo de desplazamiento.

En la trayectoria del adversario existe un punto donde el tiempo que le resta al mismo para alcanzar su objetivo

(tiempo restante o TR) es igual al tiempo que requieren las fuerzas de respuesta para interceptarlo (RFT), este punto es llamado tiempo restante crítico (TR^*).



El punto de detección crítico (CDP) es aquel que se corresponde con el punto de detección previo al tiempo restante crítico (TR^*) y se conoce así porque la detección del adversario debe ocurrir en este punto o antes del mismo para que exista una interrupción. En la figura #1 el CDP corresponde con el punto de detección p_4 . De esta forma sólo existe dos vías en la que puede el adversario puede tener éxito:

Cuando el tiempo total del camino del adversario (t_5 en la figura #1) es mayor que el tiempo de las fuerzas de respuesta (RTF) pero el adversario no es detectado en un punto anterior al tiempo restante crítico (TR^*) lo cual sería como imaginar que no existieran los puntos de detección p_1, p_2, p_3 y p_4 de la figura #1.

Cuando el tiempo total del camino del adversario (t_5 en la figura #1) es menor que el tiempo de las fuerzas de respuesta (RTF).

Por otra parte, resulta evidente que en una situación como la mostrada en la figura #1, los elementos de detección p_5 y p_6 son ineficientes para la interrupción del adversario ya que el tiempo de retardo restante que le queda al adversario en su paso es menor que el tiempo que necesitan las fuerzas de respuesta para una interrupción oportuna. Tampoco parecería eficiente proveer mucho retardo a inicio del camino del adversario si esto no va acompañado de puntos de detección. Por lo que una estrategia defensiva básica se basará en garantizar una “detección en superficie” (lo más alejada del blanco) unida a un “retardo en profundidad” creciente cuanto más se acerca al blanco.

La estrategia de penetración óptima es aquella que emplearía un adversario que conoce los valores de demora (retardo) y detección de todos los componentes del SPF, así como y el tiempo de las fuerzas de respuesta; y que pudiera hacer los cálculos tal y como lo hace el SAVI. Esta estrategia consiste en proceder a través de la ruta minimizando la detección hasta que el tiempo de demora restante de retardo sea menor que el tiempo de las fuerzas de respuesta, y luego minimizar la demora sin tener en cuenta una detección posterior. Esta estrategia separa las funciones de demora y detección, debido a que el adversario está atacando un elemento tanto minimizando la demora como minimizando la detección, en dependencia de si paso o no el punto de detección crítico (CDP).

Si bien SAVI, no decide sobre la $P(I)$ y deja esto a la valoración de analista, concordamos con la escala establecida por R. Carvajal; por cuanto en ella se expresa un criterio que bien se adecua a los intereses de los sistemas de protección física cubanos.

La escala de decisión de R. Carvajal será adoptada para nuestro trabajo y la misma plantea que:

$P(I)$	Calificación	Sugerencias
(0.95 ; 1.00]	Excelente	El sistema de protección cuenta con los elementos y medios necesarios para detectar y neutralizar la amenaza
(0.80 ; 0.95]	Buena	El sistema de protección cuenta con la capacidad de interrumpir en buena forma la acción de la amenaza; pero puede implementar aún mejor su sistema

(0.50 ; 0.80]	Regular	Se debe efectuar una revisión a los componentes del sistema de protección, con los que posee actualmente, la instalación está vulnerable a la acción de la amenaza
(0.30 ; 0.50]	Vulnerable	Se debe efectuar un mejoramiento o rediseñar el sistema de protección
[0.00 ; 0.30]	Mala	El sistema se encuentra totalmente vulnerable a la acción de la amenaza, el rediseño del sistema es imperante

Para la evaluación de los SPF el modelo SAVI considera diez puntos básicos que son los siguientes:

1. **IDENTIFICAR LOS BLANCOS DEL ADVERSARIO.** En este paso se realiza una identificación y análisis de los blancos potenciales de la instalación y posteriormente se establece una prioridad para ellos basado en las consecuencias potenciales o su atractivo para el adversario. Esto permitirá la selección de los blancos más importantes para el análisis del SPF. Este paso tiene como objetivo modelar el SPF de la instalación tal y como está
2. **CONSTRUIR UN DSA ESPECÍFICO DEL SITIO.** La construcción de los diagramas de secuencia del adversario resultan una tarea compleja y da como resultado un DSA para cada blanco o conjunto de blancos que compartan una misma ubicación. Los DSA muestran un modelo correcto de la instalación. En los DSA se muestran las diferentes áreas que modelan la instalación y entre ellas se ubican los diferentes elementos de protección que encontrará el adversario al intentar pasar de un área a otra. SAVI representa un DSA genérico que contiene básicamente un área exterior, un área limitada, un área protegida y un área del blanco; y dispone de elementos de protección tales como: Puertas, Cercas, Ventanas, Superficies, Túneles, etc.
3. **ESPECIFICAR LAS CARACTERÍSTICAS DE LA AMENAZA.** La amenaza debe ser definida según el tipo de adversario y la capacidad del mismo. Para el SAVI las características de la amenaza se establece sobre la determinación de sus atributos y sus tácticas, así como a la determinación del equipamiento que este puede emplear todo lo cual tiene un impacto directo sobre la detección y el retardo. También reconoce tres tipos de tácticas del adversario en la definición de la amenaza: la fuerza, la artimaña o engaño y la combinada donde la fuerza como táctica considera que el adversario utilizará fuerza para vencer/derrotar todos los elemen-

tos de protección. La artimaña considera que el adversario utilizará preferentemente tácticas que permitan minimizar la detección y que utilizará la fuerza sólo si es necesario; y la táctica combinada supone que el adversario utilizará una combinación optima de la fuerza y la artimaña. La cantidad de adversario no es un atributo analizado por el SAVI no obstante, indirectamente se asume cuando se consideran parámetros de retardo y de probabilidad de neutralización entre otros.

4. **DEFINIR LAS ACCIONES DE LA FUERZA DE RESPUESTA.** Para SAVI la acción de las fuerzas de respuesta se realiza a partir de dos estrategias: privación y contención. La privación por lo general es la acción de las fuerzas de respuesta que se corresponde ante amenazas de sabotaje ya que sólo analiza la trayectoria del adversario comprendida desde el exterior de la instalación hasta el blanco. La estrategia de contención es propicia ante amenazas de robo ya que analiza la trayectoria del adversario desde el exterior de la instalación hasta el blanco y desde este hasta el exterior. Se debe notar que una estrategia de privación resultaría también efectiva ante amenazas de robo.
5. **DEFINIR EL TIEMPO DE DESPLIEGUE DE LA FUERZA DE RESPUESTA.** El tiempo de las fuerzas de respuesta (RTF) incluye los tiempos requeridos para la validación de primera alarma, los requeridos para la comunicación y los requeridos para el despliegue desde un punto de ubicación a un punto de interrupción dado. Este tiempo puede ser establecido en base a pruebas de campo u otras estimaciones realizadas. Es recomendable que al definir el tiempo de respuesta se considere el despliegue de un número suficiente de fuerzas capaces de neutralizar al adversario que ataque.
6. **DEFINIR LOS VALORES DE DETECCIÓN Y RETARDO.** El modelo SAVI utiliza el concepto de tiempo de detección analizando las vulnerabilidades del sistema de protección física. Estos requerimientos especifican la probabilidad de detección y retardo de los tiempos evaluados para cada elemento de protección. Los tiempos de retardo y probabilidad de detección son determinados usando las características de los elementos de protección específicos. Ambos el tiempo de retardo y la probabilidad de detección pueden ser asociados con cada segmento de la ruta en cada uno de los elementos de protección. El tiempo de retardo es definido como la demora presentada por el adversario a lo largo de un segmento de su ruta. La probabilidad de detección es la probabilidad de detectar un adversario a lo largo de un segmento específico de su trayectoria. SAVI utiliza valores de referencia para la probabilidad de detección y el retardo que se basan en experiencia de campo y/o el juicio de peritos que se obtuvieron en los laboratorios San Días.

7. INTRODUCIR LOS DATOS Y EJECUTAR EL SAVI. En este pasos e introducen los datos obtenidos en el SAVI verificando cada uno de ellos mediante la utilización del módulo FACILITY
8. EJECUTAR LOS ANÁLISIS DE SENSIBILIDAD. El análisis de sensibilidad se realiza para determinar el efecto de los cambios realizados en el SPF sobre su capacidad de respuesta, permitiendo revelar las incertidumbres sospechadas en el desempeño de las protecciones. De un análisis de sensibilidad se pueden determinar lugares donde un pequeño cambio producirá mejoras significativas en la efectividad del SPF y/o como un cambio pequeño en el tiempo de respuesta puede llevar a cambios significativos en la probabilidad de interrupción. Aquí se debe tener presente que la incertidumbre en el tiempo de respuesta puede ser grande por lo que las rutas que no tienen excedente de tiempo considerable después de la interrupción son candidatas de mejoras. En resumen, el análisis de sensibilidad permite: Investigar la sensibilidad de los resultados en los cambios de los valores de detección, retardo y respuesta; compensar la incertidumbre en los datos de respuesta y componentes, investigar las trayectorias con una probabilidad muy alta, y confirmar los resultados a través de pruebas y ejercicios.
9. EJECUTAR LOS ANÁLISIS DE ACTUALIZACIÓN. El SAVI no determina si los valores de probabilidad de interrupción son aceptables o no, esto es una decisión del analista; pero brinda facilidades para determinar las debilidades en las funciones de retardo y detección de cada uno de los puntos. El análisis de actualización del SPF permite: Estudiar la efectividad de la actualización de los sistemas de protección física antes de su implementación, reforzar un sistema balanceado, reforzar una protección profunda, buscar los puntos comunes de los elementos de protección con trayectorias de múltiples vulnerabilidad, y cambiar los RFT para afectar todas las trayectorias.

CONCLUSIONES DEL CAPITULO

1. A partir del marco teórico desarrollado es posible conocer las principales consideraciones teóricas en materia de seguridad, centrando la atención en los sistemas de protección física.
2. Luego de realizar un minucioso estudio sobre los principales modelos numéricos utilizados como herramientas en los sistemas de protección física, fue seleccionado el SAVI debido a conduce a un análisis comprensivo de diagramas de secuencia del adversario para evaluar la efectividad de dichos sistemas.

CAPITULO 2: EL OBJETO Y SU SISTEMA DE PROTECCIÓN ACTUAL

Para nuestro trabajo conceptualizamos el término de instalación en su sentido más amplio, comprende los elementos físicos, las funciones que se desarrollan y las personas pertenecientes a ella.

PRESENTACIÓN DEL OBJETO DE ESTUDIO

Como caso de estudio de consideró que la Empresa Servicios Portuarios Tricontinental, empresa que está sujeta a las exigencias de la Organización Marítima Internacional y del Estado cubano en cuanto a la seguridad portuaria.

La Empresa Servicios Portuarios Tricontinental, perteneciente al Grupo Empresarial ASPOR, subordinada al Ministerio del Transporte se encuentra ubicada en la zona industrial # 2 O'bourke Cienfuegos, fue transferida al MITRANS en septiembre del 2006. Siendo esta anteriormente la Empresa comercializadora, operadora y negociadora del azúcar y sus derivados (con azúcar) perteneciente al grupo Empresarial ECONAZUCAR.

Limita al Norte con terreno yermo y vía férrea ramal refinería, al sur con la Empresa de Servicios Portuarios del Centro y la bahía de Cienfuegos, al Este con el destacamento de tropas Guarda Fronteras, al Oeste con la Empresa de Cereales, ocupa una superficie de mas de 110.000 metros cuadrados. Comenzó sus operaciones el 9 de noviembre de 1967 después de casi 4 años de construcción con un costo aproximado a los 16 millones de pesos, era la tercera Terminal de azúcar a granel del país, después de Guayabales y Matanzas y constituía la mayor de Cuba y de América Latina.

Sus instalaciones permiten recibir más de 14'000 toneladas diarias de azúcar, procedente fundamentalmente de las provincias centrales del país Villa Clara, Cienfuegos y Sancti Spiritus; y su área de recepción recibe alrededor del 70% del azúcar por ferrocarril mediante tolvas romanas y el 30% por camiones.

Esta instalación cuenta con dos almacenes de azúcar a granel uno parabólico que tiene una capacidad de 90,000 toneladas y el otro tipo vara en tierra de teja de fibrocemento con una capacidad de 75,000 tonelada, construido en 1991 a un costo de mas de 5 millones de pesos incluido los

conductores correspondientes y su área total de almacenaje supera los 20'000 m² y cuenta con un espigón de 209 metros de largo, donde se realizan los embarques de azúcar mediante una grúa japonesa, con una capacidad de 750 toneladas/horas.

Actualmente, la instalación posee en uno de sus almacenes hay 30'000 toneladas de azúcar, prestan servicio de almacenaje de productos como soya, maíz, trigo, sus principales clientes en estos momentos son la fábrica de cereales, la fabrica de pienso, el porcino; y su plan de producción supera los 2'000'000 de pesos.

La misión manifiesta de la instalación esta definida como: “contribuir cada vez más al éxito de nuestros crecientes clientes al realizarles los servicios portuarios y conexos, incrementando los beneficios para la empresa, nuestros empleados y la comunidad, con la mirada al mañana y argumentación logística”, plantándose en su objeto social (aprobado la Resolución 254/2006 del Ministerio de Economía y Planificación) lo siguiente:

1. Prestar servicio de carga y descarga de buques, entongues y desentongues, estibas y desestibas, recepción y entrega, agrupe y desagrupe, embalaje y pesaje; atraque y desatraque en sus instalaciones de embarcaciones o medios de transporte marítimo, pase de muelle o traslado por las instalaciones portuarias o a través de las mismas que demanden armadores de buques, navieros, fletadores, importadores, exportadores vinculados al comercio de cargas o al transporte de pasajeros de mar, de almacenaje, deposito o entrega de cargas, remociones y clasificadores a bordo y en tierra; alquiler de equipos portuarios de transportación terrestre de carga vinculada a la actividad portuaria, todo ellos en pesos cubanos a las entidades vinculadas a la canasta básica, al resto del sistema Empresarial en pesos cubanos y pesos convertibles y a las entidades mixtas y extranjeras en pesos convertibles.
2. Brindar servicios telefónicos, de agua y electricidad a embarcaciones en pesos cubanos y en pesos convertibles y a entidades cubanas radicadas en el puerto en pesos cubanos.
3. Ofrecer servicio de informaciones concerniente a dichas cargas a entidades cubanas en pesos cubanos y a las Empresas mixtas y extranjeras en pesos convertibles.
4. Prestar servicio de custodia de cargas a las entidades cubanas en pesos cubanos y a las Empresas mixtas y extranjeras en pesos convertibles.
5. Comercializar de forma mayorista y minorista el modelo de orden de carga a los propietarios de mercancías en los puertos en pesos cubanos.

6. Ofrecer servicios de alquiler de locales y espacios en sus instalaciones, de contratación de mano de obra al Ministerio del Transporte; servicios ecológicos relacionado con el medio marino y aguas interiores; de limpieza de las incrustaciones de hidrocarburos en los frentes de las instalaciones hidrotécnicas y costas; de tratamiento de reciclaje y efectuar la comercialización mayorista de los desechos de hidrocarburos y sólidos a las entidades autorizadas y alquiler de medios navales y terrestre, todo ello en pesos cubanos.
7. Brindar servicio de alojamiento no turístico y de alimentación asociado al Ministerio del Transporte en pesos cubanos.

La instalación portuaria considera su visión como “Pertener a las entidades líderes del Grupo Empresarial, a partir de la obtención de resultados totalmente satisfactorios, tanto en el orden económico financiero como lo relacionado con la eficiencia en las operaciones portuarias”.

Dispone de una fuerza laboral constituida por 15 directivos, 12 técnicos, 2 administrativos, 12 de servicio y 129 obreros. (Ver anexo #3)

CARACTERIZACIÓN DE LA SEGURIDAD Y PROTECCIÓN ACTUAL

La instalación se encuentra en una zona considerada de alta ocurrencia de hechos delictivos y datos policiales revelan la existencia de concentraciones de potencial delictivo. Por otra parte, evaluaciones hechas por la AGESP, muestran que se puede esperar que se lleven a cabo acciones vandálicas o de sabotaje en la instalación a partir de adversarios externos.

En la frontera de la instalación existen áreas de gran enhierbamiento, otras sin cercado y con una iluminación pésima que facilita el actuar del adversario.

Existe un constante movimiento de personal y vehículos por la frontera norte de la instalación a pocos metros de esta, en esta frontera se encuentra un terreno yermo y la vía férrea ramal refinera y el cercado perimetral de esta zona se encuentra en mal estado y en algunos lugares no existe.

Por el perímetro oeste, la instalación limita con la Empresa de Cereales, la cual es custodiada por el SEPSA, pero el cercado perimetral se encuentra en mal estado, con deficiente iluminación y abundante enhierbamiento. Estos perímetros son custodiados por 10 Agentes de Seguridad y Pro-

tección de AGESP, mediante la observación y los recorridos que se realizan en el perímetro, en el horario laboral la seguridad del perímetro se ve fortalecida por el personal que trabaja en las distintas áreas, los que al detectar cualquier violación actúan o se le informa al personal de Seguridad y Protección para tomar las acciones pertinentes.

La instalación tiene contrato para la protección con la empresa de seguridad y protección del transporte (AGESP), la cual cuenta con personal calificado para brindar el servicio de Seguridad y Protección empleando un total de 36 Agentes de Seguridad y 4 jefes de turnos que cubren 9 postas fijas y 1 de recorrido en un régimen de trabajo que va de 10 a 24 horas diarias.

Las fuerzas de protección disponen de radios y teléfonos para su comunicación externa y cumplen las siguientes misiones generales en el servicio:

1. Impedir el acceso de intrusos por las fronteras y accesos de la instalación.
2. Detectar posibles amenazas externas e internas.
3. Brindar protección a la técnica, medios materiales y mercancías.
4. Evitar la penetración de adversarios en su sector de responsabilidad.
5. Neutralizar todo tipo de actividad contrarrevolucionaria.

Los ASP, además de los radios y teléfonos internos asignados para las posiciones más importantes, mantendrán comunicación con el resto de las posiciones mediante la ínter vigilancia y a través de un silbato para llamar al orden, alertar cualquier situación en su área o solicitar ayuda.

La empresa en estos momentos no cuenta con medios técnicos de Seguridad y Protección ni medios alternativos para apoyar el subsistema de detección.

IDENTIFICACIÓN DE BLANCOS

En la instalación fueron identificados inicialmente 9 blancos considerando que en ellos hay tecnología o recursos que por sus funciones específicas cumplen con el proceso de producción y los servicios que son esenciales para la adecuada ejecución de las operaciones inherentes al mismo y pueden constituir un riesgo potencial para la integridad física de los trabajadores y población resi-

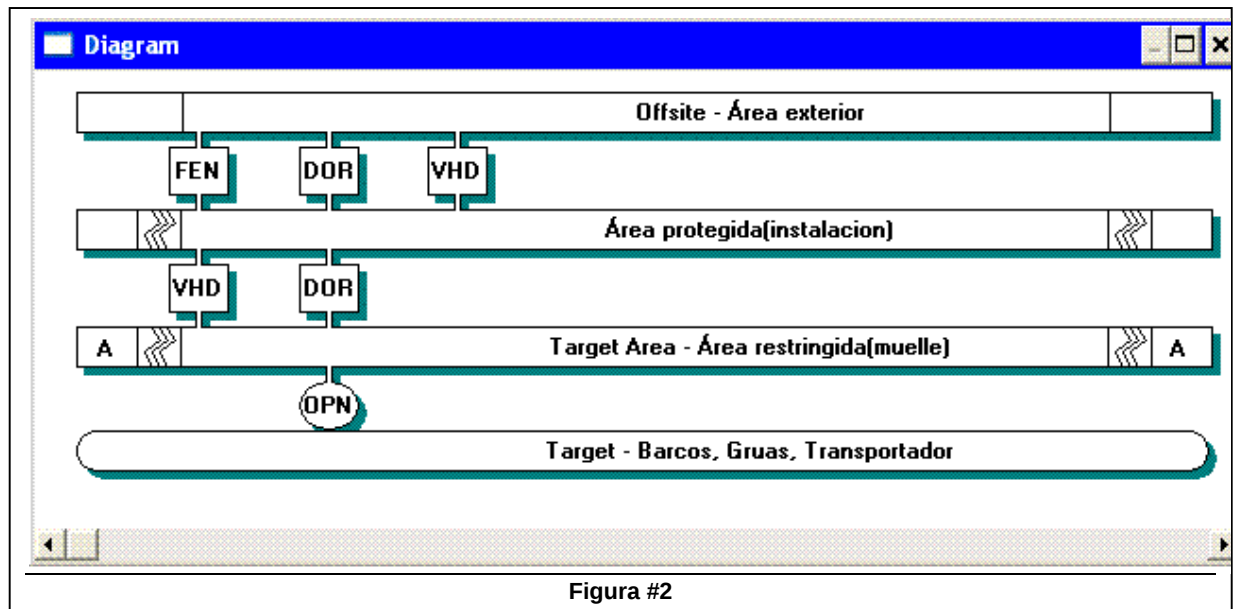
dentes en el área aledaña a la entidad, y que además resultan atractivos para el adversario. Estos son:

1. **Área de recepción:** Ubicada por la carretera a zona industrial, a la derecha de la entrada principal. Para su protección emplea: 2 ASP, barreras físicas, control de acceso y señalizaciones.
2. **Conductores:** Ubicación: Desde la recepción hasta el atraque por toda la empresa. Sus medidas de seguridad contempla la utilización de: 4 ASP, barreras físicas, control de acceso solo permanece en el mismo el personal del turno.
3. **Almacén no. 1 y 2:** Se encuentra en la parte Norte de la empresa junto al perímetro que colinda con la carretera a zona industrial. Se protege con: 2 ASP, posee puertas de acero se debe entregar a la seguridad cerrado y sellado.
4. **Torre de control del área de embarque:** Se encuentra en el interior de la empresa junto el perímetro Oeste y se protege con la utilización de: 1 ASP, barreras físicas, control de acceso y señalizaciones.
5. **Grúa de embarque:** Ubicado al final de la empresa en el atraque. Posee para su «-guridad: 1 ASP, barreras físicas, control de acceso y señalizaciones.
6. **Subestación eléctrica:** Se encuentra detrás de la torre de recepción y entre los almacenes 1 y 2. Es protegida mediante: barreras físicas, control de acceso y señalizaciones.
7. **Cuarto de compresores:** Debajo del conductor H y junto al perímetro Oeste se encuentra este punto vital que se protege con: Barreras físicas, control de acceso y señalizaciones.
8. **Cuarto de bomba y cisterna:** Se encuentra en el sur entre los dos almacenes de azúcar. Posee puertas y tapas de de acero control de acceso y señalizaciones.
9. **Atraque:** Ubicado en la parte Sur de la empresa al final de la instalación, colindante con el atraque de la empresa de cereales. Es protegido mediante 1 ASP y señalizaciones.

Especialistas de protección de SEPSA, especialistas de la sección de Protección Física del MININT y funcionarios de la instalación, entre otros que realizan parte de las indicaciones del Estado sobre seguridad portuaria, decidieron que el blanco más prioritario en cuanto a la protección física de la instalación resultaba el área de atraque razón por la cual forma parte de nuestro estudio.

DIAGRAMA DE SECUENCIA DEL ADVERSARIO

El diagrama de secuencia del adversario para evaluar la protección actual que poseen el conjunto de blancos ubicados en el área de atraque quedó de la siguiente manera:



La inspección in situ de la protección actual del área de atraque nos llevo a comprobar que en existen en la misma tres grandes conjuntos de blancos sumamente importantes que son:

- a) las embarcaciones,
- b) las grúas y el
- c) transportador.

A estos blancos se puede acceder a través de un elemento de protección que se representa como un emplazamiento abierto (OPN) desde el área restringida del muelle a la cual se accedía desde el área protegida de la instalación a través de dos elementos de protección:

1. una puerta vehicular (VHD) y
2. una puerta de personal (DOR)

Estos elementos de protección se encuentran físicamente en el mismo lugar; pero en su funcionalidad se dividen en dos dadas las protecciones y otras características de estos.

Por otra parte se determinó, en la inspección in situ, que al área protegida de la instalación sólo se puede acceder, desde el área exterior, a través de:

1. un cercado perimetral (FEN),
2. una puerta de personal (DOR) y
3. una puerta vehicular (VHD).

CARACTERÍSTICAS DE LA AMENAZA

Considerando los riesgos y las vulnerabilidades existentes por las características de sus perímetros que permite acceso de áreas aledañas, fueron identificadas amenazas en relación a:

1. Robo.
2. Sabotaje.
3. Incendio.
4. Destrucción de la información.
5. Agresión.

La determinación detallada de la amenaza y la priorización de su importancia a la luz de las exigencias de las instalaciones portuarias nos permitió determinar que la amenaza de mayor impacto potencial sobre la instalación sería proclamada como sigue:

1. Se considera la acción de adversarios externos (que son personas que no pertenecen a la instalación) con motivaciones ideológicas (contrarios a nuestra ideología y por lo general son fuentes de acciones potenciales de alta gravedad y elevados daños)
2. Estos emplearán principalmente la táctica del sigilo y la fuerza en último caso
3. Su objetivo será sabotear los blancos ubicados en el área de atraque.
4. Que en cantidad no deben superar las dos personas, no deben utilizar armamento, ni otras herramientas, así como tampoco deberán utilizar transporte para moverse dentro de la instalación; pero si deben tener conocimiento de la misma y del sistema de protección actual y,
5. No deben contar con apoyo interno

LAS ACCIONES DE LA FUERZA DE RESPUESTA

En la instalación después de definidas las principales amenazas determinamos la acción de fuerza de respuesta para el objeto de estudio y establecemos que la acción a emplear es la basada en la estrategia de contención porque las amenazas latentes conllevan a que esta estrategia es de gran efectividad tanto para el robo, como para el sabotaje.

(Criterio del cliente), por demás las exigencias de la protección portuaria implican que se deben considerar el robo y el sabotaje, e incluso para el mismo cliente resulta mas efectivo contar con unas fuerzas de respuestas que fueran capaces de neutralizar a los intrusos tanto a la salida como en la entrada, en fin si consideramos un intruso que intente un sabotaje no se considerara al mismo un extremista y en consecuencia este debe salir de la instalación.

LA DETECCIÓN Y EL RETARDO

Para SAVI, la detección y el retardo se expresan a través de las características de los elementos de protección y las áreas, y para nuestro modelo de SPF las principales características de las mismas son las siguientes:

Elementos	Características
Cercado desde el Área exterior hasta el Área protegida (instalación).	Alarmas: No presenta sistema de alarma. Detección de intrusos: Personas generalmente cerca en el interior. Retardo de acceso: El cercado compuesto de malla a 8 pies en cadena. Agentes de seguridad y protección: Por el exterior del cercado patrullas aleatoriamente y por el interior patrullas aleatorias.
Puerta entrada de personal desde el Área exterior hasta el Área protegida (instalación).	Alarma: Desplazamiento oportuno Paso: Personas (Peatones), paquetes, Posesiones personales, Equipos y herramientas. Control de Acceso: Comprobación de Identificación personal, por la credencial. Evacuación de Alarma: Activación manual Detección de Contrabando: Búsqueda de objetos, Posesiones personales, Paquetes, Equipos y herramientas.(Búsqueda rigurosa) Detección de Intrusión: Personal siempre cercano. Retardo de acceso: Puerta. Agente de seguridad y protección: Un agente de posta, en una garita desprotegida y otro agente de patrulla aleatoria.

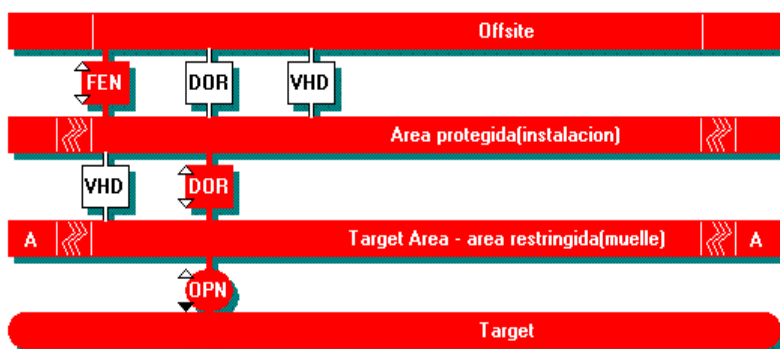
Elementos	Características
Puerta entrada de Vehículos desde el Área exterior hacia el Área protegida (instalación)	Alarma: No posee. Sistema de alarma. Paso: Personas, Peatones, Chóferes, Cargas y paquetes, Posesiones personales, Paquetes, Equipos y herramientas, Cargamentos Vehículos: Vehículos personales, Vehículos del sitio, Vehículos de carga. Control de Acceso: Chequeo de autorización de Vehículos, personales, del sitio, de carga. Chequeo visual de la licencia, y para los vehículos de carga comprobación de las facturas, para los peatones y chóferes comprobación de la credencial. Evacuación de Alarma: Activación manual. Detección de Contrabando: Búsqueda de objetos, Posesiones personales, Paquetes, Equipos y herramientas, Cargamentos. (Búsqueda rigurosa). Revisión de vehículos: Personales, del sitio, de carga. (Riguroso, incluyendo la carga). Detección de Intrusos: Personal generalmente cercano al lugar. Retardo de acceso: Barrera para vehículos. (Cable aéreo) Agente de seguridad y protección: Posta en una garita desprotegida.
Puerta de entrada vehículos desde el Área protegida (instalación), hasta el Área restringida (muelle).	Alarma: No posee sistema de alarma. Paso: Personas, Peatones, Chóferes, Cargas y paquetes, Posesiones personales, Paquetes, Equipos y herramientas, Cargamentos. Vehículos: personales, de la instalación y de carga. Control de Acceso: Chequeo de autorización de vehículos: personales, de la instalación, de carga, un chequeo visual de la licencia y para los vehículos de carga comprobación de las facturas. Chequeo de autorización por formulario, comprobación de Identificación de las credenciales: Peatones, Chóferes Evacuación de Alarma: Activación manual. Detección de Contrabando: Búsqueda de objetos, Posesiones personales, Paquetes, Equipos y herramientas, Cargamentos. (Búsqueda rigurosa). Revisión de vehículos: Revisión rigurosa (incluyendo la carga) de los vehículos del personal, de la instalación y sus cargas. Detección de Intrusión: Personal siempre en la cercanía al lugar Agente de seguridad y protección: Patrulla la entrada de la puerta de vehículos de forma aleatoria

Elementos	Características
Puerta de entrada de personal desde el Área protegida (instalación) hacia el Área restringida (muelle)	Alarma: No posee sistema de alarma. Pasos: Personas (Peatones), paquetes, posesiones personales, equipos y herramientas. Control de Acceso: Comprobación de Identificación personal por credencial. Evacuación de Alarma: Activación manual Detección de Contrabando: Búsqueda rigurosa de objetos, de posesiones personales, paquetes, equipos y herramientas. Detección de Intrusión: Personal siempre cercano. Retardo de acceso: Puerta. Agente de seguridad y protección: Agente de posta en la entrada y patrullando aleatoriamente.
Emplazamiento abierto Localizado en el Área restringida (muelle)	Alarma: Desplazamiento oportuno Control de Acceso: Chequeo de acceso al personal, autorización de entrada. Evacuación de Alarma: Solamente una señal es requerida. Detección de Intrusión: Personal generalmente cercano al lugar. Retardo de acceso: Un tiempo mínimo de trabajo en el área. Agente de seguridad y protección: Una posta sin garita y patrullando aleatoriamente.

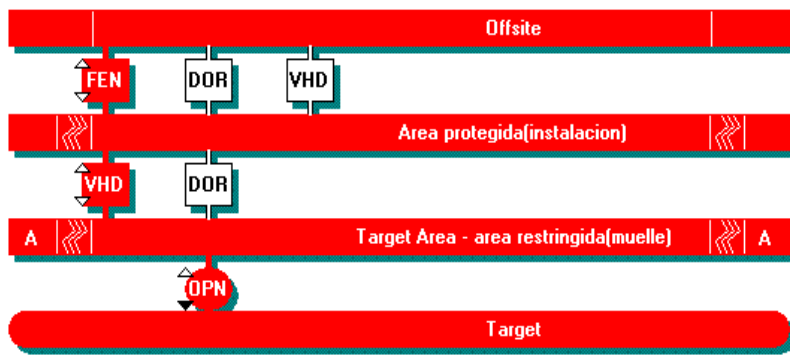
Establecidas estas características del SPF procedimos a realizar un análisis de sensibilidad del mismo ante la amenaza anteriormente definida.

ANÁLISIS DE SENSIBILIDAD DEL SPF ACTUAL

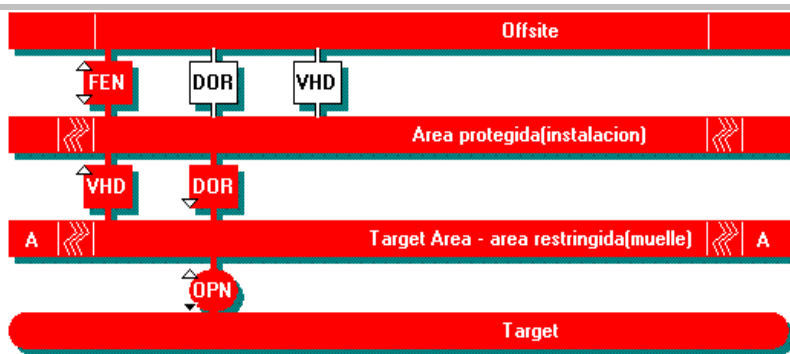
El análisis de sensibilidad del SAVI, nos permitió identificar las principales rutas del adversario o rutas más críticas que resultaron ser las siguientes:



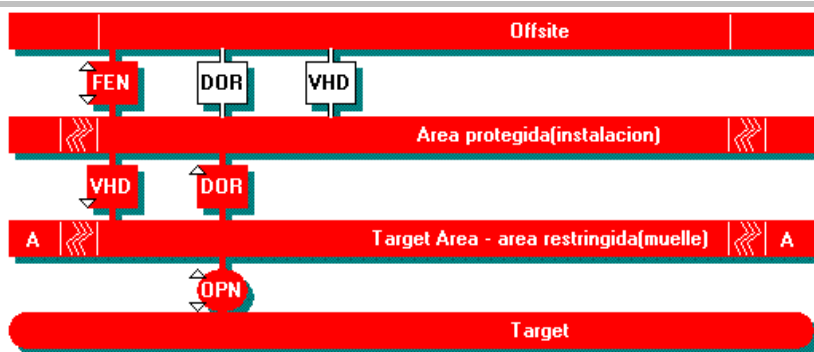
(R1) El adversario entra por la cerca al área protegida de la instalación y de esta pasa al área de los blancos por la puerta de personal y luego sale al exterior retrocediendo por el mismo lugar por el camino andado.



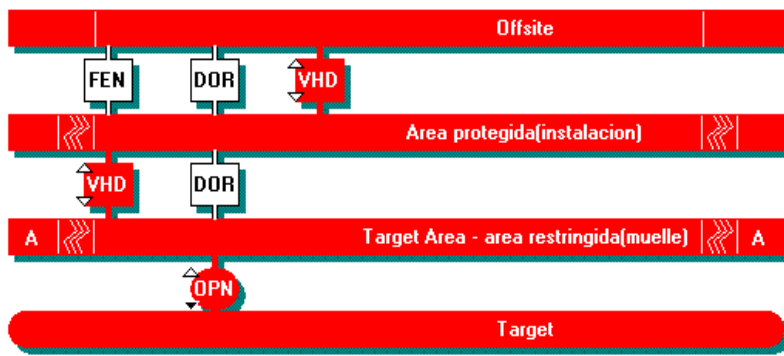
(R2) El adversario entra al área de la instalación por el cercado perimetral y de allí pasa al área de los blancos por la puerta vehicular. Luego retorna al exterior por regresando por el camino andado.



(R3) El adversario entra a la instalación por el cercado perimetral, luego pasa al área de los blancos por la puerta de acceso peatonal. Para regresar lo hace por el control de acceso vehicular hasta el área protegida de la que sale por el cercado perimetral.



(R4) El adversario entra al área protegida por el cercado perimetral, de allí pasa al área de los blancos por la puerta de control vehicular y sale de esta por el control de acceso de personal hasta el área protegida de la que sale al exterior por el cercado perimetral.



(R5) El adversario entra a la instalación por el control de acceso vehicular llegando al área protegida desde donde pasa al área restringida por la segunda puerta vehicular y retorna al exterior retrocediendo por el mismo camino por donde entró.



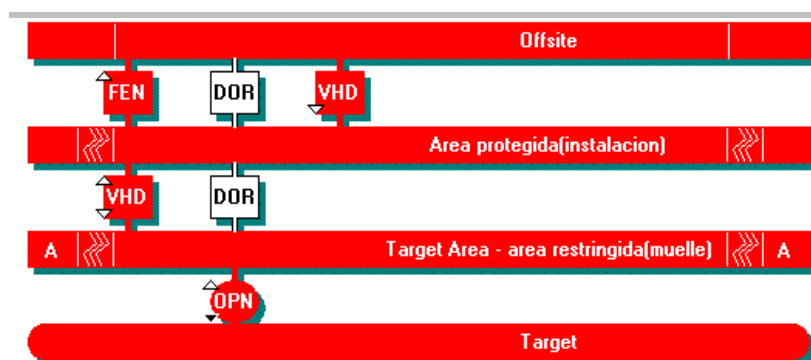
(R6) El adversario entra a la instalación por el control de acceso de personal llegando al área protegida. De allí sigue para el área restringida por la puerta vehicular y regresa al exterior siguiendo este camino a la inversa.



(R7) El adversario entra al área restringida pasando por la puerta de personal. Sigue para el área restringida pasando por la puerta de personal de la misma y regresa siguiendo este camino a la inversa.



(R8) El adversario entra a la instalación por el control de acceso vehicular llegando al área protegida desde donde pasa al área restringida por la puerta de personal y retorna por la misma siguiendo este camino a la inversa.



do este camino a la inversa.

(R9) El adversario entra a la instalación por la puerta de control de acceso vehicular hacia el área protegida y pasa para el área restringida por la segunda puerta vehicular regresando por la misma puerta alcanzando el cercado.



(R10) El adversario entra a la instalación por la puerta de control de acceso vehicular hacia el área protegida y pasa para el área restringida por la segunda puerta vehicular regresando hacia el área protegida a través de la puerta de entrada de personal alcanzando el cercado.

Apreciamos que la situación que presenta la seguridad de los blancos ante la amenaza valorada es crítica. El 40% de los caminos del adversario muestran una probabilidad de interrupción muy baja, ninguna sobrepasa el 14%, siendo en consecuencia muy vulnerable el sistema ante esta amenaza. Dado que resulta fácil para el adversario entrar a la instalación, llegar al blanco y salir de la misma sin que la fuerza de respuesta tenga el tiempo suficiente para neutralizar la acción.

Las rutas que aportan la mayor criticidad al sistema son la R1, R2, R3 y R4. Las siguientes figuras muestran la probabilidad de interrupción del adversario para cada una de dichas rutas.

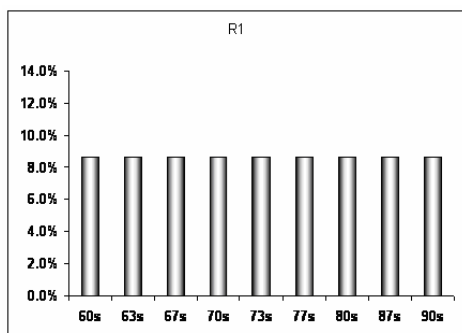


Figura #3

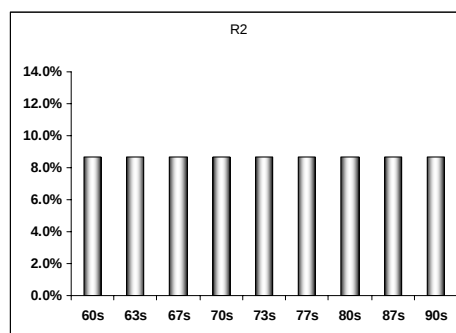


Figura #4

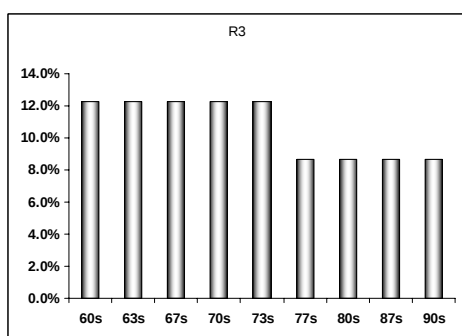


Figura #5

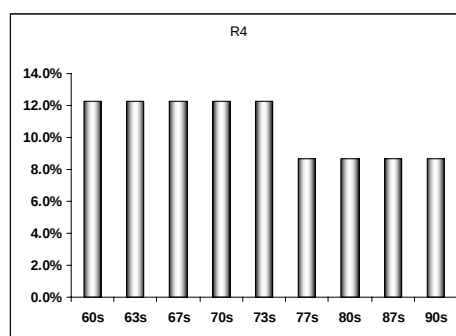


Figura #6

Resulta evidente que en el rango de tiempo empleado por la fuerza de respuesta a fin de interceptar el adversario, no existe ninguno en los que obtengan una probabilidad de interrupción que garantice la eficacia, ni la efectividad del sistema de protección física.

Análisis de la ruta 1

Dentro de la ruta R1 podemos encontrar dos puntos críticos de detección. Uno se encuentra en la misma área del muelle y otro en la puerta de salida de la instalación. El primero se alcanza si las fuerzas de respuestas garantizan un RTF entre 77 y 90 segundos y el segundo si estas pueden operar con un RTF entre 60 y 73 segundos. Dada esta situación las mejoras posibles comprenderían: la utilización de una posta fija en el control de acceso del muelle, un sistema de detección de

intrusos en el cercado perimetral del mismo y/o un sistema de CCTV que cubra el área del muelle entre otros.

Análisis de la ruta 2

En esta ruta encontramos también dos puntos críticos de detección. El primero aparece para un RTF entre 60 y 70 segundos y está ubicado en el control de acceso de personal al área del muelle y el segundo aparece para un RTF entre 77 y 90 segundos ubicado en el mismo muelle.

Una mejora del desempeño del sistema sobre esta ruta pudiera estar basada en la utilización de un sistema de detección de intrusos sobre el cercado del muelle y la colocación de una puerta que controle el acceso del personal al muelle para aumentar el retardo del adversario entre otras propuestas.

Análisis de la ruta 3

Al igual que las anteriores, esta ruta posee dos puntos críticos de detección y uno se encuentra también situado en el muelle por cuanto las mejoras propuestas anteriormente le son aplicables. El segundo punto crítico de detección se encuentra en la puerta de control de acceso de personal al área del muelle cuando el adversario intenta salir por la misma.

Análisis de la ruta 4

Igualmente posee dos puntos críticos de detección muy cercanos al área de los blancos. Uno se ubica en el mismo muelle y el otro a la salida de este por la puerta de vehículos. Todas las mejoras mencionadas en las rutas anteriores son aplicables a esta.

Valoración general

Aplicando el criterio de R. Carvajal podemos concluir que como la P(I) en estas rutas es inferior a 0.30 la calificación del sistema es MALA, y que es encenrándose totalmente vulnerable a la acción de la amenaza, es imperante el rediseño del mismo.

Por otra parte, el análisis de sensibilidad nos permitió ver que es necesario este mejoramiento y que se puede lograr a través de los elementos de retardo y detección que se encuentran actualmente en la instalación como son: el cercado perimetral que en algunas áreas se encuentra en muy mal estado y con suficiente hierba en su parte exterior imposibilitando a las fuerzas de respuestas de una oportuna detección, un sistema de detección en el mismo cercado perimetral y la colocación de una puerta entre otros.

No se quiere decir que el sistema no cumpla su objetivo pero es evidente que incrementando elementos de detección y retardo el mismo puede tener una probabilidad de interrupción del 100% en cualquiera de sus rutas.

CONCLUSIONES DEL CAPÍTULO

1. A partir de la utilización del modelo SAVI fue posible demostrar que la protección física existente en la empresa no garantiza una seguridad efectiva ante la amenaza analizada.
2. La capacidad del modelo SAVI fue validada teniendo en cuenta que los resultados obtenidos demostrando su utilidad en el análisis y diseño de instalaciones no nucleares.

CAPÍTULO 3: RESULTADOS Y DISCUSIÓN.

ALTERNATIVAS DE MEJORAS DEL SISTEMA DE PROTECCIÓN FÍSICA

En el análisis de sensibilidad realizado en el capítulo anterior pudimos comprobar que SAVI realizó una serie de propuestas de mejoras para el sistema de protección física. Estas propuestas son consideradas como “alternativas posibles” de mejora y son resumidas de la siguiente manera:

1. Para la ruta (R1) se hace necesario tener en cuenta:
 - a) Poner una posta fija de agente de seguridad y protección en la entrada del muelle para que controle con mayor efectividad el acceso al mismo,
 - b) Poner un sistema de detección de intrusos en el muelle para asegurar una mayor probabilidad de detección en el área,
 - c) Poner un sistema de detección de intrusos en el cercado perimetral del área del muelle para aumentar la probabilidad de detección del adversario por el mismo,
 - d) Colocar detectores en la puerta de entrada de personal al muelle, y
 - e) La utilización de un sistema de sistema de CCTV para cubrir toda el área del muelle.
2. Para la ruta (R2) se hace necesario tener en cuenta:
 - a) Poner un sistema de detección de intruso en la puerta de entrada de personal.
 - b) Colocar una posta fija con un agente de seguridad y protección en la puerta para el control de acceso.
 - c) Colocar una puerta en la entrada de personal que no posee para retardar la entrada.
3. Para la ruta (R3) es necesario tener en cuenta:
 - a) Poner un agente de seguridad y protección en una torre para una mayor observación de penetración del adversario.
 - b) Poner un sistema de detector de intrusos en el interior del muelle para detectar cualquier acceso al mismo.
 - c) Utilizar un sistema de CCTV para cubrir toda el área

4. Para la ruta (R4) se hace necesario tener en cuenta:

- a) Poner una posta con un agente de seguridad y protección en la puerta de control de acceso de vehículos.
- b) Colocar un agente de seguridad y protección en una torre para asegurar una mayor probabilidad de interrupción en el área.
- c) Poner detectores de intrusos tanto en la parte interior de la puerta de vehículos como en la parte exterior.

PROCESO DE ANÁLISIS Y SELECCIÓN DE LAS MEJORAS DEL SISTEMA DE PROTECCIÓN FÍSICA

Las alternativas de mejora anteriores fueron analizadas con especialistas y funcionarios de la empresa y con los especialistas de protección de SEPSA Cienfuegos, que laboran en el tema de la seguridad portuaria y llegamos a perfilar las alternativas más objetivas para el sistema de protección física. Se tuvo en cuenta la relación costo – beneficio en la decisión excluyéndose de la misma aquellas propuestas que proponían la utilización de un sistema de CCTV ya que el valor del mismo sobrepasaba los \$1'560 CUC y la empresa no disponía de recursos financieros para enfrentar una inversión de esta magnitud.

El tema de los costos de implementación y la capacidad de la empresa para cubrirlos hizo que se considerara como viable la implementación de un sistema de detección de intrusos que sería integrado a uno cuya inversión está en fase de aprobación por el organismo superior. También se consideraron viables la mejora del cercado perimetral y la utilización de barreras físicas como las puertas.

También resultó del análisis que sería igualmente viable el incremento de al menos una nueva posición de agentes de seguridad a negociar con la empresa AGEPS que actualmente le presta servicios.

Con estas premisas, conformamos cuatro variantes de mejora que modificaron el modelo SAVI. Todas estas variantes fueron sometidas a un análisis de sensibilidad y se obtuvieron los mejores resultados en la variante #3 la cual quedó conformada por los siguientes elementos de mejora.

1. En el cercado desde el área exterior hasta el área protegida (instalación), se propuso la mejora del retardo y la detección a través de realizar una reparación de su cercado perimetral y poniendo en el mismo un sistema de detección de intrusos (barreras perimetrales).
2. En la puerta entrada de personal desde el área exterior hasta el área protegida (instalación). Se propuso la colocación de detectores de intruso y una puerta de madera.
3. Para la puerta de entrada de vehículos desde el área exterior hacia el área protegida (instalación) y teniendo en cuenta la importancia de esta puerta, se propuso la colocación un agente de seguridad y protección; y se dota la misma con una barrera de vehículos.
4. En la puerta de entrada vehículos desde el área protegida (instalación) hasta el área restringida (muelle); se propuso la colocación de una barrera de vehículos y una posta de agente de seguridad y protección;
5. Por la puerta de entrada de personal desde el área protegida (instalación) hacia el área restringida (muelle) propusimos la colocación de detectores de intrusos; y
6. En la propia área del muelle se planteó la utilización de barreras perimetrales, la colocación de un agente de seguridad y protección en la parte delantera del muelle y otro en la parte de atrás.

Señalamos, como en capítulos anteriores se explicó, que estas mejoras están orientadas a los elementos de protección concebidos en el modelo y que las puertas vehiculares y peatonales establecidas se encuentran ubicadas en el mismo lugar físico; por cuanto existen mejoras que incidirán directamente en el incremento del desempeño de ambas a la vez; y en las puertas, la función de detección (sistema de detección) es realizada por los agentes de seguridad que se conciben para ellas.

DEMOSTRACIÓN DE LA VALIDEZ DE LA SOLUCIÓN

El análisis de sensibilidad de la variante #3 de mejora mostró un excelente desempeño del sistema de protección física. Como era de esperar, al introducir las mejoras, las rutas del adversario cambiaron, quedando de la siguiente forma:



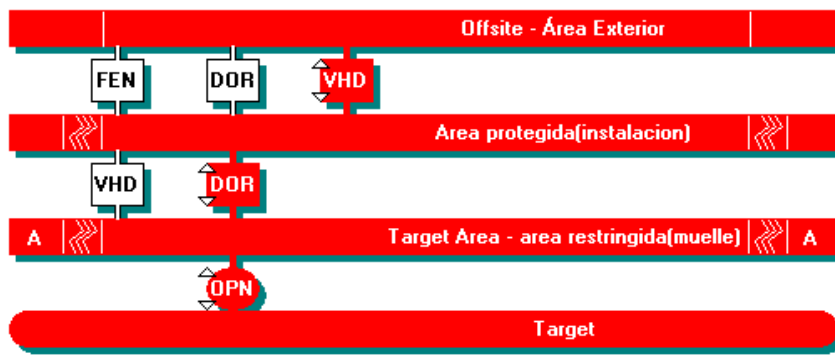
(R1) El adversario entra a la instalación por la puerta de control de acceso vehicular hacia el área protegida y pasa al área restringida a través de la puerta de control de acceso vehicular, luego sale al exterior retrocediendo por el mismo lugar.



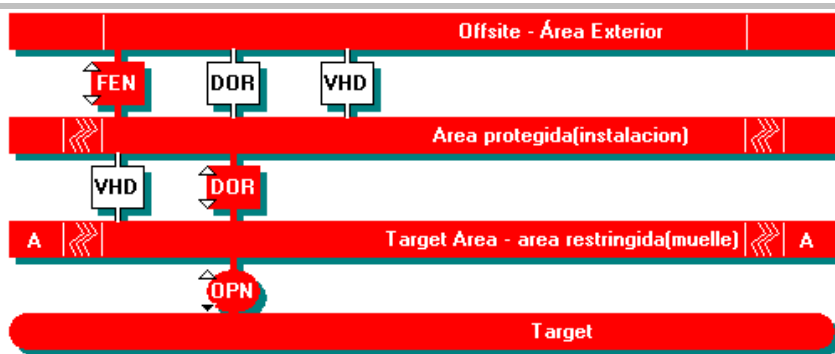
(R2) El adversario entra al área de la instalación por la puerta de control de acceso de personal y de allí pasa al área de los blancos por la puerta vehicular. Luego retorna al exterior regresando por el mismo camino andado.



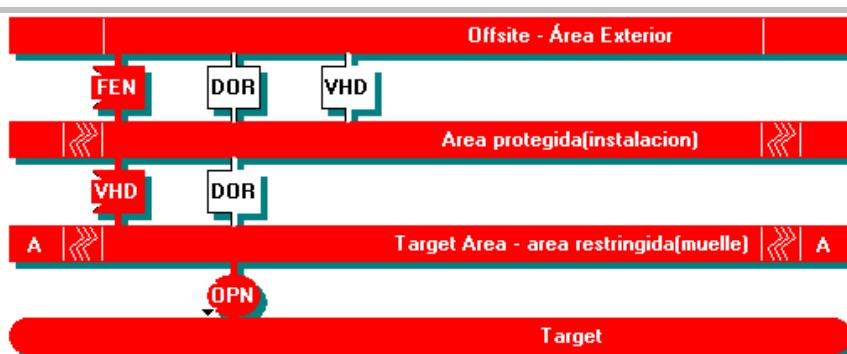
(R3) El adversario entra a la instalación por la puerta de control de acceso de personal, luego pasa al área de los blancos por la puerta de control de acceso peatonal. Para regresar realiza el mismo recorrido anteriormente.



(R4). El adversario entra a la instalación por el control de acceso vehicular llegando al área protegida desde donde pasa al área restringida por la puerta de control de acceso de personal y retorna al exterior retrocediendo por el mismo camino por donde entró



(R5) El adversario entra a la instalación por el cercado llegando al área protegida desde donde pasa al área restringida por la puerta de control de acceso de personal y retorna al exterior retrocediendo por el mismo camino por donde entró.



(R6) El adversario entra a la instalación por el cercado perimetral llegando al área protegida. De allí sigue para el área restringida por la puerta vehicular y regresa al exterior siguiendo este camino a la inversa.



(R7) El adversario entra a la instalación por el control de acceso vehicular llegando al área protegida desde donde pasa al área restringida por la puerta de control de acceso vehicular y retorna por la puerta de control de acceso de personal hacia el área protegida y hace salida por la puerta de control de acceso vehicular.



(R8) El adversario entra a la instalación por el control de acceso personal llegando al área protegida desde donde pasa al área restringida por la puerta de control de acceso vehicular y retorna por la puerta de control de acceso de personal hacia el área protegida y hace salida por la puerta de control de acceso de personal por donde mismo entro.

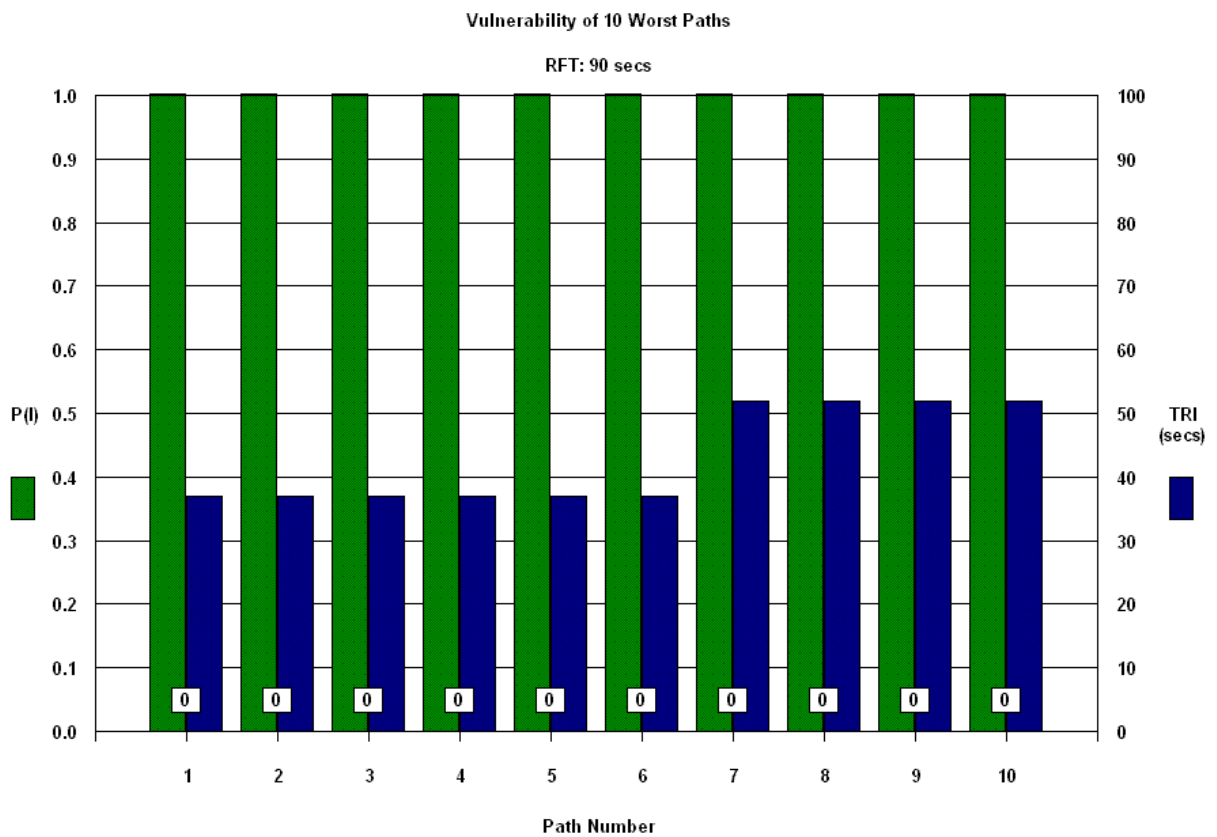


(R9) El adversario entra a la instalación por la puerta de control de acceso personal hacia el área protegida y pasa para el área restringida por la segunda puerta de acceso de personal regresando por la puerta de acceso vehicular hacia el área protegida saliendo por el mismo lugar de entrada.



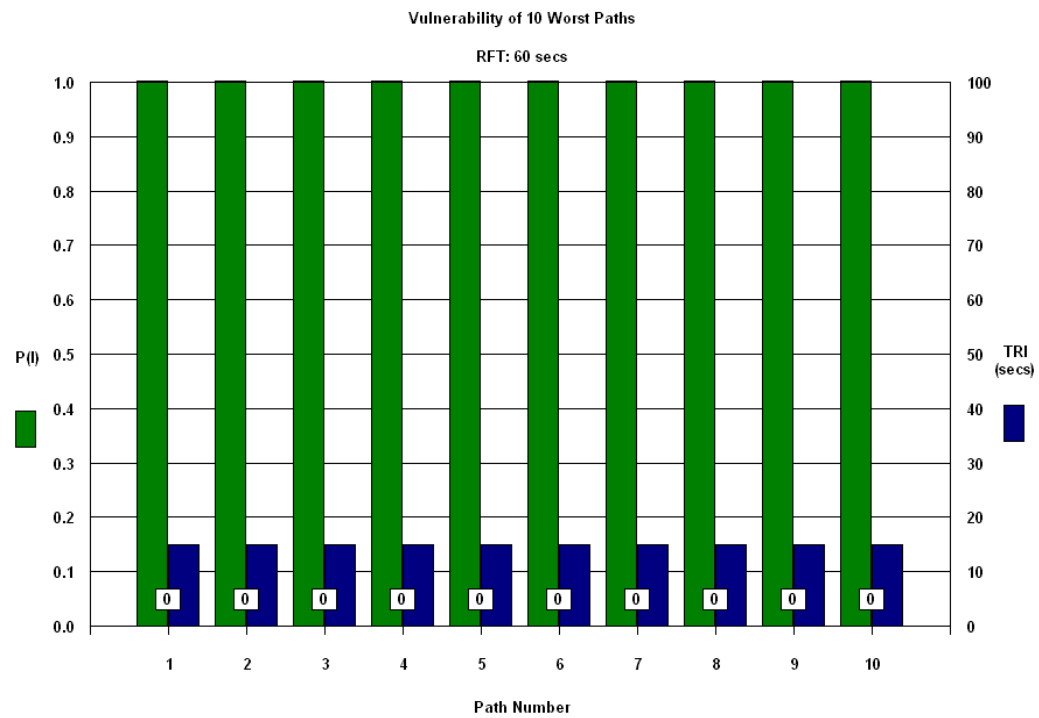
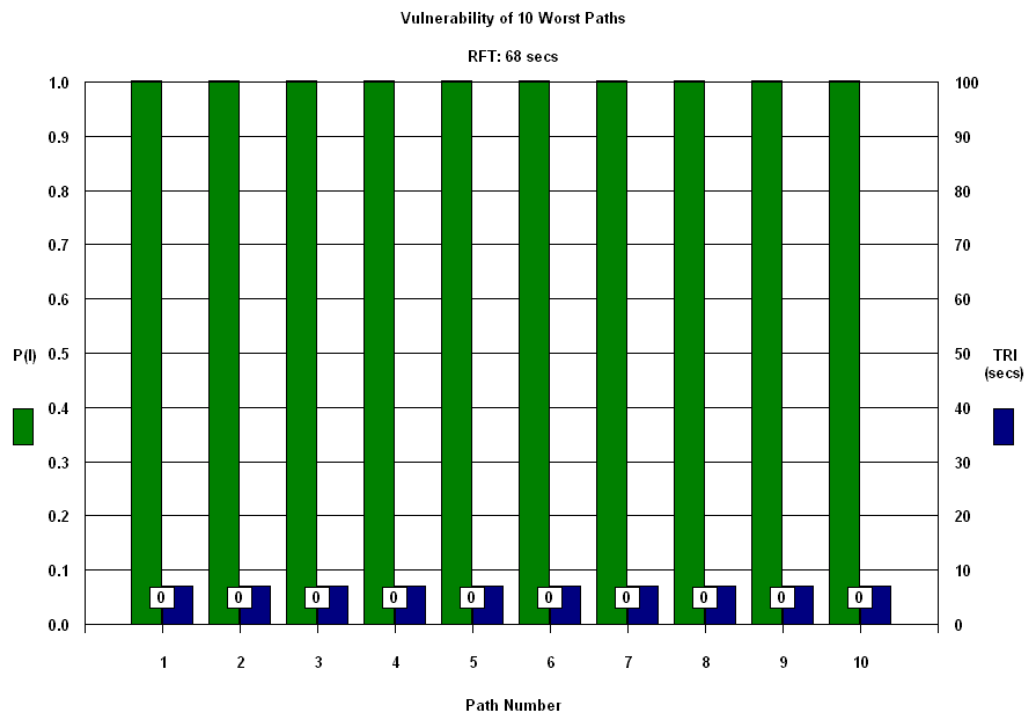
(R10) El adversario entra a la instalación por la puerta de control de acceso vehicular hacia el área protegida y pasa para el área restringida por la puerta de entrada de personal regresando hacia el área protegida a través de la puerta de entrada vehicular alcanzando la puerta vehicular por donde efectuó la entrada..

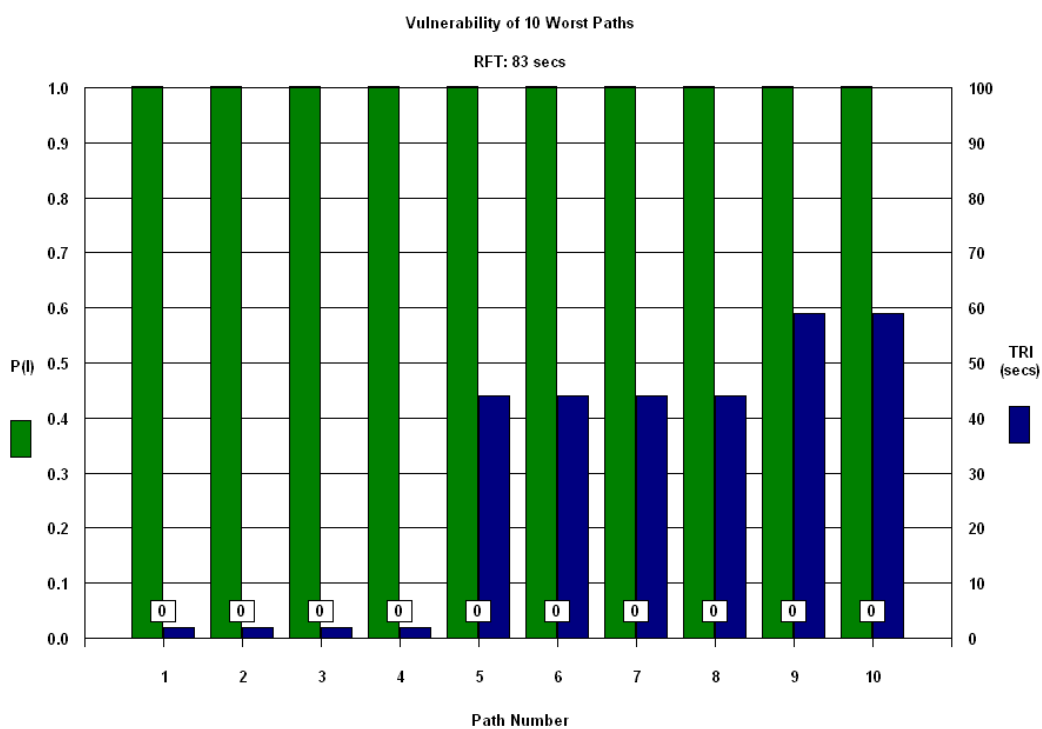
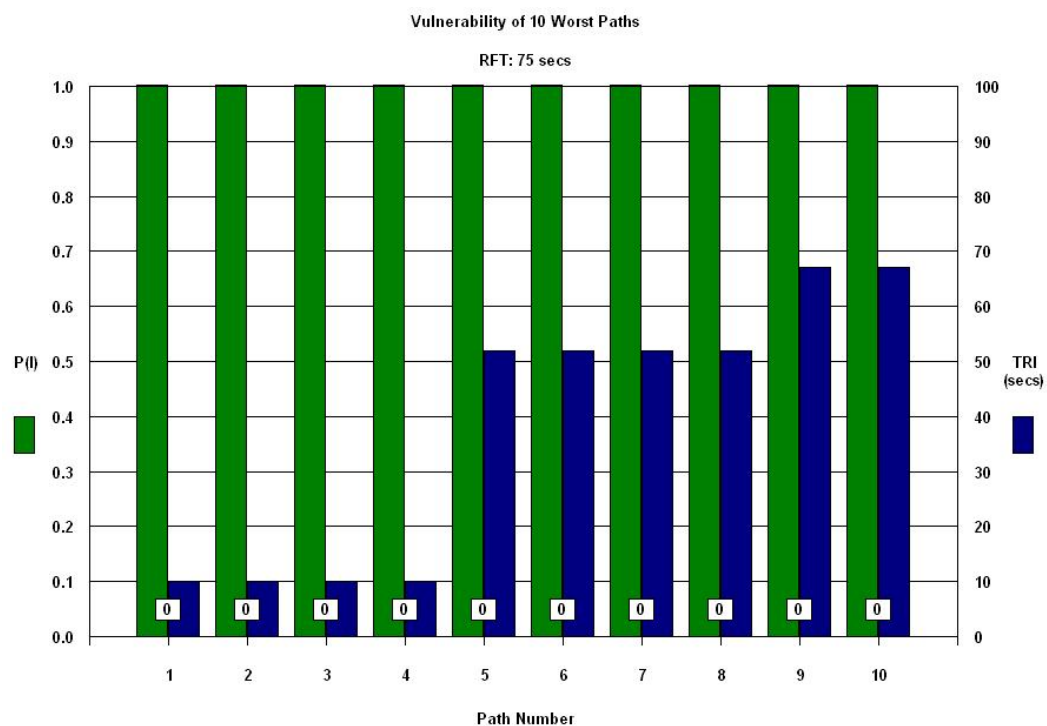
El análisis de sensibilidad demostró que para todas las rutas del adversario y para todos los tiempos de respuesta, la probabilidad de interrupción del adversario fue del 100% lo cual evidencia un desempeño óptimo del sistema de seguridad como se puede ver en la siguiente figura:



En el gráfico de vulnerabilidad del SAVI podemos apreciar como las mejoras hacen que la probabilidad de interrupción del adversario se eleva a 1.0 a través de los 10 caminos con el tiempo de las fuerzas de respuesta más crítico. También podemos apreciar como el tiempo restante a la interrupción no llega a superar los 60 segundos y en consecuencia, posterior a la detección sería un 100% probable la interrupción del adversario.

La situación de la vulnerabilidad del sistema de protección física para el resto de los tiempos de desempeño de las fuerzas de respuesta, resultó ser la siguiente:



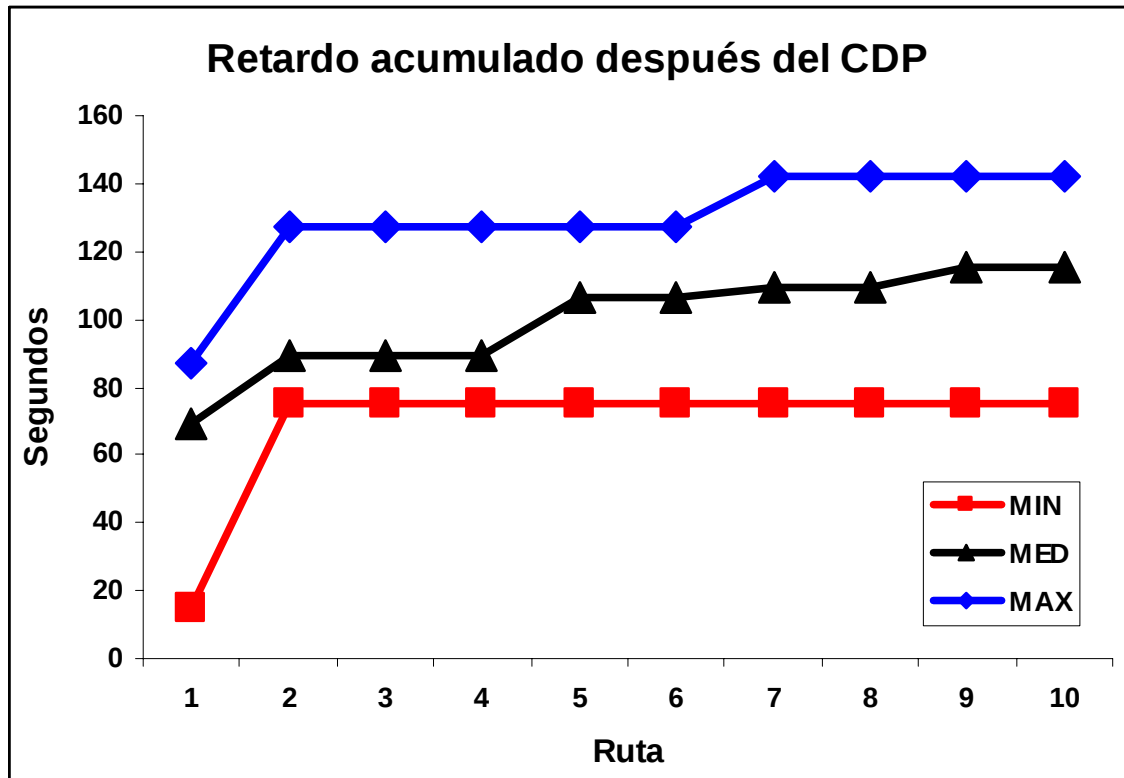


No obstante a la alta probabilidad de interrupción que muestra el sistema, existen otros aspectos a valorar como son el tiempo de retardo acumulado después de la interrupción y el potencial de

detección; pues nos pueden conducir a descubrir reservas o ausencia en cuanto al desempeño de los elementos de protección instalados.

En la valoración de las cuatro primeras rutas, dadas por el SAVI según una ponderación decreciente de vulnerabilidad tenemos los siguientes aspectos a considerar:

1. Ruta (R1): Esta ruta manifiesta un tiempo de retardo acumulado después de la interrupción cuyo mínimo es de 15 segundos, su máximo es de 87 segundos y un valor promedio de 69 segundos para el rango establecido de RTF, además el CDP se encuentra muy cerca del área de los blancos y el potencial de detección es cero. En consecuencia, no se recomienda realizar nuevos esfuerzos en incrementar la detección en zonas previas; pero de ser necesario se pudieran incluir elementos de retardo en al área de los blancos.
2. Ruta (R2): El análisis de sensibilidad de esta ruta nos muestra que aunque existe un 100% de posibilidad de interrumpir el ataque del adversario, el tiempo de retardo posterior a la interrupción oscilan entre 75 y 127 segundos promediando 89 segundos. Esto ilustra la necesidad de ser posible de adicional algunos elementos de retardo como por ejemplo, la instalación de barreras, puertas en los controles de acceso, etc.
3. Ruta (R3): Esta ruta demuestra que la probabilidad de interrupción es del 100%, el tiempo de retardo acumulado después de la interrupción es de 75 seg.y el máximo de 127 seg. con un valor promedio de 89 seg. para el tiempo establecido por RFT, el puARo de detección crítico se encuentra localizado en el área del muelle teniendo un potencial de detección igual a cero, pudiéndose considerar la posibilidad de la utilización de otros elementos de detección y retardo para lograr una mayor probabilidad de interrupción en dicha ruta.
4. Ruta (4): El análisis de sensibilidad realizado a esta ruta en la cual el tiempo de retardo acumulado después de la interrupción de 75 segundos y un valor máximo de 127 segundos ,con un valor promedio de 69 segundos, el punto de detección crítico esta ubicado en el área restringida y su potencial de detección es igual a cero. SAVI da opciones de mejoras relacionadas también con elementos de retardo en el área.



El gráfico anterior muestra el comportamiento mínimo, máximo y promedio del tiempo acumulado de retardo posterior al CDP, en este podemos ver que los menores valores corresponden a las primeras rutas que resultan ser de todas las más críticas. Recordemos que mientras menor sea este tiempo mayor será en consecuencia el nivel de completamiento que hace el adversario de su ataque.

En sentido general, podemos apreciar que el adversario tiene posibilidades reales de introducirse en la instalación, aunque el sistema mejorado tiene a su vez una probabilidad máxima de garantizar la interrupción del mismo aún cuando este intente salir de la instalación.

Por demás, esta solución final fue nuevamente puesta en consideración de funcionarios y especialistas de la empresa coincidieron en que la solución es realmente óptima y se adapta a las características de la empresa y de la amenaza planteada.

Por otra parte, los especialistas de seguridad portuaria de SEPSA, reconocieron la similitud de los resultados obtenidos a partir de este modelo con los obtenidos por ellos al aplicar su metodología de análisis de seguridad portuaria.

FORMAS DE IMPLEMENTACIÓN DE LA SOLUCIÓN

Es recomendable que la entidad tenga presente los siguientes aspectos para la implementación de los resultados de este trabajo:

1. Los resultados están orientados a la protección física de los blancos específicos que están asociados directamente con las exigencias de la seguridad portuaria.
2. La amenaza puede cambiar y con ella la definición que de ella se hizo; por consiguiente debe estar atenta a los indicadores de cambio en la misma.

La entidad debería tener presente que no se requieren grandes inversiones para implementar las mejoras al sistema y obrar en primer lugar por la ejecución de los trabajos de mejoramiento del cercado perimetral que requiere de la limpieza y reparación.

La instalación debería iniciar los contactos con la agencia de protección a fin de garantizar la posición que se requiere para el control de acceso.

CONCLUSIONES DEL CAPÍTULO

1. Fueron identificadas y evaluadas las variantes de mejora del sistema de protección física de la instalación.
2. Se determinó y evaluó la variante óptima del sistema de protección física que garantiza una alta probabilidad de interrupción del adversario y satisface las restricciones de costo - beneficio establecido por la empresa.

CONCLUSIONES GENERALES

1. El desarrollo de las exigencias de la protección física actuales no va a la par del desarrollo de la teoría en nuestro país, donde existe poca información publicada al respecto y en el escenario internacional toma cada día más fuerza.
2. Las nuevas tecnologías informáticas han creado condiciones para facilitar el trabajo de análisis y diseño de los sistemas de protección física, reduciendo la subjetividad que prima en ellos. En este sentido aparecen la técnica de simulación como una valiosa herramienta.
3. El modelo SAVI resulta una herramienta valiosa para la evaluación y diseño de los sistemas de protección física ante amenazas externas brindando un sólido análisis de la vulnerabilidad del sistema que permite la optimización en la toma de decisiones al respecto.
4. Pese a su orientación hacia el análisis de sistemas de protección física complejos, el modelo SAVI puede ser utilizado, con igual propósito, para el análisis de instalaciones menos complejas dando resultados que caracterizan razonablemente las principales vulnerabilidades de estos sistemas y las posibilidades de mejoras a los mismos.
5. En el caso de estudio, el SAVI demostró significativas vulnerabilidades del sistema de protección con vistas a garantizar la seguridad portuaria ante una amenaza objetiva, reconocida por la administración y autoridades competentes.
6. Las mejoras del sistema de protección, realizadas con ayuda del análisis de vulnerabilidad que brinda el SAVI, permiten incrementar la capacidad defensiva de la empresa y la seguridad de sus operaciones portuarias.
7. Dado que nuestro país no cuenta con un sistema que le brinden la capacidad de poder evaluar los diseños de los sistemas de protección física de forma objetiva, ni que permitan que las organizaciones poder demostrar al Estado las características y requerimientos de su protección física; este trabajo aporta una idea viable para ello.

RECOMENDACIONES

1. Considerar la necesidad de desarrollar cursos de capacitación para nuestros profesionales en la protección física como una función más de la empresa cubana para el mejoramiento de su desempeño.
2. Estudiar otros modelos que existen y se pueden aplicar para el análisis y diseño de los sistemas de protección física. Reiteramos que modelos de simulación similares, han estado siendo empleados en muchos países desde más de una década y con resultados efectivos.
3. Crear proyectos de trabajo para la creación de modelos nacionales que se ajusten más racionalmente a las condiciones de nuestras instalaciones.

BIBLIOGRAFÍA

- Alonso Sánchez, Armando. Curso Interregional sobre Protección Física de Instalaciones y Sustancias Nucleares: Recomendaciones para la Organización de un Sistema de Protección Física/ Armando Alonso Sánchez.__ Madrid: [s.n.], 1994.__ 27p.
- Balonso, SA. Recomendaciones para la Organización de un Sistema de Protección Física/ SA Balonso.__ Nuevo México: [s.n.], 1994.__ 93p.
- Carvajal Calderón, Tcl Rigoberto. Utilización de Modelos de Simulación para El Análisis Costo-Efectividad de un Sistema de Protección de Instalaciones Sensibles/ Tcl Rigoberto Carvajal Calderón.__ Santiago de Chile: [s.n.], 1998.__ 125p.
- Cienfuegos. Servicios Especializados de Protección S.A. Informe final de la primera etapa de trabajo del proyecto SSMAT de la gerencia territorial de SEPSA Cienfuegos – Villa Clara: Identificación, Evaluación y Gestión de Prevención o Administración de Riesgos que afectan la Seguridad y la Salud de los Trabajadores/ SEPSA Cienfuegos.__ Cienfuegos: [s.n.], 2003.__ 59p.
- Cortes Díaz, José María. Técnica de Prevención de Riesgos Laborales/ José María Cortes Díaz.__ Madrid: Tébar Flores, 1996.__ 110p.
- Cuba. Escuela Superior del MIMBAS. Curso Superior para Jefes de Seguridad y Protección/ ESMIMBAS.__ La Habana: [s.n.], 2000.__ 4t.
- Cuba. Instituto de Estudios e investigaciones del trabajo. Gestión de Seguridad y Salud en el trabajo. Compendio metodológico sobre política laboral y salarial. / IEIT.__ La Habana: [s.p.], 2000.__ 5p.
- Cuba. Ministerio del Interior. Decreto Ley 186 / MININT.__ La Habana: Gaceta oficial de la República de Cuba, 1996.__ 23p.
- _____.Formato y contenido del Plan de Seguridad y Protección / MININT.__ La Habana, Cuba: [s.n.], 2003.__ 7p.
- _____. Ley 62/87 / MININT.__ La Habana: Gaceta oficial de la República de Cuba, 1996. __ 18p.
- DeLoach, James. Enterprise - wide Risk Management: Strategies for linking risks and opportunity / James DeLoach.__ Madrid:[s.n.], 1997.__ 27p.

España. Curso Interregional sobre Protección Física de Instalaciones y Sustancias Nucleares.____
Madrid: [s.n.], 1984.____ 98p.

Estados Unidos de América. Departament of Defense U.S. Design Guidelines for Physical
Security of Facilities / DDUS.____ Washintong: [s.n.], 1993.____ 192p.

_____. Report / DDUS.____ Washintong: [s.n.], 1996.____ 41p.

_____.Report / DDUS.____ Washintong: [s.n.], 1993.____ 41p.

_____.Report / DDUS.____ Washintong: [s.n.], 1996.____ 53p.

Estrategias para vincular el riesgo con la oportunidad: Resumen Ejecutivo.____ Santiago de Chile:
[s.n.], 1990.____ 32p.

Díaz de Tuesta, José. Selección del Personal de Protección / José Díaz de Tuesta.____ Madrid:
OIEA, 1994.____38p.

Farreras, Joan. Cuadernos de Seguridad: Componentes y Tecnología/ Joan Farreras.____ Madrid:
[s.n.], 2002.____ 21p.

Filosofía de seguridad física. Tomado de: www.seguriteca.com.mx, 25 de Enero 2007.

García Hernández, Julio. Curso Interregional sobre Protección Física de Instalaciones y Sustancia
Nucleares: Sistema Estatal de Protección Física/ Julio García Hernández.____ Madrid: [s.n.],
1994.____ 25p.

García Herrera, Ramón. Curso Interregional sobre Protección Física de Instalaciones y Sustancia
Nucleares: Sistema Estatal de Protección Física/ Ramón García Herrera.____ Madrid: [s.n.],
1984.____ 12p.

Gerenciando la seguridad. Tomado de: www.securitymanagement.com, 10 de Enero 2007.

Iturbe, Luis. Conferencia Problemas de Recursos Humanos en los Proyectos/ Luis Iturbe.____ La
Habana: [s.n.], 1999.____ [s.p.].

Jalpi Remis, Javier. La Amenaza / Javier Jalpi Remis.____ Madrid: [s.n.], 19984.____ 17p.

Koontz, Heber. Administración/ Heber Koontz.____ México: McGraw-Hill, 1990.____ 417p.

La Seguridad: ¿Función Empresarial. Tomado de: www.seguridadcorporativa.org, 14 de Enero
del 2007.

La seguridad como ciencia. Tomado de: www.seguridadcorporativa.org, 14 de Enero del 2007.

Leira Rodríguez, Gabriel. Móviles de la Amenaza/Gabriel Leira Rodríguez.____ Madrid: [s.n.],
1986.____ 19p.

- _____. Curso Interregional sobre Protección Física de Instalaciones y Sustancia Nucleares: Móviles de la Amenaza/Gabriel Leira Rodríguez.____ Madrid: [s.n.], 1994.____ 45p.
- Madrid-Dávila, Enrique de. La consultaría de Seguridad: Organizaciones y Competidores/Enrique de Madrid-Dávila.____ México: [s.n.], 1992.____ 2p.
- Manual del Director de Seguridad.____ España: PROSEGUR, 1996.____ 235p.
- México. Sandia National Laboratories. The International Training course/ SNL.____ New Mexico: [s.n.], 1994.____ 221p.
- _____. The International Training course/ SNL.____ New Mexico: [s.n.], 1998.____ 237p.
- _____. Informe del Curso Internacional de Protección Física de Instalaciones y Materiales Nucleares/ SNL.____ New Mexico: [s.n.], 1980.____ 42p.
- El paradigma de la seguridad. Tomado de: www.seguridad-la.com, 10 de Febrero del 2007.
- Novedades de la integración de seguridad. Tomado de: www.halvisegur.com, 19 de Diciembre del 2002.
- Rodríguez Márquez, Antonio. Curso Interregional sobre Protección Física de Instalaciones y Sustancia Nucleares: Sistema Estatal de Protección Física/ Antonio Rodríguez Márquez.____ Madrid: [s.n.], 1984.____ 23p.
- Sánchez Gómez, Manuel. Conferencia sobre Delitos Corporativos/ Manuel Sánchez Gómez.____ La Habana: GET, 2001.____ [s.p.].
- Viena.Organización Nacional de Energía Atómica. Curso Regional de Capacitación para la Protección Física de Centrales Nucleares/ OIEA.-- Argentina: [s.n.], 1998.____ 262p.
- Walpole, Regist. Probabilidad y Estadística/ Regist Walpole.____ México: McGraw-Hill, 1992.____ 210p.
- _____. Probabilidad y Estadística/ Regist Walpole.-- México: McGraw-Hill, 1990. -- 147p.

ANEXOS

ANEXO - 1. FUNDAMENTALES CONSIDERACIONES PARA LA CONFECCIÓN DE UN PLAN DE SEGURIDAD.

En forma general, a la hora de afrontar la confección de un Plan de Seguridad, es conveniente tomar en cuenta las siguientes consideraciones:

1. No hay un sistema de seguridad universal. No se puede aplicar exactamente el mismo patrón a dos centros o instalaciones con distinto emplazamiento geográfico, aún cuando sus características sean idénticas. Solo se puede hablar de directrices o características universales.
2. Cada instalación presenta una problemática diferente, de forma que aún cuando se contemplen dos instalaciones distintas y con una finalidad común, al analizar en detalle sus peculiaridades se llega a la conclusión de que lo que es bueno para una puede no serlo para la otra. Normalmente la justificación se halla en el factor humano, ya que las personas de uno y otro lugar son distintas.
3. La presencia humana en los sistemas de seguridad resulta imprescindible. Una adecuada protección debe combinar medios físicos, técnicos, humanos, de infraestructura y auxiliares, apareciendo siempre el elemento humano como fundamental, tanto directamente como complementando a los otros medios.
4. El estudio de seguridad no debe dejar nada sujeto a improvisaciones. Esto únicamente es posible cuando se hayan tenido en cuenta todos los riesgos por muy insignificantes o descabellados que parezcan, y dentro de cada riesgo, cuando se llegue a los más mínimos detalles. Esto viene a constituir lo que se denomina la “regla de oro” en los estudios de seguridad: la subdivisión o escalonamiento hasta las últimas consecuencias.
5. El estudio de seguridad que se adopte debe responder a las características de adaptación a los distintos riesgos existentes de modo proporcional a su importancia. Además debe tener homogeneidad, a cuyo efecto se entiende que los distintos medios empleados deben integrarse en un todo armónico y flexibilidad para absorber nuevos riesgos, sin modificaciones esenciales del sistema.
6. Todo plan de un sistema de seguridad es afectado fundamentalmente por el análisis previo de las posibles acciones contra la instalación, por las repercusiones que ellas mismas ocasionarían y por el binomio eficacia-costos considerado en conjunto y no aisladamente, ya que si lo

ideal es la obtención de una gran eficacia debe, también procurarse que el costo de la implantación del sistema no sea desproporcionado a las hipotéticas repercusiones que podrían ocasionarse con los actos lesivos. Se habla de costo y no gasto, ya que el costo, es una inversión y el gasto una pérdida.

ANEXO - 2. RESULTADOS GENERALES DEL DIAGNÓSTICO A LOS SPF DEL PAÍS EN 1998

1. Dificultades en los procesos de selección, procesamiento, estimulación y capacitación de las fuerzas de seguridad.
2. Serias violaciones con el uso y custodia de las armas de fuego puestas a disposición de las fuerzas de seguridad
3. Inadecuado uso de los medios técnicos y las barreras físicas con un excesivo uso de personal de seguridad.
4. Baja motivación laboral entre las fuerzas de seguridad y un deterioro de su imagen como cuerpo de seguridad.
5. Falta de compatibilidad de la política general de seguridad de la organización con la seguridad.
6. La legislación de seguridad tenía limitaciones en cuanto a la definición de las funciones de la dirección de las organizaciones en los diferentes niveles, del MININT y de los Jefes de Seguridad y Protección.
7. Las organizaciones delegaron las funciones de la seguridad corporativa a funcionarios sin la debida preparación e incluso a algunos cuyas funciones no tenían nada de compatibles con la seguridad.
8. Las organizaciones no potenciaron la creación y complemento cualitativo de los cargos vinculados con la dirección de la seguridad corporativa en los organismos, órganos y entidades.
9. La seguridad poseía una doble subordinación del personal profesional de seguridad, por un lado se subordinaban al MININT y por otro a la administración de las organizaciones.

ANEXO - 3. ORGANIGRAMA DE LA INSTALACIÓN

