UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

PROGRAMA DE MAESTRÍA Y DOCTORADO EN INGENIERÍA

FACULTAD DE INGENIERÍA

REDISEÑO DE LA ESTRUCTURA DE UN SISTEMA DE SEGURIDAD FÍSICA BAJO UN ESQUEMA DE PLANEACIÓN NORMATIVA-ADAPTATIVA

T E S I S

QUE PARA OBTENER EL GRADO DE:

MAESTRO EN INGENIERÍA

SISTEMAS – PLANEACIÓN

P R ES E N T A:

RICARDO GINES TRINIDAD

DIRECTOR DE TESIS

DR. BENITO SÁNCHEZ LARA

Índice

INTRODUCCIÓN

El término seguridad cotidianamente se refiere, según la Real Academia Española a "la ausencia de riesgo o confianza en alguien o algo". Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia. En términos de seguridad física, ésta es vista como un conjunto de principios aplicados a un sistema de protección (Sistema de Seguridad Física, SSF) que obran de forma lógica y razonable para generar una situación o estado de tranquilidad (Cordero, 2010). El objetivo de este sistema es resguardar físicamente la seguridad patrimonial o activos estratégicos de las personas, comunidades y organizaciones, con la finalidad de reducir las pérdidas asociadas a los riesgos, fortalecer la capacidad de supervivencia y mantener la continuidad operativa.

La seguridad aumenta su relevancia en la medida que las relaciones entre los involucrados en un evento que compromete la seguridad de un determinado objeto aumentan, debido a que las perdidas asociadas a los riesgos identificados se intensifican. En la era posterior al llamado 911 (septiembre 11, ataque a las torres gemelas en Nueva York), gobiernos y corporaciones alrededor del mundo han tenido que aprender a pensar creativamente en materia de seguridad y a reconsiderar las amenazas y vulnerabilidades actuales de sus infraestructuras crítica, como aeropuertos, puertos marítimos, refinerías, plantas generadoras de energía, oficinas claves de gobierno y lugares de similar importancia, no sólo

por la relevancia de estas infraestructuras, sino por el grado de interrelaciones que forman estas Infraestructuras con otros sistemas de diversa naturaleza: sociales, ambientales, económicos, políticos e industriales, y que las ha llevado a evolucionar en lo que se conoce como Infraestructuras Críticas Grandes y Complejas (Large Critical Complex Infrastructure, LCCI's).

La mayor parte de los sistemas de seguridad física actuales favorecen a medidas tecnológicas para hacer frente a las amenazas, y no contemplan medidas contextuales que integren factores sociales, organizacionales, institucionales, que permitan fortalecer la capacidad para responder o absorber el impacto no sólo de la organización sino de los involucrados en el sistema.

El presente trabajo busca proponer una estructura de funciones de un sistema de seguridad física para una LCCI cuyos elementos no sólo estén inmersos en un marco normativo, sino que sean congruentes con su contexto, para que el sistema tenga una mejor posibilidad de adaptarse y sobrevivir al entorno de la organización, y dar así la mejor respuesta posible ante un evento.

El primer Capítulo de esta tesis proporciona los antecedentes y definiciones clave para el entendimiento de la naturaleza de un SSF, y los aspectos que se consideran relevantes en la conformación de este sistema. Posteriormente se define el concepto de LCCI, modelo que es tomado como caso de aplicación del sistema propuesto, y se particulariza con el caso de PEMEX Petroquímica (PQ), bojo la consideración de que la industria petrolera y sus derivados forman parte de la llamada infraestructura crítica. El Capítulo expone la problemática entorno a la seguridad física que presenta la principal zona petroquímica de PEMEX (y de México), la zona sur del estado Veracruz, con la descripción los elementos que se encuentran involucrados en este sistema: vulnerabilidades, amenazas y riesgos, para culminar con el problema de seguridad física que enfrenta no sólo PQ, sino las LCCI's en general. Se expone también dentro de este Capítulo el objetivo general que persigue éste trabajo de tesis, su justificación, alcance y la metodología planteada para su desarrollo.

El Capítulo dos establece el marco teórico bajo el cual se realizó este trabajo, en el cual se hace mención a la Planeación Adaptativa, cuyos orígenes se encuentran principalmente en los trabajos de Emery y Trist (1965), Ackoff (1981) y Ozbekhan (1977). Se hace una revisión sobre el concepto de Planeación Normativa propuesto por Ozbekhan, quien plantea cuatro fases de la planeación, como una Planeación Interactiva Normativa. Por su parte Ackoff plantea una metodología de la Planeación Interactiva que consta de dos partes:

idealización y realización, las cuales a su vez se dividen en seis fases interrelacionadas, con las que busca que un rediseño del sistema de manera holística a fin de lograr un estado futuro deseable en el que los problemas no aparezcan en el primer lugar y que esté orientado a la predicción y preparación. Finalmente se hace referencia al concepto de construcción del sistema por medio de un proceso de descomposición propuesto por Gelman y Negroe (1982).

En el Capítulo tres a partir de lo establecido en el marco teórico se desarrolla la propuesta de estructura de SSF. En este Capítulo se establecen los ambientes interno y externo de la organización, así como el entorno transaccional, se hace un análisis de las obstrucciones que no permiten llegar al estado deseado, y se establecen escenarios de referencia que ayudan a comprender la importancia de la necesidad del rediseño de los actuales sistemas de seguridad. A partir de esta información generada y con el marco normativo establecido por el Plan Rector de PEMEX, se establecieron las propiedades deseadas del SSF, para posteriormente, por un proceso de construcción por descomposición establecer la estructura del SSF propuesto. Finalmente, se detallan las partes que conforman este sistema.

Capítulo 1. La Planeación de la Seguridad Física

1 .1 Definiciones

Antes de comenzar, es necesario dar algunas definiciones que permitan poner las bases necesarias del rumbo que siguió este trabajo. Resulta importante señalar que en el español no existe una palabra que permita hacer una distinción entre la seguridad industrial y la seguridad física, siendo que ambos a pesar de ser conceptos que suelen cruzarse en algunas de sus funciones, tienen una razón de ser y un objetivo diferentes.

En el idioma inglés, por el contrario, estos conceptos son manejados por dos palabras: *safety* y *security*. El termino *safety* se refiere a los medios y procedimientos que ayuden a garantizar la seguridad de los trabajadores de una organización ante aquellos riesgos implícitos a sus labores y ambiente de trabajo, a través de identificar, evaluar y controlar aquellos factores de riesgo ambientales presentes en el medio de trabajo causantes de los accidentes de trabajo (seguridad industrial). Por su parte, el concepto Security aborda aspectos que conciernen de lo que entendemos por seguridad física o lo que comúnmente se llama protección, el cual hace referencia a todos aquellos mecanismos (generalmente de disuasión, prevención, detección y reacción)

destinados a proteger físicamente cualquier recurso de un sistema u objeto determinado.

Existen diferentes acepciones en torno al significado de la palabra y el concepto seguridad. Etimológicamente, el Diccionario de la Real Academia Española (2001) señala: seguridad proviene del latín *securĭtas (*que a su vez se deriva del adjetivo *secūrus* que significa seguro*)*: definido como la cualidad de seguro. Mientras que la palabra seguro, se define como algo que está libre y exento de todo peligro, daño o riesgo (Alarcón, 1998). Así, la seguridad es el sentirse o sentir algo como libre y exento de riesgo, es una sensación que se puede percibir y cotidianamente se refiere a la a la ausencia de riesgo o también a la confianza en algo o alguien. Sin embargo, el término puede tomar diversos sentidos según el área o campo a la que haga referencia. Existen más acepciones en cuanto a las palabras seguridad y seguro, sin embargo, estas son las definiciones que más compiten en lo referente al tema que aquí tratado.

A nivel conceptual, Cordero (2010), especialista en seguridad física, señala que la seguridad es vista como el conjunto de principios aplicados a un adecuado sistema de protección (Sistema de Seguridad Física), unidos a una actitud de obrar en forma lógica y razonable para generar una situación o estado de tranquilidad real; a su vez es un conjunto de normas adoptadas para prevenir un peligro, riesgo o amenaza.

A partir de la definición anterior sobresalen algunos aspectos relevantes. En primer lugar, se habla de "generar una situación o estado de tranquilidad real", la cual podríamos definir, como generar un estado deseado, el cual debe de proceder, naturalmente de la identificación de una situación o estado actual. De igual manera durante la identificación de este estado actual se puede proyectar un estado futuro al cual se dirige el la organización o sujeto/objeto de no ser intervenido. Este "escenario" es parte de un análisis de riesgos. Ahora bien, el segundo punto a resaltar es la llamada "actitud de obrar en forma lógica y razonable". Esta actitud, es parte del proceso por el cual se deberán seleccionar tanto "el conjunto de principios aplicados" así como las "normas adoptadas para prevenir un peligro, riesgo o amenaza", es decir, es un proceso lógico y razonable (o racional) para la mejor adopción de medios para alcanzar la garantía de seguridad (o los fines), (Banfield, 1959). La mejor forma de canalizar esta actitud para lograr el objetivo de la seguridad física será a través de proceso de planeación.

Señala Cordero (2001), que la seguridad física son aquellos aspectos relacionados con la protección de personas, bienes e instalaciones, de los riesgos que pueden atentar contra su integridad y las técnicas que se utilizan para prevenir y controlar dichos riesgos. La seguridad física, como sistema, hace referencia a todos aquellos elementos (generalmente de disuasión, prevención, detección y reacción) que tienen por objetivo común el resguardar físicamente la seguridad patrimonial o de activos estratégicos de las personas, comunidades y organizaciones. Estos elementos van desde actividades humanas, uso de tecnologías, normas, procedimientos y mecanismos de control, los cuales tienen la finalidad de proteger y responder ante amenazas físicas (producidas tanto por el hombre como por la naturaleza: desastres naturales, incendios, inundaciones, amenazas ocasionadas involuntariamente por personas, acciones hostiles deliberadas, robo, sabotaje, etc.) que atenten contra la organización, para permitir de esta forma reducir la pérdidas potenciales asociadas a los riesgos existentes, aumentar su capacidad de supervivencia y mantener la continuidad operacional. Los elementos en sí son: físico-tecnológicos (dispositivos para control de acceso, circuitos cerrados de televisión, barreras y alarmas perimetrales y centros de mando); humanos (operadores, administradores, vigilantes); y de gestión (normas, procedimientos, convenios, etc.), los cuales trabajan directamente sobre las vulnerabilidades de la organización a proteger. Como sistema, el SSF está inmerso en un suprasistema de diferente naturaleza, el cual es quien es el blanco de las amenazas y donde se localizan algunas de las principales vulnerabilidades.

El mismo autor ante mencionado, indica que los requisitos sobre seguridad física varían considerablemente según las organizaciones y dependen de la escala y de la organización de los sistemas de información. Sin embargo son aplicables a nivel general los conceptos de asegurar áreas, controlar perímetros, controlar las entradas físicas e implantar equipamientos de seguridad. Se puede entonces generalizar los aspectos que debe cubrir la seguridad, pero no se puede generalizar la aplicación de estos. Adicionalmente, González (2008) señala que se debe tener presente que los diferentes roles y actividades que se llevan a cabo en las diversas instalaciones, sean públicas o privadas, así como los ambientes que las rodean, nos conducen a pensar que ninguna norma de seguridad física puede ser extendida y aplicada universalmente a todas las instalaciones. Cada nuevo proyecto destinado a la selección de los elementos y cursos de acción para lograr la salvaguarda del sujeto/objeto, deberá ser producto de un estudio particular de dicho sujeto/objeto.

La seguridad física tiene por objetivo fundamental mantener un ambiente de salvaguarda para el personal que allí labora; así como también los activos, la continuidad operacional y la propiedad intelectual (González, 2008). En este sentido, los elementos que conforman este Sistema tendrán como fin común alcanzar este objetivo. Para ello es necesario coordinar los elementos del sistema: pautando las líneas y acciones estratégicas, los elementos materiales, actividades substanciales de apoyo, procedimientos operativos, y elementos de evaluación y control. Esto puede ser logrado a través de establecer un Programa Integral de Seguridad Física el cual deberá permitir coordinar las actividades de los elementos del encargados de proporcionar seguridad a través de especificar las acciones operativas en forma de procedimientos, establecer mecanismos de coordinación, y dotar de la información estratégica necesaria para dar apoyo a las actividades en torno a la seguridad física.

Ahora bien, la conformación de un sistema de seguridad física (SSF) debe integrar aquellos aspectos que permitan garantizar un ambiente de seguridad: los recursos humanos y físico-tecnológicos disponibles, las políticas y normas que dan sustento legal y legitimizan los procedimientos que definan y establezcan las actividades a realizar, y la información estratégica para la operación. De igual manera se deben integrar elementos que si bien no forman parte directa de las tareas y funciones para garantizar la seguridad, sí afectan a esta debido a la interacción con el objeto a resguardo, y que producen propiedades emergentes desencadenadas de dicha interacción, esto es información del medio ambiente social de la región, desastres naturales, índices delictivos, antecedentes de actividades de sabotaje o terrorismo. El entendimiento del cómo se relacionan estos elementos, y la afectación que tienen en la Organización en su totalidad, permiten explotar de mejor forma los recursos e información disponibles. Aunado a un proceso de planeación que permita enfrentar proactivamente las amenazas, termina por redondear el producto.

1.2 Aspectos relevantes en la planeación de la seguridad

A fin de asegurar que el proceso de seguridad física del objeto a resguardar cumpla con lograr el llamado “estado de tranquilidad real” (el estado de seguridad deseado, el cual garantice las mínimas pérdidas para la organización), es necesario llevar a cabo la planeación de las medidas de seguridad y de las respuestas adecuadas con base en la evaluación de los riesgos de los procesos y tareas internas de dicho objeto, así como del entorno o ambiente del objeto. Existen sin embargo, una serie de elementos a considerar

dentro de esta planeación, que permiten conformar una estructura con un enfoque que permita integrar a los elementos y actores involucrados y afectados en la labor de seguridad, y definir las responsabilidades dentro del sistema, para así compartir recursos y tener una óptima administración de estos.

La planeación y operación de un SSF, según señala Lynn (2001), consta de tres fases o procesos. En el primer principio o fase se trata de determinar los objetivos. Esto a través de entender la instalación, definir riesgos y posibles amenazas, identificar los posibles blancos ("targets") o activos estratégicos y mediante regulaciones y la administración de riesgos. En la segunda etapa, se diseña el dispositivo (SSF), como la materialización y aplicación de las medidas de protección necesarias para reducir y controlar la vulnerabilidad del sujeto/objeto a proteger. Esto a través de medidas físicas y administrativas. Finalmente, la tercera etapa, análisis y evaluación, se evalúa la efectividad del sistema a partir de una serie de herramientas como el análisis de riesgos y el análisis de neutralización. A partir de una analogía con la Planeación Interactiva propuesta por Ackoff (2001), la primera etapa debe corresponder con la formulación de la problemática (mess), con ello se garantiza el entendimiento de la organización. Por su parte la etapa dos, conjunta las etapas de planeación de fines, medios y recursos, así como el diseño de la implantación. Finalmente en la etapa tres, tiene una equivalencia a la etapa de diseño de controles propuesta por Ackoff (2001). Adicionalmente a lo explicado en estas etapas, es necesario contemplar que para el diseño del sistema se deben satisfacer ciertas cualidades, las cuales garanticen un enfoque integral del sistema y permitan un mejor aprovechamiento de los recursos (humanos y materiales) y delimitación de las responsabilidades.

Coordinación con otros organismos

Tanto en situaciones de seguridad industrial, como en situaciones de seguridad física, proporcionar seguridad debe implicar la cooperación intensiva con otros órganos estatales (fuerzas policiales y militares), que tienen sus propias prioridades y métodos de operaciones que pueden no coincidir exactamente con los desarrollados para el sujeto/objeto a resguardar. Aunque por la naturaleza de los eventos implicados en la seguridad física, los cuales implican una componente de orden legal, de la violación de o atentado contra la ley, hacen este requisito no sólo esencial, sino vital. Se debe garantizar que al planear las medidas de seguridad para el sujeto/objeto se incluyan las siguientes acciones (Lynn, 2001):

- Asegurar que se cuente con recursos de seguridad suficientes en áreas específicas y durante las horas requeridas;
- Fomentar una coordinación muy cercana entre la administración de las fuerzas de seguridad externas (fuerzas de seguridad federales, estatales y/ o municipales) y los administradores internos de la seguridad del sujeto/objeto, para desarrollar planes y respuestas de seguridad para el sitio que contemplen acciones conjuntas;
- Identificar claramente las cadenas de mando y de responsabilidad para planear la seguridad y las acciones entre las fuerzas de seguridad internas (que pueden ser o no privadas) y las fuerzas de externas seguridad.

Estos factores en el proceso de seguridad serán más críticos conforme mayores sean los riesgos de seguridad y el grado de amenaza que se presente, tal es el caso de las LCCI. Sin importar cuál sea la situación de seguridad, se requiere cierto grado de planeación y cooperación entre los organismos de administración de seguridad internos (del sujeto/objeto) y las fuerzas de seguridad externas.

Responsabilidades

Debe quedar claro para todos los involucrados en la planeación de la seguridad, la asignación de responsabilidades de los diferentes actores participantes, con la finalidad de delimitar las funciones de cada uno (Lynn, 2001). En general se puede describir los siguientes tipos de responsabilidades:

- Responsabilidad de las áreas encargadas de la administración de la seguridad en la organización (sujeto/objeto) en las decisiones sobre la planeación de la seguridad que puedan afectar los procesos de esta (aceptando los consejos adecuados sobre cuestiones tales como las implicaciones de seguridad de la región donde se localiza la organización);
- Responsabilidad de las fuerzas de seguridad para determinar cuál es el uso adecuado de la fuerza o la autoridad para asegurar la seguridad en respuesta a las situaciones que puedan surgir durante algún evento.

Estructura de planeación conjunta

Las estructuras instrumentadas para desarrollar planes y programas de seguridad también variarán de acuerdo con el nivel de los riesgos en la organización, y por lo tanto al grado de amenaza y a la vulnerabilidad. En

cualquier caso, el intercambio continuo de información entre los administradores de la seguridad de la organización y las fuerzas de seguridad externas es benéfico. Incluso sin estructuras formales de asesoría, es muy útil para los encargados de la administración de la seguridad física de la organización, como para los de las fuerzas de seguridad externas mantener contacto, compartir información en materia de seguridad, y reunirse constantemente para asegurar que el conocimiento corporativo de las actividades de cada uno esté actualizado dentro de estas organizaciones, a esta función se le llama Inteligencia. Esta vinculación está determinada directamente en virtud al nivel de riesgo que represente la organización. Para niveles de bajo riesgo (con un potencial de pérdidas menor para la sociedad) dicha vinculación puede carecer de una estructura formal. Sin embargo, en niveles de mayor riesgo (aquellos en los cuales los eventos pueden impactar no sólo al personal e instalaciones de la organización, sino también a la población aledaña, la sociedad en general, o incluso a la imagen pública del gobierno), y específicamente aquellos cuya operación puede ser considerada estratégica para la económica y laboral del país, se necesita tener una estructura formal la cual proponga una constante reunión para discutir cuestiones de seguridad (Lynn, 2001).

Planeación de recursos

Al planear los requisitos de seguridad, todos los participantes deben darse cuenta de que las fuerzas de seguridad generalmente no están familiarizadas con los procesos y tareas llevadas a cabo por la organización, y por el contrario, que los administradores dentro de la organización generalmente no son expertos en las respuestas adecuadas de seguridad. Es de utilidad que la seguridad se aborde como otras cuestiones técnicas, con necesidades y especificaciones delimitadas por la organización, planes y programas preliminares elaborados por las fuerzas de seguridad para cumplir con dichas necesidades y especificaciones, que se sometan a aprobación en una reunión conjunta, y de ser posible recurrir al personal de las fuerzas de seguridad que haya adquirido una comprensión de las necesidades de la organización mediante experiencia previa.

Respuestas de emergencia

Parte del proceso de planeación consiste en desarrollar lineamientos claros para las respuestas ante las emergencias; ya sean por causas naturales como por ejemplo, un incendio (los cuales generalmente son responsabilidad directa de seguridad industrial), o definitivamente causadas premeditadamente por el

hombre (aquellos que competen más a la seguridad física), tales como: amenazas de bomba o ataque de personal armado. Para dicha planeación, es necesario coordinar algunas de estas acciones con el personal de seguridad industrial y/o con personal de protección civil.

Cadenas de mando y rendición de cuentas

Es importante determinar quién es responsable y quién debe rendir cuentas no sólo de la planeación integral de la seguridad, sino también para delimitar las responsabilidades. Una cadena de mando permite establecer la estructura organizativa del área responsable de la seguridad física, a través de esquematizar la jerarquización y división de las funciones y componentes de esta, y establecer líneas de autoridad (de arriba hacia abajo) a través de los diversos niveles y de delimitar las responsabilidades de cada elemento.

Comunicaciones

Para la instrumentación eficaz de los planes de seguridad, es necesario elaborar una estrategia clara de comunicaciones, tanto en términos de las redes físicas empleadas, así como de las políticas del uso de las comunicaciones. La comunicación dentro de un sistema de seguridad es una piedra angular, puesto que para poder responder efectivamente ante un evento se requiere de canales de comunicación que hagan ágil y eficiente la comunicación.

Hasta este punto se ha descrito tanto lo que es la seguridad física, como su proceso de planeación, mediante el cual partiremos para proponer el rediseño del SSF. Lo consecuente será definir el SSF y en qué consiste dicho rediseño, a partir de definir algunos conceptos que permitan establecer a algunos de los actores, elementos y factores clave del objeto de estudio.

1.3 Ámbitos de la seguridad

El ámbito de responsabilidad de procuración de la seguridad física sobre el objeto u organización a resguardar dependerá de la naturaleza de esta, es decir del rol que tenga. Ilustrísima En este rubro, se pueden señalar tres ámbitos o esferas de seguridad física: nacional, pública y privada (Velazco, 2004). Cabe señalar que el ámbito de seguridad define a los responsables de procuración de seguridad.

A nivel nacional, la seguridad recae en el Estado, el cual debe de garantizar la sobrevivencia e integridad de la nación en la comunidad internacional, como un estado libre y soberano (Velazco, 2004). Las instituciones encargadas de la

procuración de esta seguridad son las fuerzas armadas y los servicios de inteligencia. En el ámbito de la seguridad pública, el Estado debe garantizar la inexistencia de amenazas que socaven los bienes y derechos de la ciudadanía. De igual manera debe de promover la convivencia pacífica y el desarrollo individual y colectivo de la sociedad. Sus instituciones son las policías, procuradurías, prisiones preventivas, etc. En el ámbito de la seguridad privada, este es la encargada de garantizar la seguridad de las personas físicas a través de la prestación de un servicio en particular, por medio de escoltas, guardias, consultores privados, etc. Ya se ha mencionado que para un mejor aprovechamiento de los recursos y dar una mejor atención a los eventos, deberá existir un determinado grado de comunicación y coordinación entre estos elementos.

1.4 Riesgo, Vulnerabilidad y Amenaza

Como se explicó anteriormente, el establecimiento de los elementos que deberán integrar el llamado sistema seguridad de nuestro sujeto/objeto a resguardo está en función tres elementos: riesgo, amenaza y vulnerabilidad. De acuerdo con Cardona (2001), a lo largo de la historia estos tres conceptos han tenido diversas acepciones. En general, hoy se acepta que el concepto de amenaza se refiere a un peligro latente o factor de riesgo externo de un sistema o de un sujeto expuesto, que se puede expresar en forma matemática como la probabilidad de exceder un nivel de ocurrencia de un suceso con una cierta intensidad, en un sitio específico y durante un tiempo de exposición determinado. Por otra parte, la vulnerabilidad se entiende, en general, como un factor de riesgo interno que matemáticamente está expresado como la factibilidad de que el sujeto o sistema expuesto sea afectado por el fenómeno que caracteriza la amenaza. De esta manera, el riesgo corresponde al potencial de pérdidas que pueden ocurrirle al objeto u organización expuesta, resultado de la "convolución" de la amenaza y la vulnerabilidad. Así, el riesgo puede expresarse en forma matemática como la probabilidad de exceder un nivel de consecuencias económicas, sociales o ambientales en un cierto sitio y durante un cierto período de tiempo.

Es importante mencionar que la convolución es un concepto que se refiere a la correlación y mutuo condicionamiento, en este caso, de la amenaza y la vulnerabilidad. Dicho de otra forma, no se puede ser vulnerable si no se está amenazado y no existe una condición de amenaza para un elemento, sujeto o sistema si no está expuesto y es vulnerable a la acción potencial que representa dicha amenaza. En otras palabras, no existe amenaza o vulnerabilidad

independientemente, pues son situaciones mutuamente condicionantes que se definen en forma conceptual de manera independiente para efectos metodológicos y para una mejor comprensión del riesgo (Cardona, 2001).

Así, al intervenir uno o los dos componentes del riesgo se está interviniendo el riesgo mismo. Sin embargo, dado que en muchos casos no es posible intervenir la amenaza, para reducir el riesgo no queda otra alternativa que modificar las condiciones de vulnerabilidad de los elementos expuestos. Esta es la razón por la cual con mucha frecuencia en la literatura técnica se hace énfasis en el estudio de la vulnerabilidad y en la necesidad de reducirla mediante medidas de prevención-mitigación, sin embargo lo que realmente se intenta de esta manera es la reducción del riesgo.

De acuerdo con lo anterior, la vulnerabilidad se puede definir como un factor de riesgo interno de un sujeto o sistema expuesto a una amenaza, correspondiente a su predisposición intrínseca a ser afectado o de ser susceptible a sufrir un daño. La vulnerabilidad, en otras palabras, es la predisposición o susceptibilidad física, económica, política o social que tiene el sujeto/objeto de ser afectado o de sufrir daños en caso que un fenómeno desestabilizador de origen natural o antropogénico se manifieste. La diferencia de vulnerabilidad del contexto social y material expuesto ante un fenómeno peligroso determina el carácter selectivo de la severidad de los efectos de dicho fenómeno (Cardona, 2001).

Análisis de los riesgos

Como se mencionó, el análisis de riesgos es una función de la amenaza y la vulnerabilidad, y puede ser llevado con distintos grados de refinamiento, en función de la información de riesgos y datos disponibles. De conformidad con el estándar AS/NZS 4360:1999, para la Administración de Riesgos, de acuerdo con las circunstancias, el análisis puede ser cualitativo, semi-cuantitativo o cuantitativo o una combinación de estos. El orden de complejidad y costos de estos análisis en orden ascendente, es cualitativo, semi-cuantitativo y cuantitativo. Se debe de utilizar una combinación de análisis. El detalle de los tipos de análisis es el siguiente:

a) Análisis cualitativo

El análisis cualitativo utiliza formatos de palabras o escalas descriptivas para representar la magnitud de las consecuencias potenciales y la probabilidad de que esas consecuencias ocurran. Estas escalas se pueden modificar o ajustar

para adaptarlas a las circunstancias, y se pueden utilizar distintas descripciones para riesgos diferentes (AS/NZS, 1999).

El análisis cualitativo se utiliza:

I. como una actividad inicial de tamiz, para identificar los riesgos que requieren un análisis más detallado;
II. cuando el nivel de riesgo no justifica el tiempo y esfuerzo requerido para un análisis más completo;
III. cuando los datos numéricos son inadecuados para un análisis cuantitativo.

b) Análisis semi-cuantitativo

En el análisis semi-cuantitativo, a las escalas cualitativas, se les asignan valores. El número asignado a cada descripción no tiene que guardar una relación precisa con la magnitud real de las consecuencias o probabilidades. Los números pueden ser combinados en cualquier rango de fórmula dado que el sistema utilizado para priorizar confronta el sistema seleccionado para asignar números y combinarlos. El objetivo es producir un ordenamiento de prioridades más detallado que el que se logra normalmente en el análisis cualitativo, y no sugerir valores realistas para los riesgos tales como los que se procuran en el análisis cuantitativo (AS/NZS, 1999). Se debe tener cuidado con el uso del análisis semi-cuantitativo porque los números seleccionados podrían no reflejar apropiadamente las relatividades, lo que podría conducir a resultados inconsistentes. El análisis semi-cuantitativo puede no diferenciar apropiadamente entre distintos riesgos, particularmente cuando las consecuencias o las probabilidades son extremas.

Es apropiado en ocasiones considerar la probabilidad compuesta de dos elementos, a los que se refiere generalmente como frecuencia de la exposición y probabilidad. Frecuencia de la exposición es la extensión a la cual una fuente de riesgo existe, y probabilidad es la oportunidad de que, cuando existe esa fuente de riesgo, le seguirán las consecuencias. Deberá ejercerse precaución en las situaciones en que las relaciones entre los dos elementos no es completamente independiente, ejemplo: cuando hay una fuerte relación entre frecuencia de la exposición y la probabilidad. Este enfoque se puede aplicar en el análisis semi-cuantitativo y cuantitativo.

c) Análisis cuantitativo

El análisis cuantitativo utiliza valores numéricos para las consecuencias y probabilidades (en lugar de las escalas descriptivas utilizadas en los análisis cualitativos y semi-cuantitativos) por medio de datos de distintas fuentes. La calidad del análisis depende de la precisión e integridad de los valores numéricos utilizados. Las consecuencias pueden ser estimadas al modelar los resultados de un evento o conjunto de eventos, o por extrapolación a partir de estudios experimentales o datos del pasado. Las consecuencias pueden ser expresadas en términos de criterios monetarios, técnicos o humanos, o cualquier otro. En algunos casos se requiere más de un valor numérico para especificar las consecuencias para distintos momentos, lugares, grupos o situaciones. La probabilidad es expresada generalmente como una probabilidad, una frecuencia, o una combinación de exposición y probabilidad. La forma en que se expresan las probabilidades y las consecuencias y las formas en que las mismas son combinadas para proveer un nivel de riesgo varían de acuerdo con el tipo de riesgo y el contexto en el cual se va a utilizar el nivel de riesgo (AS/NZS, 1999). La expresión formal de un riesgo es una oración que resume los elementos característicos de un riesgo dando una forma que facilite su comprensión y comunicación. Debe de ser completa, clara, precisa y concisa. Para ello podemos utilizar el siguiente modelo:

"Riesgo de que la cualidad benéfica de un bien en una determinadas circunstancias, pueda sufrir una manifestación, motivada por una causa con resultados consecuencias negativas".

Ahora cabe señalar algo relevante sobre estos conceptos. Se mencionó que la amenaza se puede expresar matemáticamente como una probabilidad, sin embargo en materia de seguridad física el estudio sobre probabilidades de amenazas antropogénicas (robos, delincuencia organizada, secuestros, vandalismo, sabotaje, etc.), aún se encuentra en desarrollo, por lo cual estas amenazas no son tratadas matemáticamente, sino cualitativamente a través de diferentes métodos: investigación de la zona, registros anteriores, experiencia relevante, etc. Por lo que generalmente se emplea el análisis cualitativo o semi-cuantitativo en materia de seguridad física.

El tratamiento de los riesgos.

El tratamiento de los riesgos involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este

tratamiento y ejecutarlos. Las opciones, que no son exclusivas, ni excluyentes, tampoco son apropiadas en todas las circunstancias. Son las siguientes:

a) **Evitar el riesgo.** Conseguir la eliminación absoluta de un determinado riesgo, a través de la anulación de la fuente de peligro o de los activos que intervienen en la actividad, o de no proceder con la actividad que probablemente generaría el riesgo.
b) **Reducir la probabilidad de la ocurrencia.** Es la reducción de los riesgos a través de intervenir en la reducción de la probabilidad y la minimización de la intensidad. Para lo primero se actúa sobre las fuentes de peligro, los activos y el medio mediante medidas preventivas puras. Para la minimizarlas se actúa sobre las vulnerabilidades, al identificar y atender estas.
c) **Reducir las consecuencias.** Minimizar la intensidad al actuar sobre los activos dañados y el medio, y al adoptar medidas asistenciales y reparadoras.
d) **Transferir los riesgos.** Implica que otra parte, un tercero, soporte o comparta parte del riesgo.
e) **Retener los riesgos.** Luego de que los riesgos hayan sido reducidos o transferidos, habrá riesgos residuales que pueden ser retenidos, es decir que se acepta su existencia y se toma responsabilidad y consciencia de sus posibles consecuencias. A veces esta retención no es voluntaria, sino que viene impuesta por la imposibilidad de transferir los mismos.

En todo caso, en el riesgo convergen simultáneamente tres aspectos separados: la eventualidad, las consecuencias y el contexto, que contribuyen a la hora de intentar llevar a cabo cualquier estimación o calificación del riesgo. En un análisis de riesgo, el contexto (capacidad de la gestión y actores relacionados) determina los límites, las razones, el propósito y las interacciones a considerar. Cualquier análisis que se realice debe ser congruente con el contexto y tenerlo en cuenta en todos los aspectos que le sean relevantes, de lo contrario el análisis sería totalmente inútil e irrelevante (Cardona, 2001).

1.5 Las infraestructuras críticas como caso de estudio

El término de infraestructuras críticas se define como una red distribuida de procesos repartidos e independientes que trabajan en colaboración y sinérgicamente para producir y distribuir un servicio esencial (Balducelli, 2003), y es usado por los gobiernos para describir los activos que son esenciales para el funcionamiento de una sociedad y economía y son aquellas

instalaciones físicas e información tecnología, redes, servicios y activos que, en caso de interrupción o destrucción, tendrían repercusiones graves sobre la salud, la seguridad, la protección, el bienestar económico, y el funcionamiento efectivo de la sociedad y del gobierno (Diu, 2007). Esta infraestructura crítica puede ser:

- Pública o privada
- Local, regional, nacional e internacional
- Grande y complejo. Normalmente, una red de redes
- Con una fuerte interdependencia entre ellas
- Con una dependencia que se en incremento en Tecnologías de la Información y redes de comunicación
- Son un eje vital de las sociedades modernas
- Con una conexión económica y social fuerte

Las instalaciones comúnmente asociadas con el término son:

- generación, transmisión y distribución de energía eléctrica;
- producción, transporte y distribución de gas;
- producción, transporte y distribución de petróleo y sus productos;
- telecomunicaciones;
- suministro de agua (agua potable, aguas residuales / aguas residuales, procedentes de las aguas superficiales (por ejemplo, diques y esclusas));
- agricultura, producción y distribución de alimentos;
- salud pública (hospitales, ambulancias);
- sistemas de transporte (de suministro de combustible, red ferroviaria, aeropuertos, puertos);
- servicios financieros (banca);
- servicios de seguridad (policía, militares).

Las infraestructuras críticas, con su evolución se han convertido en sistemas altamente interconectados e interdependiente, dando paso a un término conocido como Grandes Infraestructuras Críticas y Complejas (*LCCI*, *Large Complex Critical Infrastructure*). En ellas se presenta una intradependencia, es decir una dependencia mutua del mismo tipo de infraestructuras pertenecientes a diferentes regiones o países, y una interdependencia, esto es, una dependencia mutua entre los diferentes tipos de infraestructuras. Esta interdependencia puede ser:

- Física (Servicios o materia prima empleadas para otra infraestructura)
- Informática (Vínculos de información electrónica)

- Geográfica (Uso de mismo corredor o de compartir instalaciones)
- Lógico (dependencia mercados financieros)

Los LCCI se caracterizan por tener diferentes capas, en las cuales se identifican diferentes sistemas que se interconectan de un nivel a otro para dar soporte al sistema de infraestructura (físicamente el mayor de estos). Particularmente, la Red de Sistemas de Información Intensiva (NIISs, Networked Information Intensive Systems), gestiona la parte de TI que da soporte a las actividades de la infraestructura y es una de las características especiales de los LCCI.

Las intrusiones e interrupciones en una infraestructura de esta naturaleza podrían provocar fallos inesperados a otros sistemas e infraestructuras. El cómo manejar las interdependencias e intradependencias se convierte entonces un problema importante, y el asunto de la seguridad de estas infraestructuras toma cada vez mayor relevancia. Las LCCI se encuentran a merced de diferentes tipos de amenazas: desastres naturales, errores e incidentes humanos y actos humanos perniciosos premeditados, y es hoy en día un blanco preferido de las amenazas. La seguridad en las infraestructuras críticas tiene por objeto reducir la vulnerabilidad de estas estructuras, incrementar su capacidad de supervivencia y su capacidad de resistencia, así como reducir las pérdidas potenciales asociadas a los riesgos existentes.

La protección de infraestructuras críticas (*CIP, Critical Infrastructure Protection)* es un concepto que se refiere a la preparación y respuesta a incidentes graves que involucran a la infraestructura crítica de una región o nación. En Estados Unido de Norteamérica, la *American Presidential Directive* PDD-63 de mayo de 1998 establece un programa nacional de "protección de infraestructuras críticas". Por su parte, en Europa, su equivalente es el Programa Europeo para la Protección de Infraestructuras Críticas (*PEPIC*, European Programme for Critical Infrastructure Protection) se refiere a la doctrina o programas específicos creados como resultado de la directiva UE COM 2006, 786 de la Comisión Europea, que designa a las infraestructuras críticas europeas que, en caso de fallo , incidente o ataque, podrían tener un impacto tanto en el país donde se encuentra alojada como por lo menos otro Estado miembro de la Comunidad Europea. Los Estados miembros están obligados a adoptar la Directiva 2006 en sus legislaciones nacionales. Un enfoque integral para el análisis de las LCCI´s en la elaboración de los planes para la protección de esta infraestructura, proporcionara a estas una mejor capacidad de supervivencia.

La industria petroquímica como LCCI

La industria del petróleo y sus derivados forma parte de la llamada infraestructura crítica, como ya se ha mencionado, dada la vital importancia que tiene para la nación industria energética, no sólo por su aportación económica, sino que además, entre otros factores, por su relevancia social, impacto ambiental y político. Esta es la razón por la cual garantizar la seguridad de la infraestructura de Petróleos Mexicanos y sus Organismos subsidiarios resultan de un gran valor estratégico.

PEMEX es una LCCI porque cumple en principio con el concepto de ser una infraestructura crítica. En PEMEX se lleva a cabo diferentes procesos repartidos a lo largo de todo el país, y su interdependencia con otros sistemas e infraestructuras resulta evidente, (mayoritariamente como proveedor de materia prima más que de servicios), u tienen una fuerte relación económica con el país no sólo como generador de recursos económicos, sino también como proveedor de empleos y motor económico regional, además de ser un actor político relevante y ser parte del consiente colectivo de la sociedad mexicana. Su crecimiento a lo largo del tiempo ha llevado a PEMEX a una mayor de dependencia de los sistemas de apoyo tecnológicos como sólo el uso de Tecnologías de la información y el empleo de tecnología que permite garantizar la operación continua de sus instalaciones.

PEMEX opera por conducto de un corporativo y cuatro organismos subsidiarios:

- **Petróleos Mexicanos.** Es el responsable de la conducción central y de la dirección estratégica de la industria petrolera estatal, y de asegurar su integridad y unidad de acción.
- **PEMEX Exploración y Producción (PEP).** Es el responsable de la exploración y explotación del petróleo y el gas natural; su transporte, almacenamiento en terminales y su comercialización de primera mano; estas actividades se realizan cotidianamente en cuatro regiones geográficas que abarcan la totalidad del territorio mexicano: Norte, Sur, Marina Noreste y Marina Suroeste. PEP a nivel mundial ocupa el tercer lugar en términos de producción de crudo, el primero en producción de hidrocarburos costa fuera, el noveno en reservas de crudo y el doceavo en ingresos.
- **PEMEX Refinación (PR).** Sus funciones básicas son los procesos industriales de refinación, elaboración de productos petrolíferos y derivados del petróleo, su distribución, almacenamiento y venta de

primera mano. La Subdirección Comercial de PEMEX Refinación realiza la planeación, administración y control de la red comercial, así como la suscripción de contratos con inversionistas privados mexicanos para el establecimiento y operación de las Estaciones de Servicio integrantes de la Franquicia PEMEX para atender el mercado al menudeo de combustibles automotrices.

- **PEMEX Gas y Petroquímica Básica (PGPB).** Dentro de la cadena del petróleo, PEMEX Gas y Petroquímica Básica ocupa una posición estratégica al tener la responsabilidad del procesamiento del gas natural y sus líquidos, así como del transporte, comercialización y almacenamiento de sus productos. En el ámbito internacional, PEMEX Gas y Petroquímica Básica es una de las principales empresas procesadoras de gas natural, con un volumen procesado cercano a 4 mil millones de pies cúbicos diarios (mmpcd) durante el 2004, y la segunda empresa productora de líquidos, con una producción de 451 mil barriles diarios (mbd) en los 11 Centros Procesadores de Gas a cargo del Organismo. Cuenta con una extensa red de gasoductos, superior a 12 mil kilómetros, a través de la cual se transportan más de 3,600 mmpcd de gas natural, lo que la ubica en el décimo lugar entre las principales empresas transportistas de este energético en Norteamérica. En México, PEMEX Gas y Petroquímica Básica se encuentra entre las 10 más grandes por su nivel de ingresos, superiores a 16,300 millones de dólares en 2004, con activos cercanos a 9,000 millones de dólares. Adicionalmente, PEMEX Gas y Petroquímica Básica constituye una fuente importante de trabajo, al emplear del orden de 12 mil trabajadores.
- **Pemex Petroquímica (PQ).** Elabora, comercializa y distribuye productos para satisfacer la demanda del mercado a través de sus centros de trabajo. Su actividad fundamental son los procesos petroquímicos no básicos derivados de la primera transformación del gas natural, metano, etano, propano y naftas de Petróleos Mexicanos. PEMEX Petroquímica guarda una estrecha relación comercial con empresas privadas nacionales dedicadas a la elaboración de fertilizantes, plásticos, fibras y hules sintéticos, fármacos, refrigerantes, aditivos, etc.

De acuerdo con documentos elaborados por Petróleos Mexicanos, en el interior de todo su sistema hay vulnerabilidad y no existen garantías de seguridad, aun cuando el Ejército y la Armada intensifiquen la vigilancia sobre sus instalaciones estratégicas para evitar actos terroristas o sabotajes. Información

oficial de PEMEX indica que los principales problemas son el escaso control de acceso a las instalaciones en general, especialmente fuera de las ciudades; equipos de informática obsoletos que no permiten monitorear adecuadamente las instalaciones ni las operaciones de la empresa; y que el Plan Rector de Seguridad Física no se cumple en ninguna de las cuatro filiales.[1] Esta situación, según la propia paraestatal dificulta la capacidad de minimizar el impacto en el negocio de cualquier amenaza interna o externa, el proteger información estratégica y activos, así como lograr la continuidad del negocio.

La madrugada del 10 de septiembre de 2007, se registraron una serie de explosiones en seis puntos diferentes de ductos de Veracruz y Tlaxcala, cuya autoría se adjudicó el Ejército Popular Revolucionario (EPR). Esa organización también se responsabilizó de los actos de sabotaje ocurridos el 5 y 10 de julio del mismo año en ductos de Pemex en Guanajuato y Querétaro. Los reportes de PEMEX concluyen que la seguridad de 364 campos de producción, 6 mil 80 pozos, 199 plataformas, 6 refinerías, 12 centros procesadores de gas, 8 centros petroquímicos, 77 terminales de almacenamiento de refinados y 20 de gas LP, estaría en entredicho.

La problemática trascendió partir de las explosiones de julio de 2007 en ductos de Guanajuato y Querétaro, lo cual obligó a las filiales PEMEX Exploración y Producción (PEP), Pemex Refinación (PR), Pemex Gas y Petroquímica Básica (PGPB) y Pemex Petroquímica (PPQ) a solicitar recursos presupuestales para fortalecer sus sistemas de seguridad. Sin embargo, todas las solicitudes fueron registradas pero no atendidas por la Secretaría de Hacienda, que las clasificó como "sin asignación presupuestal" para 2008". Por ejemplo, PEP solicitó mil 372 millones de pesos para "desarrollo de proyectos de investigación y aplicación de nuevas tecnologías para resolver la problemática específica que plantean los procesos de explotación de hidrocarburos y contar con equipos de cómputo para planes contingentes". En el caso de PR, el diagnóstico señala que la base instalada de computadoras personales en todas las áreas de la filial era de 13 mil 512 equipos, de los que 6 mil 48 cumplirán en 2007 cinco o más años de antigüedad, considerándose como tecnología obsoleta que presenta un rango de operaciones limitado, lo que incrementa el riesgo de seguridad y de fallos en los sistemas computacionales y aumenta la posibilidad de perder información (Cruz, 2007).

[1] El Universal, nota de Noé Cruz Serrano y Silvia Otero, Jueves 13 de septiembre de 2007, en http://www.eluniversal.com.mx/nacion/154143.html

En las inspecciones realizadas a PGPB por la Auditoria de Seguridad Industrial y Protección Ambiental (ASIPA, organismo de PEMEX), que incluye visitas del reaseguro internacional, programas de mantenimiento y pruebas a los sistemas de procesamiento y servicios auxiliares existentes, se detectó el incumplimiento de los requerimientos técnicos normativos vigentes, sobre todo por obsolescencia tecnológica, por lo que aún no se ha podido garantizar la confiabilidad de centros procesadores, tanto en términos operativos como de seguridad (Cruz, 2007). Para PEMEX resulta de alta prioridad garantizar medidas de seguridad física que comprendan un conjunto coordinado de acciones cuyo objetivo sea asegurar la integridad física del personal, instalaciones, bienes y medio ambiente ante riesgos y posibles daños producidos por la acción intencional del hombre; así como los propios riesgos de los procesos industriales (estos últimos cubiertos con procedimientos de seguridad industrial). Para ello cuenta con el Plan Rector de Seguridad física de Petróleos Mexicanos y Organismos Subsidiarios. En dicho plan se definen los objetivos estratégicos, líneas estratégicas, líneas de acción y actividades sustantivas, que orientaran la elaboración y aplicación de los programas que en esta materia se establezcan al interior de Petróleos Mexicanos y Organismos Subsidiarios y, al exterior, en coordinación con otras dependencias con responsabilidades en la Seguridad Nacional y Publica, en los términos que conforme a la ley aplicable procédala (PEMEX, Plan Rector, 2001) y refleja los ideales de lo que se espera sea la seguridad dentro de las instalaciones de PEMEX.

Para ejemplificar los conceptos descritos anteriormente, el área Petroquímica de PEMEX, a partir del cual se explicaran los elementos involucrados en la seguridad física en este tipo de infraestructura (LCCI). PEMEX PQ tiene una estructura en la que se identifica una Dirección General de Petroquímica, la cual se llevan las labores de operación, planeación, comercialización, administración y finanzas de petroquímica en general, y 7 filiales o Complejos Petroquímicos: Cangrejera, Cosoleacaque, Escolín, Morelos, Pajaritos, Tula y la Unidad Petroquímica Camargo. Dichos Complejos y la Dirección General, componen la infraestructura de PQ.

El sur del estado de Veracruz concentra no sólo la mayor cantidad de infraestructura petroquímica de PEMEX, sino también la más importante de México. En esta zona se ubican las oficinas centrales de la Dirección General (en la Ciudad de Coatzacoalcos) y 4 de los principales Complejos Petroquímicos: Cosoleacaque, Cangrejera, Morelos y Pajaritos (muy cercanos a esta misma

ciudad). La siguiente figura ilustra la ubicación de los Complejos petroquímicos de PQ.

Figura 1. Ubicación de los 8 Complejos Petroquímicos de PEMEX PQ.
Fuente: PEMEX PQ

La industria petroquímica es una plataforma fundamental para el crecimiento y desarrollo de importantes cadenas industriales como son la textil y del vestido; la automotriz y del transporte; la electrónica; la de construcción; la de los plásticos; la de los alimentos; la de los fertilizantes; la farmacéutica y la química, entre otras. Actualmente PEMEX Petroquímica aporta el 2% de PIB nacional.

La infraestructura de PQ puede ser vista como una LCCI, en primer lugar porque se trata de una infraestructura crítica, con una gran cantidad de interrelaciones: su aportación a la economía nacional, su relación con la industria privada con la aportación de materia prima, como fuente de empleo y motor de la economía regional y por lo que su simple imagen significa, entre otros. Como ya se ha explicado, es debido a estas interrelaciones que el tema de la seguridad de este tipo de infraestructuras se vuelve de alta prioridad. Para ejemplificar algunos de los aspectos que en materia de seguridad ya se han

explicado, se ha tomado como sujeto de apoyo a PEMEX PQ, específicamente la zona sur del Estado de Veracruz.

Ámbitos de seguridad y responsabilidad en PEMEX PQ

Anteriormente se mencionó que los ámbitos de la seguridad determinan a los actores responsables de la procuración de seguridad y sus responsabilidades. En PEMEX PQ, como se ha explicado, su posición en la economía nacional la convierte en un objetivo estratégico para la nación. Por ello, el ámbito de seguridad abarca los tres ámbitos explicados.

a) Secretaria de la Defensa Nacional (SEDENA)

Es el responsable a nivel Federal (es decir el Estado) de proveer servicios de seguridad física a este tipo de instalaciones dada su posición y naturaleza. En el caso de la infraestructura petrolera, a través del Convenio de Colaboración PEMEX-SEDENA, el cual tiene por objeto definir que la SEDENA a través de su personal militar, proporcione permanentemente a PEMEX y a sus Organismos Subsidiarios: PEP, PR, PGPB, y PQ, protección, seguridad física a las instalaciones de la industria petrolera estatal y patrullaje a su Red de Ductos, localizadas en el territorio nacional. Dichas actividades son realizadas en coordinación con la administración interna de seguridad física de cada subsidiaria y con los elementos de la Gerencia de Servicios de Seguridad Física (GSSF). Implementa en coordinación con el personal de GSSF y vigilancia, las acciones necesarias para que se brinde seguridad física a las instalaciones y patrullaje sobre los derechos de vía, y en caso de que se presente una emergencia que atente en contra de las instalaciones. Pueden también detener, en caso de flagrancia, a los sujetos que sean sorprendidos realizando alguna actividad delictiva que atente contra de las instalaciones y el personal de la organización, y ponerlos sin demora a disposición de las autoridades competentes más cercanas al lugar de los hechos, previa coordinación con personal de GSSF.

b) Seguridad pública (Policías municipal y estatal)

A nivel municipal y estatal no existe un acuerdo directo para la procuración de seguridad física, sin embargo en los procedimientos de conducción de sospechosos o responsables de algún evento existe un determinado grado de colaboración.

c) Personal interno de seguridad física

La procuración de seguridad física al interior de los Complejos de PQ es realizada a través de personal del Departamento de Vigilancia de cada Complejo, así como por personal de la GSSF, estos últimos bajo las órdenes del Corporativo de PEMEX Petroquímica, bajo el Convenio de Colaboración PEMEX Petroquímica-GSSF, mediante el cual tiene por objeto la colaboración entre las partes (PEMEX Petroquímica y GSSF) a efecto de que PEMEX (Corporativo) por conducto de la GSSF brinde seguridad física a las instalaciones de Petroquímica. Estos dos elementos son los responsables directos de llevar a cabo la aplicación de las medidas y acciones en materia de seguridad física (procedimientos para la entrada y salida de Complejo, así como procedimientos operativos de seguridad física como son: amenaza de bomba, sabotaje, bloqueo de las instalaciones, etc.). El personal de vigilancia está estructurado por medio de una jefatura de vigilancia, a cargo de los porteros, cabos y vigilantes, y se encuentra supervisada por la Superintendencia de Higiene Industrial, Normatividad y Estadística (SHINE). La jefatura de seguridad física coordina conjuntamente a la GSSF las acciones de seguridad física dentro de cada complejo en operación normal, bajo sospecha o en presencia de una contingencia, con el apoyo que ambos consideren necesario por parte de la SEDENA. Revisa las medidas y dispositivos en materia de seguridad física del Complejo.

Por otra parte, el personal de la GSSF es el encargado realizar las labores de investigación, así como de detención y conducción de sospechosos o de aquellos sujetos sorprendidos en delito fragante para ponerlos a disposición de la autoridad competente más cercana. Tiene también las funciones, dirigir y controlar la ejecución de acciones que permitan detectar riesgos y prevenir la realización de actos de sabotaje, atentados o agresiones, que pongan en peligro el orden laboral, la integridad del personal, bienes y valores del Complejo. Reporta de manera inmediata las anomalías e incidentes que ocurran, así como los materiales y/o equipos recuperados y/o asegurados, al titular de la Gerencia del centro de trabajo, Superintendencia de Calidad, Seguridad Industrial y Protección Ambiental (responsables de la seguridad industrial en cada Complejo), así como a la Superintendencia de Higiene Industrial Normatividad y Estadísticas. Otra de las tareas de la GSSF es proporcionar apoyo logístico a funcionarios, búsqueda y recolección de información de hechos que puedan atentar contra sus instalaciones y trabajadores, así como supervisar el cumplimiento de las normas de seguridad física y proponer el establecimiento de medidas y sistemas de protección en las instalaciones.

Por su parte la Superintendencia de Higiene Industrial Normatividad y Estadísticas tiene es la responsable de vigilar que se mantengan vigentes y se cumplan los acuerdos y convenios establecidos entre PEMEX y la SEDENA. Proporcionar el apoyo necesario a la organización de seguridad física para cumplir con lo establecido en los programas de Seguridad física. Mantener en condiciones de operación los sistemas de seguridad física (elementos físico-tecnológicos) que se tengan establecidos, así como su apropiado mantenimiento.

d) PEMEX Corporativo

PEMEX Corporativo es el responsable de establecer y elaborar la normatividad en materia de Seguridad física. Es también responsable directo de la GSSF y coordina con ellos directamente las labores de investigación y recibe los reportes de eventos de estos. Es también el encargado de revisar, aprobar y supervisar los proyectos en materia de Seguridad física que propuestos para el Complejo, así como de proveer los recursos financieros para la implementación de dichos proyectos.

e) Protección civil

Protección civil del estado (Veracruz) mantiene una vinculación con la industria en general en la zona, para poder responder conjuntamente ante emergencias que pudieran poner en riesgo a la comunidad. Esta coordinación es con el área encargada de la seguridad industrial del Complejo, y atiende primordialmente a las emergencias provocadas por fenómenos naturales: sismos, huracanes, inundaciones, etc.

Amenazas

Antecedentes delictivos y problemas de seguridad en la zona

En el estado de Veracruz, durante el año de 2002, se cometieron 65,523 delitos, mientras que en 2007, 76,560 (Zavaleta, 2010). Los delitos del fuero común que más incremento tuvieron en este periodo fueron el robo, los daños y las violaciones. Los delitos del fuero común se han incrementado en Veracruz en términos absolutos durante el periodo 2004- 2007. Los delitos con mayor tasa delictiva son el robo, los daños, las lesiones y las violaciones. El robo, el delito más frecuente, se incrementó de 16,079 a 20,910 en las modalidades de robo común y abigeato durante el periodo 2003-2007. En la ciudad de Xalapa se cometieron 3,304 robos en 2005-2006; en Veracruz Puerto se cometieron 3,304 robos sólo en 2005; en Coatzacoalcos, 2,486 entre 2005 y el primer semestre de 2006; en Boca del Río 1,672 robos en 2005- 2006; en Poza Rica, 1,181 robos en

2005-2006; en Tuxpan, 608 en 2005, en Minatitlán 523, en Córdoba 746, y en Orizaba, 530 en el mismo año (Zavaleta, 2010). Los municipios con mayor tasa delictiva son Pánuco, Ozulama, Huayacocotla, Poza Rica, Martínez de la Torre, Perote, Xico, Veracruz, Boca del Río, La Antigua, Minatitlán, Las Choapas, Coatzacoalcos, Acayucan, Tierra Blanca y Cosamaloapan.

De acuerdo con estudios estadísticos (Zavaleta, 2010), los delitos con mayor crecimiento absoluto fueron el robo, las lesiones, los daños y las coacciones. En el mismo periodo, los delitos del fuero federal cometidos en Veracruz se incrementaron de 378 a 583. Los delitos de este tipo más cometidos fueron el comercio y la posesión de drogas, la violación a la ley de población y los delitos fiscales. Entre el último trimestre de 2007 y el tercero de 2008 se recibieron 139 denuncias de narcomenudeo, 103 denuncias anónimas. En el primer cuatrimestre de 2007 se ejecutaron en Veracruz a 28 personas.

La delincuencia organizada en Veracruz

En Veracruz, de acuerdo con la Secretaria de Seguridad Pública Federal (SSPF), no hay narco-municipios, aunque sí están ubicados algunos municipios de los 353 clasificados por la misma SSPF con altos índices de inseguridad, entre otros, Pánuco, Naranjos, Tuxpan, Álamo, Poza Rica, Martínez, Perote, Cardel, Xalapa, Huatusco, Córdoba, Orizaba, Cuitláhuac, Tierra Blanca, Veracruz, Alvarado, Cosamaloapan, San Andrés, Acayucan, Coatzacoalcos, Minatitlán y Las Choapas (Zavaleta, 2010).

En el estado operan básicamente dos organizaciones delictivas y sus respectivos grupos de sicarios: La organización de Sinaloa con su grupo Gente Nueva y la organización del Golfo y los Zetas. Hay presencia en los municipios de Coatzacoalcos y Minatitlán de redes de la organización de Oaxaca. Estas células de organizaciones delictivas son segmentos de los llamados cárteles de Sinaloa, Cártel del Golfo y del Cártel de Pedro Díaz Parada.

Las actividades delictivas organizadas son diversas, tráfico de drogas, narcomenudeo, secuestros, asaltos, robo de automóviles. El mercado de los delitos organizados en Veracruz es controlado básicamente por la Organización del Golfo, pero ahora la organización de Sinaloa disputa el centro y el sur del Estado mediante levantones y ejecuciones. Las plazas de disputa son las el Puerto, Boca del Río y las ciudades medias tales como Poza Rica, Martínez de la Torre, Xalapa, Córdoba, Coatzacoalcos. Estos mercados delictivos funcionan con protección sin embargo, no es posible afirmar con pruebas la existencia de redes de narco-política.

El mapa del narcotráfico en el estado está divido en tres, el norte del estado está controlado por el Cártel del Golfo y los zetas, el centro del estado, el cual incluye a Xalapa y Veracruz, está controlada por Gente Nueva y el sur lo comanda el Chapo Guzmán. Las ejecuciones se han concentrado en la zona urbana de Veracruz Puerto- Boca del Río, Coatzacoalcos, Minatitlán, Poza Rica y Xalapa. En las elecciones intermedias hubo denuncias de la existencia de vínculos entre candidatos y narcotraficantes pero no hay evidencias empíricas de la institucionalización de la narco-política en el Estado (Zavaleta, 2010).

Antecedentes de sabotajes en la zona

En el 2007 PEMEX fue víctima de actos de sabotaje en esta región. Seis explosiones provocadas se registraron en la madrugada del 10 de septiembre de 2007 en varias instalaciones de la red de gasoductos este estado, pero no dejaron heridos.[2] Las explosiones se debieron a actos premeditados que obligaron a evacuar varias comunidades de este estado del golfo de México, uno de los que tiene más instalaciones petroleras en el país. Las detonaciones causaron al menos cuatro incendios que fueron controlados por personal de la paraestatal y Protección Civil estatal y municipal. Las autoridades evacuaron a más de 16,250 personas de cinco comunidades vecinas a los lugares en que se presentaron las explosiones provocadas.

A principios de julio del mismo año hubo otras detonaciones provocadas en varias instalaciones de PEMEX en el centro del país, también sin daños personales. Los atentados de septiembre de 2007 se registraron en los municipios de La Antigua, Omealca, Minatitlán y Actopan, donde se detectó una pérdida de presión inusual en seis puntos diferentes. El Ejército Popular Revolucionario (EPR), se adjudicó ambos atentados.

Los atentados se presentaron en una válvula del gasoducto de 48 pulgadas de gas natural Cactus-San Fernando, a la altura del Municipio La Antigua, donde autoridades de protección civil evacuaron a más de 6,000 personas. En ese mismo gasoducto ocurrió otro estallido en una válvula situada cerca al río Actopan. Otra explosión tuvo lugar en el gasoducto Zempoala-Santa a la altura de Delicias. Asimismo se presentaron tres detonaciones más en distintos puntos del gasoducto Minatitlán-México, que afectaron a un gasoducto de 30 pulgadas. La comunicación por carretera fue suspendida en los tramos que van

[2] El Universal, nota de Juan Veledíaz, Alejandro Suverza y Blanca Patricia Galindo, Martes 11 de septiembre de 2007

de Xalapa al puerto de Veracruz, de Córdoba a Ciudad de México y de Minatitlán al puerto de Coatzacoalcos.

Antecedentes de desastres naturales

El área del Sur de Veracruz puede ser afectada por la presencia de sistemas ciclónicos que se desarrollan en el Atlántico y que pueden entrar al Golfo de México. Generalmente estos sistemas no tienen trayectorias que se dirijan directamente hacia el área de Coatzacoalcos, sin embargo en ocasiones pueden llegar a Impactarse en esa zona. La peligrosidad por frecuencia de impacto en la zona es baja, pero a nivel de intensidad puede llegar a ser media, ya que durante el periodo de análisis (1960-1998) ha llegado a tener penetraciones directas en tierra del municipio de huracanes con categoría 1. Lo anterior se traduce en vientos de hasta 130 km/h y marejadas de 1.5m., los meses más afectados por la influencia de ciclones van de julio a octubre, con impactos en agosto y octubre.

Lluvias torrenciales

Se presentan en la zona en los meses de junio a septiembre con una precipitación que va de 200 a 400 mm. Existen antecedentes de lluvias torrenciales en el año 2003 los cuales otorgaron a la zona la Declaratoria de Desastre Natural.

Actividad sísmica

De acuerdo con la regionalización sísmica de la república mexicana se establece como un área de riesgo sísmico medio a moderado. El último sismo registrado en la Entidad fue el pasado 31 de mayo de 2010 con una magnitud de 4.2 grados y el epicentro tuvo su origen 73 kilómetros al suroeste de Coatzacoalcos.

Actividad volcánica

El riesgo por actividad volcánica se encuentra considerado como mediano debido a que se encuentra a tan sólo 50 kilómetros de la región de los Tuxtlas en Veracruz, el volcán Chichonal se encuentra a una distancia de 160 kilómetros al sureste en el estado de Chiapas y la región de los volcanes de Guatemala a 480 kilómetros de distancia al sureste.

Vulnerabilidades

Ya anteriormente en este mismo Capítulo se señalaba de forma general que los problemas que enfrentan las diferentes filiales de PEMEX son: el escaso control

de acceso a las instalaciones en general; equipos de informática obsoletos que no permiten monitorear adecuadamente las instalaciones ni las operaciones de la empresa; y que no se cumple con el Plan Rector de Seguridad Física en ninguna de las filiales.

Este trabajo parte de un estudio de reciente elaboración el cual obtuvo las vulnerabilidades de los diferentes Complejos Petroquímicos a través de un levantamiento en campo y un cruce de información con una investigación documental. En el proceso de investigación documental se realizó una recopilación de información que permitió determinar la posición estratégica de los diferentes Complejos en la industria petroquímica, conocer los procesos realizados, la importancia y peligrosidad de los productos manejados, así como toda aquella información referente a la seguridad física (procedimientos, programas, recursos humanos y materiales, etc.). Se obtuvo también información del los escenarios de riesgo dentro de cada Complejo (aquellas situaciones que de producirse representarían pérdidas potenciales humanas, materiales y económicas), así como su correspondiente estimación de consecuencias.

En el levantamiento en campo se determinaron la vulnerabilidad de los sistemas de seguridad de cada Complejo (factor de riesgo interno, que como, como se mencionó es la predisposición o susceptibilidad física, económica, política o social que tiene el sujeto/objeto de ser afectado o de sufrir daños en caso que un fenómeno desestabilizador de origen natural o antropogénico). Esto se obtuvo a través de la observación directa y posterior evaluación de los sistemas de seguridad, al estudiar su entorno, estado físico, ubicación, proceso de uso y manteamiento, así como de entrevistas semi-estructuradas con el personal del área de vigilancia (desde el menor hasta el mayor rango), utilización de grupos multidisciplinarios de expertos y evaluaciones individuales para cada elemento del sistema (físicos y administrativos). Esto para cada uno de los "anillos de seguridad" que conforman el Complejo. El Primer Anillo es la línea imaginaria que se constituye con medios humanos y materiales diversos para dar protección a las áreas vitales, estas áreas generalmente se encuentran al interior de las instalaciones, pero pueden también encontrarse fuera de las mismas. El segundo anillo queda constituido por los límites artificiales y/o naturales de la Instalación; generalmente se trata de bardas o cercas, así como obstáculos naturales, ríos o barrancas con características que permitan dar seguridad y protección pasiva. El tercer anillo, está definido como el área de patrullaje exterior. Cada uno de estos anillos contempla elementos propios lo cuales fueron evaluados durante este

levantamiento.

Los resultados obtenidos, de acuerdo con lo planteado por Anderson y Woodrow (1989), pueden integrarse en los siguientes aspectos que a largo plazo afectan a la organización en la capacidad para responder a sucesos y la hacen susceptible a sufrir consecuencias:

a) Físico-material. Son aquellos aspectos relacionados con el medio ambiente, la infraestructura, la tecnología y el capital. En este caso resulta evidente que por el tipo de zona (manglar-selvática), se propicia un ambiente de vulnerabilidad, dado que la maleza invade zonas del perímetro de los complejos, lo cual dificulta las labores vigilancia y patrullaje, compromete la integridad y daña las barreras perimetrales. A nivel de infraestructura, es una común que por las mismas características de la región, los caminos perimetrales suelen no existir, o no ser lo suficientemente adecuados para facilitar las labores de vigilancia y patrullaje. Así mismo, otro de los problemas que se suele enfrentar en este mismo ámbito es el incumplimiento a normatividades en materia de seguridad, que aplican a la infraestructura, como es el caso de barreras perimetrales que no satisfacen las medidas de seguridad necesarias, o iluminación perimetral insuficiente o inapropiada para las labores de vigilancia y patrullaje. En relación a la tecnología, mucha de la tecnología empleada en las labores de seguridad puede resultar obsoleta, encontrarse deteriorada o fuera de operación por fallas o falta de mantenimiento. Generalmente esta situación deriva de que el gasto en seguridad física es un gasto que "no se ve", es decir pareciera no contribuir a generar valor para la organización, situación que va de la mano con el asunto de capital.

b) Social-organizacional. Aspectos relativos a las actividades sociales y económicas y a las estructuras formales para la toma de decisiones. En este aspecto, existe una fuerte cantidad de reportes y es de conocimiento general, la constante de invasión a la zona por parte de los pobladores de las zonas aledañas, a pesar de ser una zona federal protegida. En estas invasiones muchas la infraestructura de seguridad es víctima de vandalismo o robo lo que compromete las labores de seguridad. De igual forma se tiene registro de problemas de robo hormiga por parte de los trabajadores, de equipo y material empleado o que da soporte a las labores de seguridad. Sobre las estructuras formales, generalmente en las organizaciones se suele no tener plena conciencia de las funciones,

alcances y responsabilidades del personal seguridad física o no se tienen procedimientos suficientes para responder a los diferentes eventos que pueden suscitarse.

c) De motivación y actitud. Esto se refiere a la concepción que tiene la organización de ella misma y sus interrelaciones con el medio ambiente y la sociedad. En ocasiones, la organización suele no contemplar el amplio espectro de amenazas a la que es susceptible, o no considera adecuadamente el nivel de impacto que las repercusiones que un evento negativo para ella generaría para la aquellos con los que tiene una interrelación.

Riesgos

A través de la investigación documental y del levantamiento en campo (amenazas y vulnerabilidades) se establecieron descripciones cualitativas de los sucesos que pudieran ocurrir (intrusiones, sabotaje, terrorismo, robo, etc.) en cada área determinada (anillos de seguridad), se definieron la naturaleza de estos (estratégicos, operacionales, financieros, etc.), se cuantificaron la importancia y probabilidad (cualitativamente), y se establecieron el potencial de pérdidas e impacto financiero y geográfico (riesgos). Todo esto a través de un método semi-cuantitativo.

El producto de este análisis y evaluación de riesgos permitió establecer el tratamiento del riesgo y mecanismos de control, así como las acciones potenciales de mejora, a través de recomendaciones para reducir el riesgo (o reducir la vulnerabilidad).

El resultado fue la identificación y jerarquización de riesgos en las plantas y zonas consideradas como áreas críticas que integran cada uno de los Complejos. En estos resultados se señala el índice de riesgo (menor, moderado o mayor); el escenario de riesgo (descripción del evento, por ejemplo una fuga de etileno en una línea/junta, por ejemplo en una tubería del separador, que se convierte en nube de vapor con masa de 500 kg., antes de ocasionar una explosión de vapor no confinada); la ubicación y el tipo de accidente que ocurriría, pérdidas potenciales derivadas.

Sin embargo, para poder cumplir con un análisis de riesgos que pueda ser conceptualizado de forma integral y no fragmentada, es necesario estimar el riesgo, desde un punto de vista multidisciplinar, no solamente el daño físico esperado, las víctimas o pérdidas económicas equivalentes, sino también

factores sociales, organizacionales e institucionales, que permitan evaluar la capacidad para responder o absorber el impacto de los involucrados en el sistema (Cardona, 2001). Información, comunicación y conocimiento deficientes entre los actores sociales, así como la ausencia de organización institucional y comunitaria, debilidad en la preparación para la atención de emergencias, inestabilidad política, falta de salud pública y una económica débil en un área geográfica contribuyen a tener un mayor riesgo. Por lo tanto, las consecuencias potenciales no sólo están relacionadas con el impacto del suceso, sino también con la capacidad para soportar el impacto y las implicaciones del mismo respecto del área geográfica considerada.

Visto desde esta perspectiva, el riesgo está también en función de la existencia de las estructuras administrativas de apoyo a emergencias, la capacidad de la infraestructura de salud y el tejido social. En este tenor, la industria de la zona cuenta con un Plan de Respuesta a Emergencias (PRE), que a través de un Comité Local de Ayuda Mutua (CLAM) que pone las bases para la respuesta a una emergencia mayor para compartir los recursos de los miembros de dicho comité. Sobre la infraestructura de salud, el municipio de Coatzacoalcos cuenta con 12 hospitales de la Secretaría de Salud, 2 del IMSS, 2 del ISSSTE, 1 de la Cruz Roja, 1 de PEMEX y 1 de la Secretaría de Marina, para la atención de 347 223 habitantes[3]. Si bien, en caso de presentarse un evento negativo de gran repercusión se tiene la capacidad material y administrativa para responder, la marcada desigualdad social de la zona podría tener como consecuencia una recuperación lenta a un evento de esta naturaleza.

Externalidades derivadas de la operación del objeto en función de la seguridad

Es necesario para terminar de redondear el carácter integral de este trabajo, definir algunas de las consecuencias de los eventos que pudieran acontecer, lo que ayudará a entender y componer el sistema de estudio.

Pérdidas económicas

En 2006 PEMEX ocupaba el lugar número 22 en la lista de los principales productores petroquímicos, y fue el principal de los productos el Etileno, y Veracruz es el líder nacional en ramas como la petroquímica básica, que equivale al 93.2% del total nacional. La siguiente tabla muestra la producción de petroquímicos por complejo petroquímico. En ella puede observarse que durante el 2007 La Cangrejera aumentó su participación en 20% respecto a

[3] Fuente: Enciclopedia de los Municipios de México, http://www.inafed.gob.mx/work/templates/enciclo/veracruz/municipios/30039a.htm

2006, para llegar así a una participación del 43.2% de la producción nacional, Cosoleacaque, por su parte, contribuyó durante el 2007 con el 23.3% de la producción, para lograr un aumento del 32.6% respecto a su producción el 2006, y Morelos, aunque contribuye casi con el 20% de la producción de PPQ tuvo una disminución del 4.6% respecto a 2006[4].

Complejo petroquímico	Producción en miles de toneladas 2006	Producción en miles de toneladas 2007	Variación anual (%)	(%) de producción de PPQ en 2007
Cosoleacaque	1,318.8	1,748.4	32.6	23.3
La Cangrejera	2,698.3	3,239.0	20.0	43.2
Morelos	1,552.9	1,481.0	-4.6	19.8
Pajaritos	864.7	966.5	11.8	12.9
Independencia	98.9	23.5	-76.3	0.3
Escolín	38.5	10.3	-73.2	0.1
Tula		27.4		0.4
Total PPQ	6,572.1	7,496.0	14.1	100.0

Tabla 1. Producción de petroquímicos por complejo petroquímico 2006-2007
Fuente: Portal de PEMEX Petroquímica

La siguiente tabla muestra algunos de los precios de los productos elaborados en este complejo, con información del 2007.

Producto	Precio Pesos por tonelada métrica
Estireno	17,230.1
Oxido de etileno	8,801.6
Polietileno baja densidad	16,926.1
Tolueno	11,729.4

Tabla 2. Precio promedio al público de productos petroquímicos seleccionados en el 2007, en pesos por tonelada métrica.
Fuente: Portal de PEMEX Petroquímica

Los datos anteriores señalan del potencial de pérdidas económicas derivadas de un paro de actividades. Más aún, en caso de presentarse un evento que atentara contra las instalaciones PQ las pérdidas económicas producidas por

[4] Fuente: PEMEX Petroquímica, www.ptq.pemex.com/

un paro de actividades se sumarían las pérdidas económicas ocasionadas por los daños producidos a la infraestructura PQ, específicamente a las diferentes plantas procesadoras, las cuales tienen un valor que va desde los 7 hasta los 50 Millones de Dólares (MDD). Además de las pérdidas mencionadas, se acumularían las correspondientes a gastos de seguro médico del personal, así como de los daños ocasionados a la comunidad aledaña, y la afectación de la industria regional que gravita en torno a PQ.

Existen también actos ilícitos que reportan pérdidas económicas derivadas de las vulnerabilidades en los sistemas de seguridad física, como el robo hormiga, robo de material, robo de cableado del alumbrado, etc., que aunque no se puedan cuantificar exactamente las pérdidas económicas que esto actos representan, sí contribuyen a aumentar el riesgo, ya que propician y favorecen a situaciones de vulnerabilidad para cualquier organización.

Veracruz ocupa el sexto lugar en la economía nacional. Las principales actividades productivas de Veracruz son la agricultura, la ganadería, la pesca, la industria metálica básica, los alimentos, bebidas, tabaco, petroquímica y electricidad; mientras que el sector industrial manufacturero ocupa la quinta posición del país. Un dato interesante es que el 80% de los activos fijos industriales del sureste de México se ubican en Veracruz, y a nivel nacional cuenta con el 9.75% del total de los activos fijos de la industria manufacturera. Tanto el municipio de Coatzacoalcos, como Minatitlán, son municipios urbanos con una alta actividad del sector terciario, (comercio, transporte y comunicaciones, servicios financieros, de administración pública y defensa, comunales y sociales, profesionales y técnicos, restaurantes, hoteles, manufactura y otros); y en casos como Nanchital, con una dependencia mayoritaria de la industria petroquímica, lo cual representaría una pérdida de actividad económica considerable. Adicionalmente, Veracruz cuenta con tres de los puertos más importantes de México, ubicados estratégicamente en el norte, centro y sur del Estado (este último en la zona petroquímica). En conjunto estos tres puertos operan el 28.48% de la carga contenerizada del país, así como el 40% del total nacional de los contenedores (Programa Sectorial de Desarrollo Económico, 2005).

Pérdidas humanas y materiales

En función del objetivo del evento, es decir del lugar en el que se presente el atentado, y si este llegara a producir una afectación que desencadene una situación de riesgo (aunado a un factor de tiempo), las perdidas irán desde los 8

metros (personal y equipo cercano a la zona), hasta los 7000 metros, (personal e infraestructura dentro de cualquiera de los Complejos y población alrededor de estos), y es este último el peor de los escenarios, ya que podría producirse una reacción en cadena que aumentaría aún más el área de pérdidas potenciales, pues un accidente de esta magnitud en uno de los Complejos podría iniciar un reacción de igual magnitud en alguno de los otros Complejos. Un accidente de esa magnitud afectaría a casi la mitad de la superficie total del municipio de Coatzacoalcos (especialmente la zona céntrica), el cual tiene un total de 347 223 habitantes; y la totalidad del municipio de Nanchital con 26 804 habitantes. El caso más drástico entre los eventos de emergencia que pudieran presentarse en la zona petroquímica de Veracruz, se encuentra en el Complejo Petroquímico Cosoleacaque, el cual se encuentra rodeado completamente por la zona urbana de Minatitlán, con un total de 356 020 habitantes, y que en caso de presentarse el peor de los escenarios posibles, cubriría la superficie total del municipio.

Impacto ambiental

La mayoría de los materiales que se utilizan en la fabricación de químicos y petroquímicos son inflamables y explosivos. Si bien muchos de los químicos y petroquímicos son tóxicos, algunos también son carcinogénicos. En la industria Petroquímica los riesgos potenciales de explosión son más severos, comparados, por ejemplo, con la industria de refinación, porque los compuestos son muy reactivos y las presiones que ocurren durante su manufactura y manejo son altas.

Los materiales muy tóxicos que causan lesiones inmediatas, son clasificados como un peligro para la seguridad. Otros causan efectos a largo plazo, a veces con concentraciones muy bajas. En los estudios realizados sobre la producción de químicos y su impacto ambiental, se encontró que las consideraciones de toxicidad, peligro y operatividad juegan un papel importante. Un evento que comprometa la estructura operacional de los Complejos pone en grave riesgo al medio ambiente de la zona, ya que como se ha explicado, las sustancias aquí manejadas tienen una afectación negativa considerable, tanto para la población, como para el medio ambiente, además que el manejo de la fuga de estos materiales requiere de mayor especialidad.

El 35 % de las aguas superficiales mexicanas atraviesa el territorio veracruzano, y en los ecosistemas que coexisten la zona sur específicamente son el de selva alta perennifolia con palmares, manglares y pastizales, donde se desarrolló una fauna compuesta por poblaciones de mamíferos silvestres como armadillo, ardilla, conejo, tejón; reptiles y aves tales como garzas, tordos,

palomas, grullas y golondrinas, lo cual nos habla de la gran diversidad en flora y fauna que pudiera verse afectada en caso de ocurrir un evento que implique la fuga de material de cualquiera de los Complejos Petroquímicos.

Adicionalmente, ya desde la década de los 80, se declaró oficialmente como "Zona Crítica", a la zona Coatzacoalcos-Minatitlán en el aspecto de ordenamiento ecológico y protección ambiental. Los problemas ambientales principales de la zona son la contaminación del río Coatzacoalcos y sus afluentes por grandes cantidades de desechos industriales y la mala calidad del aire que se respira; y el pantano Santa Alejandrina, el cual es afectado por las grandes cargas residuales y deforestación, y las especies de animales que lo habitan son severamente afectadas por la gran concentración de desechos tóxicos. En 2001, el pantano Santa Alejandrina fue gravemente afectado por el derrame de hidrocarburos; considerado como el más contaminado de México. Cualquier evento que involucre la fuga o derrame no controlado de las sustancias manejadas contribuiría a agravar esta situación.

Daño a la imagen pública del Estado

En cualquier situación de violencia que ocurra dentro del país, el Estado tendrá una imagen de desprestigio, mientras más graves sean las consecuencias de estos eventos (pérdidas humanas, materiales y económicas). Los actos hostiles y de terrorismo perpetrados en contra de las instituciones de gobierno, son una afrenta directa contra este, y dañan la imagen y prestigio de la administración en turno, al poner entre dicho el control de esta y su capacidad de respuesta. En el caso de las infraestructuras críticas esta situación se acentúa aún más, por el grado de interconectividad que estas representan. Un atentado en contra de la infraestructura crítica no sólo afecta a la imagen del Estado, sino que afecta también a su capacidad de respuesta y genera un ambiente de desestabilidad social y económica. El Estado no sólo pierde recursos económicos, sino que tiene que invertir nuevamente en reparar los daños materiales y tiene un largo camino en recuperar la confianza de la sociedad.

Resiliencia de la comunidad propensa

La resiliencia de la comunidad se entiende como su capacidad para responder o absorber el impacto, esta se encuentra relacionada con los factores sociales, organizacionales e institucionales de la región (Cardona, 2001), como se menciona anteriormente en este mismo Capítulo. Se mencionaba también que si bien se cuentan con las estructuras administrativas y materiales suficientes para dar respuesta a un evento, el principal problema se encuentra en el tejido

social. La pobreza en la que se encuentra sumida la sierra norte del estado de Veracruz, donde las clases más desfavorecidas son los indígenas, contrasta con ciudades altamente industrializadas como son Veracruz, Orizaba, Coatzacoalcos y Poza Rica. Sus principales ciudades son, al norte: Tuxpan y Poza Rica, al centro: Veracruz, Xalapa, Córdoba y Orizaba, y al sur: Coatzacoalcos y Minatitlán. Sin embargo existen en esta zona (Coatzacoalcos-Minatitlán) una muy marcada desigualdad social. Parte de sus pobladores emigraron de sus lugares de origen hacia esta zona en el auge de la industria petroquímica, ocupando empleos en la construcción de la infraestructura necesaria para ella. Sin embargo, una vez terminados los trabajos de construcción muchos de ellos no volvieron a sus ciudades de origen, quedándose en la zona, desprovistos del empleo que temporalmente habían tenido. Esta situación se ve reflejada en los materiales empleados en la construcción de sus viviendas por parte de la gente de menores recursos, como son: madera, lámina, palma y tejamanil, y las cuales los vuelven vulnerables ante un evento de desastre. Parte de esta fragilidad social quedo expuesta en las inundaciones ocurridas durante el año de 2010, donde quedo de manifiesto que los sectores económicamente más bajos fueron los más afectados, lo que es un claro escenario de lo que podría suceder en caso de un accidente mayor en cualquiera de los Complejos de la zona.

Lo hasta aquí descrito particulariza los problemas entorno a la seguridad física de una parte de una de las infraestructuras críticas mencionadas, la industria de petróleo y sus derivados. No se puede decir si tal o cual infraestructura es más importante, su grado de interconectividad las ha llevado a ser todas ellas piezas clave del engranaje que mantiene en movimiento la vida económica, social y política de cualquier sociedad. Hablar entonces de la seguridad de estas infraestructuras se convierte en un tema de interés desde el punto de vista de esas interconexiones. Establecer los medios de seguridad necesarios para proteger esta infraestructura, requiere estimar el riesgo desde un punto de vista multidisciplinar, no solamente el daño físico esperado, las víctimas o pérdidas económicas equivalentes, sino también factores sociales, organizacionales e institucionales relacionados con el sistema y su entorno.

Para ello es indispensable una visión holística, es decir, de una valoración integral y multidisciplinar que permita desagregar el sistema en sus componentes de diferente índole. Una concepción holística, consistente y coherente, fundamentada en los planteamientos teóricos de la complejidad, que tenga en cuenta no sólo variables técnicas y normativas, sino también variables económicas, organizacionales, sociales, políticas, culturales o de cualquier otro

tipo que puedan facilitar y orientar la toma de decisiones en este tipo de organizaciones (Infraestructuras Críticas). Un enfoque de este tipo, integral y multidisciplinar podría tener en cuenta de manera más consistente las relaciones no lineales de los parámetros del contexto y la complejidad y dinámica de los sistemas, e igualmente, contribuir a mejorar la efectividad de la gestión y a identificar y priorizar medidas factibles y eficientes para la reducción del riesgo por parte de los actores principales, fundamental para lograr una actitud no sólo preventiva, sino también proactiva ante los fenómenos peligrosos.

A continuación, la figura 1 sintetiza la problemática de los sistemas de seguridad física en las LCCI´s. Como se ha explicado, el objetivo de un SSF es el resguardo del patrimonio y/o activos estratégicos de un determinado sistema, ante las posibles amenazas (naturales o antropogénicas, las cuales se encuentran en el ambiente externo del sistema) que atentan contra su integridad. La manera lograrlo es a través de actuar directamente sobre las vulnerabilidades del sistema (físico-materiales, social-organizacionales y de motivación y actitud.). La interacción de las amenazas y las vulnerabilidades dan origen a los riesgos, de ahí que un SSF sea una forma de administrar los riegos, mismos que de no tener un control apropiado de ellos se pueden trasladar al ambiente externo (como otras infraestructuras, y sistemas sociales, ambientales y/o económicos).

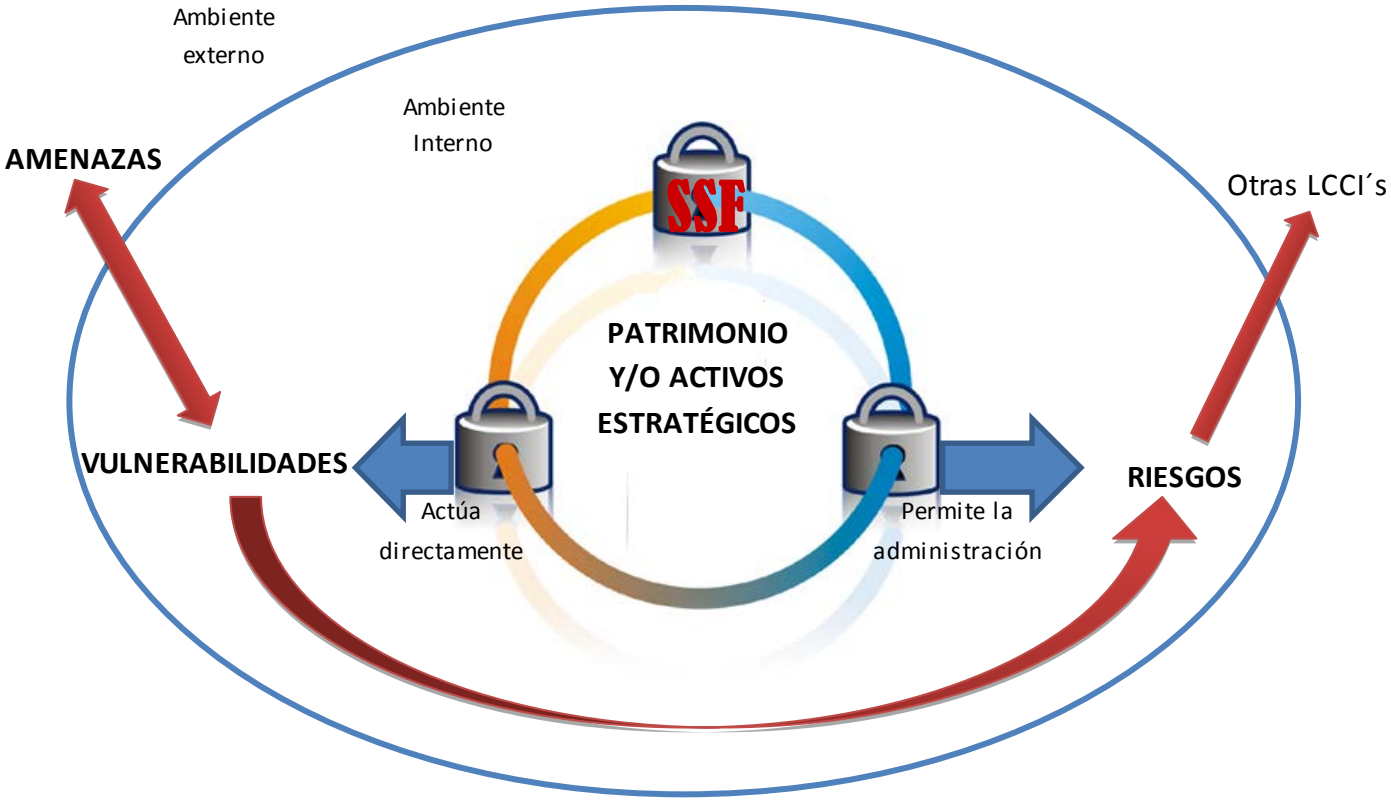

Figura 2. Problemática de los Sistemas de Seguridad Física de los LCCI
Fuente: Elaboración propia

Lo anterior nos lleva al punto de este trabajo, la necesidad de que el diseño de los sistemas de seguridad física empleados en la infraestructura crítica, deban ser establecidos dentro de un marco normativo al cual tienen alinearse, (de acuerdo con el tipo de infraestructura), a través de un enfoque holístico y un diseño adaptativo e interactivo que permita seleccionar los cursos de acción en materia de seguridad física, y de asumir las eventuales adversidades o contingencias asociados a dichas acciones, que sean congruentes con el contexto, tomen en cuenta los aspectos que sean relevantes en el sistema y cuyas características garanticen el éxito del sistema a través de crear las condiciones necesarias para poder reducir las pérdidas potenciales, aumentar la capacidad de supervivencia y mantener la continuidad operativa de la organización.

1.6 Objetivo General

Proponer la estructura de un SSF para una LCCI, en un marco de planeación normativa y adaptativa, con la finalidad de reducir la vulnerabilidad de estas

estructuras, incrementar su capacidad de supervivencia y su capacidad de resistencia, así como reducir las pérdidas potenciales asociadas a los riesgos existentes.

1.7 Justificación

Después de realizar una revisión a la literatura del tema y realizar una investigación documental, es evidente que existe un creciente interés en el tema de la seguridad de la Infraestructura Crítica, sin embargo es necesario garantizar que este tema sea abordado desde una visión holística, que contemple más aspectos que sólo los técnicos, dada la complejidad de este tipo de sistemas.

1.8 Alcance

Alinear las actividades en materia de seguridad física, con la correspondiente normatividad estipulada de acuerdo con la naturaleza de la organización a resguardar. Diseñar una estructura básica que pueda ser empleada en otras LCCI preocupadas por la seguridad física de sus instalaciones o de sus activos estratégicos.

1.9 Estrategia de Investigación

Este trabajo está basado en las experiencias profesionales del trabajo en las actividades de seguridad física. El inicio del trabajo parte de una investigación de campo sobre los niveles de seguridad de PEMEX PQ, y su grado de cumplimiento al Plan Rector. A partir de esta investigación de campo, de una investigación documental sobre los diferentes involucrados en el sistema, y de los resultados arrojados por el análisis de riesgos se comenzó la conceptualización de un SSF que fuera acorde a las necesidades de la infraestructura de estudio. Dicha conceptualización requirió de un proceso de construcción del sistema por descomposición, y de diseñar dicho sistema en un marco de planeación normativa que permitiera alinear al sistema con la normativa requerida, de planeación interactiva y adaptiva que permitieran manejar de la mejor forma la complejidad del sistema y atender a las diferentes interrelaciones y actores involucrados. EL grupo de trabajo estuvo encabezado por Profesionales Certificados en Protección (CPP por sus siglas del inglés *Certified Protection Professional),* al frente de un grupo de profesionistas con experiencia en seguridad física, así como con la colaboración del personal del propio PEMEX PQ (del departamento de vigilancia y de la GSSF de cada uno de los complejos).

Capítulo 2. Planeación adaptativa, normativa e interactiva

2.1 Planeación adaptativa

La Planeación Adaptativa sintetiza elementos de la Planeación Racional Comprensiva y del Incrementalismo Disjunto, y tiene como base conceptual el Paradigma de Sistemas Activos Adaptativos. Como escuela de planeación, sus orígenes se encuentran principalmente en los trabajos de Emery y Trist (1965), Ackoff (1981) y Ozbekhan (1977).

De acuerdo con Emery y Trist (1972), los planeadores de tendencia tradicional ponen un excesivo énfasis en la adopción de medidas que sólo sirven para adaptar un sistema a las circunstancias dadas. Como alternativa a esta "adaptación pasiva", Emery y Trist proponen un proceso de "planeación adaptativa activa" que promueve la adaptación a un estado futuro deseable. Este futuro no se espera que se pueda lograr de manera automática, sino que requiere un esfuerzo deliberado. De acuerdo con Cámpelo y González (2004), en el clima turbulento actual de la sociedad moderna, los valores son más necesarios que nunca para guiar a las personas y a las organizaciones que enfrentan un futuro incierto. Las características fundamentales delineadas por Trist involucran el siguiente conjunto de elementos.

En primer lugar, la primacía del nivel normativo en la planeación es postulada por Ozbekhan, al indicar que es imperativo hacer explícitos los valores que definen los fines, estableciendo, dentro de lo posible, las probables consecuencias en el largo plazo como resultado de cursos de acción alternativos (Cámpelo y González, 2004).

En segundo lugar, el planeamiento adaptativo implica una postura proactiva o interactiva, refiriéndose al sistema que busca cambiar el ambiente, a través de establecer un estado o futuro deseado, con el compromiso y la actuación necesarios para avanzar en esa dirección. También, la Planeación Adaptativa es vista como un proceso continuo, necesario para el aprendizaje del sistema. Ese proceso incluye la definición de un estado deseado o concepción del sistema, su implementación y evaluación. La evaluación debe contar con la participación de los actores afectados por el proceso y posibilitar la redefinición de la imagen del estado deseado, de los objetivos y de los cursos de acción. Después de la evaluación, se inicia un nuevo ciclo en el proceso, en el cual la concepción del sistema, o la definición del estado futuro deseado para el sistema, debe ser hecha a partir de una concepción holística, al involucrar la coordinación de los diversos elementos del sistema y la integración en sus diferentes niveles. La implementación sigue un patrón incremental, siendo necesario para su realización involucrar múltiples grupos de interés, a fin de dominar la resistencia al cambio de estos grupos y posibilitar el aprendizaje. En ese sentido, la Planeación Adaptativa es necesariamente un proceso participativo (Ackoff, 1981).

La Planeación Adaptativa incluye dos subconjuntos integrados por varios enfoques de planeación: el Rediseño Normativo de Sistemas y la Planeación Adaptativa no Sinóptica (Cámpelo y González, 2004). El primer conjunto incluye enfoques tales como la Planeación Interactiva (Ackoff, 2001), la Planeación Normativa (Ozbekhan, 1977) y la Metodología de Sistemas Suaves (Checkland, 1999). Por otro lado, la Planificación Adaptativa no Sinóptica incluye un conjunto de conceptos y enfoques de planificación específicos, siendo los más representativos la Planificación Basada en Interés de Chevalier, el Enfoque de la Selección Estratégica de Friend y Jessop, la Intervención Estratégica de Cohen, entre otros. En particular, para los propósitos de esta investigación, interesa destacar dos enfoques específicos del Rediseño Normativo de Sistemas: la Planeación Interactiva (Ackoff) y la Planeación Normativa (Ozbekhan). La aplicación de estos enfoques a la planeación de los sistemas de seguridad permitió la conceptualización la estructura de un SSF

bajo un marco normativo especifico, y al determinar las propiedades específicas y elementos del diseño bajo una perspectiva holística y que ayude al sistema a diseñar de forma proactiva su futuro.

2.2 Planeación Normativa

Ozbekhan comparte las ideas de Emery y Trist de orientar la planeación hacia el futuro y no hacia el presente. El presente, que enfrenta el planeador, es la que Ozbekhan llama una "problématique". Ésta es un conjunto de consecuencias generar problema, intencionales y no intencionales, de acciones anteriores. Esta problématique no puede ser descompuesta en problemas bien delimitados y por tanto no puede ser objeto de técnicas de optimización simple, el planeador debe ocuparse de diseñar las acciones. Esto tendrá un mejor efecto por un enfoque de planeación que trate con "futuros" en lugar de "hechos", y hacerlo de tal manera que el futuro imprima su configuración en el presente y no al revés (Ozbekhan, 1977)

En su teoría de planeación, Ozbekhan delimita el concepto de futuro mediante la introducción de una distinción entre los futuros "lógicos" y "deseables". Los futuros lógicos son meras extensiones y extrapolaciones del presente con los cuales los planeadores tradicionales están preocupados. Los futuros de deseados van más allá de lo inmediatamente posible, sino que son el resultado del juicio y de elección deliberada. Desear un estado futuro en particular, de cualquier sistema es un acto de elección que involucra evaluaciones, juicios y decisiones que se refieren a la consecución de los fines determinados por el hombre y la selección de los medios adecuados para conseguir tales fines. Los valores definen lo “deseable” y la actividad de planeación que lleva a las medidas adoptadas a promover o lograr lo “deseado” se denomina Planeación Normativa. Al estar basada en una visión explícita de lo deseado y las normas necesarias para lograrlo, la Planeación Normativa está a un nivel más alto que la Planeación estratégica y operacional.

La concepción de esta Planeación Normativa (interactiva) presentada por Ozbekhan deriva en los siguientes postulados:

1. La planeación es holística, en contra al incrementalismo, un enfoque para la solución de problemas interrelacionados, no segregables como un conjunto de problemas complejos.

2. En planeación, lo que significa solución es el "diseño" de la representación de nuevas situaciones, un resultado el cual tiene más valor que la situación presente.
3. Planeación siempre implica "experimentación" en el diseño de los resultados y en la selección de los medios para lograr tales resultados.
4. Planeación es una toma de decisiones, por lo tanto un proceso voluntarista
5. Planeación está encaminada a la formulación de "políticas"

Conjuntamente a los postulados establecidos por Ozbekhan (1977), Delgado y Serna (1977) señalan que la planeación normativa sostiene que el ser humano, elemento principal de las organizaciones, es capaz de diseñar un futuro para sí mismo, y no sólo se adapta a su medio ambiente. Esta actitud hacia el futuro, es lo que da importancia y actualidad a la planeación normativa, y proponen las siguientes características (Rodríguez, 1998):

1. En la planeación normativa se reconoce que los problemas que enfrenta una organización o sistema no se presentan aisladamente, sino que se interrelacionan con otros, que por lo regular no son percibidos fácilmente, pero que son tanto o más importantes que aquéllos que son visibles. Se enfrenta entonces a situaciones problemáticas, o bien, a sistemas de problemas, cuya complejidad hace necesario adoptar una visión sistémica para su atención.

Al Confrontar lo anterior con el primer postulado de Ozbekhan (1977), se entiende que la planeación normativa debe ser ***integral***, es decir, que ha de considerar todos los componentes de la organización planeada, así como sus interrelaciones. En el caso de un SSF resulta primordial este entendimiento, no sólo para la elaboración de alternativas que integren a los elementos físicos y administrativos bajo un mismo fin común, sino que contemplen su interacción contextual (medio ambiente) cuya componente social y ambiental es de gran relevancia.

2. En este proceso de planeación, toman parte sistemas de participantes y no participantes aislados e independientes. Ello significa que se deben tomar en cuenta las opiniones y valores de todos los involucrados o "stakeholders", que son aquéllos que resultan afectados por las acciones que se derivan de la planeación.

Visto desde este punto, la planeación normativa es también ***participativa***, lo que implica que la toma de decisiones, y en general todo el proceso de planeación, sea realizado *por* la organización y no *para* ella.

La participación, extendida a todos los ámbitos de la estructura organizacional de un sistema que se planea a sí mismo, produce resultados como:

- Facilidad para la implantación de las decisiones, debido a que quienes deben ejecutarlas, son también quienes participan en su diseño.
- Se fomenta la creatividad de los miembros del sistema, lo que genera tal información, que resulta enriquecida la visión global de la situación bajo estudio.
- Facilita el aprendizaje y el desarrollo de los participantes, lo que los hace más aptos como individuos y como grupo, para adaptarse activamente a su medio ambiente.

En el Capítulo anterior, la planeación de recursos hace énfasis a este punto, ya que el diseño de las medidas entorno a la seguridad debe estar aprobado conjuntamente por la parte administrativa y la operativa del sistema. Es de señalar que las propiedades específicas de esquema propuesto en este trabajo, se tomó directamente de las necesidades de la organización a través de entrevistas con los responsables y mediante juntas de retroalimentación en las que se exponían las propuestas de medidas a recomendar, es decir se trabajó bajo un esquema de participativo el cual pudiera garantizar las necesidades de las partes administrativa y técnica.

3. En la planeación normativa se reconoce la naturaleza dinámica del entorno organizacional, y el nivel de incertidumbre de su comportamiento. El objetivo debe ser convivir con el entorno de manera aceptablemente armónica, al consolidar no sólo oportunidades de supervivencia sino también de desarrollo. Por ello, la actividad planeadora tendrá que ser ***continua***. Es decir, debe considerar la permanente modificación de los planes para adecuarlos a la problemática del entorno, que está en constante transformación. En la planeación normativa se da más importancia al proceso de planeación y menos a su "producto", los planes, que requieren una continua revisión.

Lo anterior, es reforzado con lo propuesto por Ozbekhan en su segundo postulado, que en planeación, lo que significa solución es el “diseño” de la representación de nuevas situaciones, ya que es este proceso de continuo es el

que permite adaptarse al sistema de acuerdo con los cambios que manifieste su ambiente. Este el proceso de este diseño lo que genera más valor que el producto final, por el nivel de experiencia y participación que de este se derivan.

4. Este enfoque de planeación abre la posibilidad para diseñar futuros diferentes, y no sólo prepararse para aquél al que las tendencias apuntan. Así, los involucrados en el proceso de planeación tienen la oportunidad de desarrollar su creatividad, para que, mediante la participación, cooperen en la generación de una imagen compartida de su futuro deseado. A la imagen de este futuro se le denomina futuro ideal, que en esencia es inalcanzable, pero asintóticamente aproximable.

El futuro ideal es un reflejo de los valores de los individuos como miembros del sistema, la integración de éstos, conforma el conjunto de valores que posee el sistema. Es precisamente la inclusión de dichos valores, lo que hace que esta forma de planeación sea ***normativa***. Según Ozbekhan, la planeación normativa consiste en definir ideales, y a partir de esto derivar objetivos mediante el diseño de diferentes futuros deseados. Los valores son, por lo tanto, la guía de conducta que apoyará el "día a día", para trabajar en el cumplimiento de lo planeado.

En este caso de estudio, dichos valores (para la infraestructura petrolera) están plasmados en el Plan Rector de Seguridad física para Petróleos Mexicanos y Organismos Subsidiarios. En este documento, se definen los objetivos estratégicos, líneas estratégicas, líneas de acción y actividades sustantivas, que orientaran la elaboración y aplicación de los programas que en esta materia se establezcan al interior de Petróleos Mexicanos y Organismos Subsidiarios y, al exterior, en coordinación con otras dependencias con responsabilidades en la Seguridad Nacional y Pública, en los términos que conforme a la ley aplicable proceda. En otros palabras marca el ***deber ser,*** para las acciones que se tomen en materia de Seguridad física en forma de programas, es el marco normativo al que se deberán alinear estas acciones.

La continuidad en el proceso de planeación, exigida por la naturaleza cambiante de los entornos, entraña en sí misma la habilidad del sistema para detectar inadecuaciones derivadas de las decisiones ya acordadas. Esta habilidad depende de la capacidad de aprendizaje y adaptación de dicho sistema. Ello conduce al hecho de que los planeadores han de "aprender a

aprender", a través del continuo rediseño de decisiones y planes, llevado a cabo de forma activa y con el objetivo de concretar nuevas oportunidades. Por ello, la planeación normativa también es ***adaptativa y de aprendizaje***.

Ahora bien, anteriormente se mencionó que el planeamiento adaptativo implica una postura pro-activa o interactiva (tema que expuso Ackoff y que se detalla más adelante dentro de este mismo Capítulo). Ozbekhan por su parte, plantea las fases de la planeación, como una planeación interactiva normativa (lo cual le da esta cualidad adaptativa), y cuyas fases se explican a continuación.

Fase 1: Proyección de Referencia

Menciona Ozbekhan, que la proyección de referencia es un intento de estructurar un conjunto de problemas confusos, traslapados, en lo que llama "problématique" , una especie de modelo capaz de sugerir vínculos causales entre estos problemas, que permite tener una percepción de la situación actual.

Para construir ese modelo es necesario para visualizar la problématique en todas sus dimensiones pertinentes, es decir, como pertenecientes a un sistema jerarquizado. Este último puede ser concebido como un conjunto de tres ambientes concéntricos: el interno, transaccional y el contextual. Estos ambientes deberán ser delimitados de acuerdo con el grado de "intersensibilidad" y la sinergia entre los eventos generados por cada uno y como lo trasmiten hacia todo el sistema jerarquizado, para posteriormente identificar y nombrar sus principales componentes funcionales y estructurales.

Lo anterior permite un mapeo del sistema jerarquizado, para que de esta forma las interacciones más intensas entre los elementos puedan ser encontradas y así sean investigadas con cierta profundidad. Ozbekhan propone un análisis de disonancia para estudiar el patrón de las interacciones existentes, para posteriormente proponer imágenes del futuro lógico y/o exploración de escenarios de los cursos de acción posibles.

Fase 2. Plan normativo

Una vez que la estructura de la problemática actual se ha completado (problématique), se hace necesario el diseño de los futuros estados del sistema, los cuales son considerados buenos, por lo tanto, "deseable". El diseño de estos Estados Futuros requiere, en primer lugar, que las decisiones concertadas sean definidas como lo que es deseable, y en segundo lugar, que las acciones concertadas sean definidas para realizar dichas decisiones. Es en la fase de

plan normativo que se hace referencia a la cuestión del futuro deseable. Esto se hace mediante la visualización de dos tipos de estados futuros para el sistema: (i) los "fines" que los actores son capaces de concebir en forma de ideales a los que se puede aproximar constantemente, pero nunca se logran del todo, y 'objetivos' (ii) que son los estados más valorados futuro y que pueden derivar de tales fines, y que al mismo tiempo permanecen más allá del horizonte de la planeación.

La identificación de los fines, da pie a establecer los objetivos, los cuales parten del diseño de "futuros alternativos" y que para tal diseño se emplea el escenario normativo. El escenario normativo propone un estado futuro del sistema de acuerdo con las relaciones contextuales asumidas que se han identificado en el proceso de fijación de los extremos (estado actual, estado deseado o valores). Entonces el sistema, es rediseñado (cambiado, alterado y manipulado) de manera que sea capaz de acercarse al máximo sus «fines», y reducir al mínimo o, posiblemente, eliminar, las disfunciones en su situación actual (brecha). Por lo tanto, estos escenarios se construyen en torno a un conjunto de relaciones variables que asumen configuraciones futuras de los ambientes transaccional y contextual y la imagen actual idealizada de un ambiente interno disfuncional. Son "normativos" en el sentido de que, si bien los ambientes exteriores están basadas en hipótesis o supuestos, la forma y el comportamiento del entorno interno es prescrita (deber ser).

Fase 3: Plan estratégico

Conocido como los medios de la planeación, identificación y organización de los medios necesarios para lograr los objetivos (medios, metas, políticas, programas). Las metas se definen como los resultados deseados de la acción posible dentro del horizonte temporal de la planeación. Se derivan de los objetivos. Las políticas (nuevas políticas) se extraen de los objetivos y los programas son la elaboración de estas políticas en actividades específicas, organizadas y programadas. El cálculo de los recursos necesarios será el siguiente paso en esta fase, con la prioridad de buscar dentro del programa las metas más críticas y significantes.

Fase 4: Plan de organización e implementación

La fase final propone los pasos para llegar al estado deseado, a través de un Plan organizacional y de implementación, mediante el cual se realizará la asignación de recursos, reorganización de las acciones y el rediseño de la nueva institución.

2.3 Planeación interactiva

Ackoff hace énfasis en la consideración del futuro como punto de partida para la planeación y la acción. Llama a su práctica de planeación como Planeación Interactiva para distinguirla de las formas tradicionales de planeación, que se clasifica "inactiva" (la no planeación), "reactiva" (a corto plazo e identificación de deficiencias para eliminarlas una a una) y "proactiva" (orientada a la predicción y preparación, planea para el futuro y no el futuro). Ackoff desarrolla el concepto de la problématique de Ozbekhan como "mess" (problemática) como una serie de problemas superpuestos, sociales y organizacionales frente a un sistema social. Al darse cuenta de que los problemas en una "mess" o problemática no se puede resolver por separado, el planeador interactivo pretende rediseñar todo el sistema de manera holística a fin de lograr un estado futuro deseable en el que estos problemas no aparezcan en el primer lugar. Dicho futuro debe ser diseñado y producido por las personas que posean una participación en el desempeño del sistema (empleados, propietarios, etc.), es decir, sus *stakeholders* o grupos de interés.

La Planeación se basa en la creencia de que el futuro de una organización depende de qué hace esta entre el ahora y el entonces, y sobre qué se hace. Consiste en el diseño de un presente deseable y la selección o invención de formas de aproximarse a éste tanto como sea posible. Crea el futuro a partir de cerrar la brecha entre dónde se está en algún momento en el tiempo y dónde se quiere estar.

La metodología de la Planeación Interactiva tiene dos partes: **idealización y realización**. Estas partes se dividen en seis fases interrelacionadas: (1) formulación de la problemática (mess), (2) planeación de fines, (3) planeación de medios, (4) planeación de recursos, y (5) diseño de la implantación, y (6) diseño de controles.

En la formulación de la problemática (mess) se mapea la situación actual y se utilizan extrapolaciones de las tendencias actuales para dar una imagen (un escenario de referencia, similar a los futuros lógicos de Ozbekhan, (1977)) del futuro que el sistema tendrá si no se lleva a cabo la planeación. La formulación de la problemática, tiene por objeto alertar a las partes interesadas sobre la necesidad de una acción radical.

A continuación sigue el proceso de "idealización", durante el cual los interesados (stakeholders) diseñan el sistema que más les gustaría tener en

este momento, si pudieran. Este diseño de un mejor sistema que se llama Diseño Idealizado, el cual no es una utopía ideal, pero si el mejor diseño que las partes interesadas pueden presentar en el momento. El Diseño Idealizado es un todo sistémico en el que todas las piezas están diseñadas para encajar, y que debe ser capaz de aprender y adaptarse.

De acuerdo con Sánchez Lara (2007), las restricciones en el diseño idealizado que requiere cumplir tres condiciones: factibilidad técnica (el diseño no debe incorporar ninguna tecnología que actualmente sea desconocida o inaplicable, pero puede incluir innovaciones tecnológicas en prototipo, siempre y cuando sean factibles); viabilidad operativa (el sistema diseñado debe ser capaz de sobrevivir una vez que esté en funcionamiento, es decir, poder operar en el ambiente actual del sistema) y flexibilidad (el sistema diseñado debe ser capaz de aprender y adaptarse). El procedimiento del Diseño Idealizado consta de tres grandes bloques o fases: formulación de la misión (1), especificación de las propiedades deseadas (2) y rediseño o diseño idealizado (3).

En la primera etapa, se deberá formular la problemática, cuyo objetivo es determinar qué pasaría con la organización si su comportamiento continuara; si fuera incapaz de adaptarse. Esto implica elaborar:

1. Un análisis de sistemas, el cual describa detalladamente cómo opera el sistema actualmente,
2. Un análisis de obstrucciones, que permita identificar las características y propiedades de la organización que obstruyen su progreso,
3. Proyecciones de referencia, proyectando aspectos del futuro de la organización a partir de asumir (1) que no se dan cambios en sus planes, políticas, programas, etc. y (2) el ambiente futuro que se espera hoy,
4. Escenarios de referencia, a través de describir cómo y por qué la organización se destruiría si las suposiciones fueran ciertas. El escenario debe ser una síntesis de lo elaborado anteriormente.

Esta misma etapa implica la formulación de la Misión, la cual es entendida como la razón de existencia y aspiraciones del sistema. Es la manera en que el sistema incide en su ambiente para llevar a cabo en la práctica su visión. Así como las formas de lograr alcanzar lo que se desea ser y el propósito que pretende poner en acción a toda la organización.

La misión debe (a) identificar las maneras de que la organización sea efectiva y única, (2) unificar a los stakeholders en el propósito, (3) hacer la diferencia en

lo que la organización hace e (4) impulsar el progreso hacia los objetivos medibles de la organización.

La segunda etapa, especificación de las propiedades deseadas, son declaraciones acerca de las propiedades que desean tenga el sistema idealizado. Deben estar ligadas a la misión del sistema y al resultado del análisis de la problemática. Los aspectos a cubrir con las especificaciones son materia de elección.

Finalmente, en la etapa 3, diseño del sistema, deben convertirse las especificaciones en acciones o actividades y especificarse cómo obtener cada propiedad, que serán los elementos de diseño (qué actividades llevar a cabo). Este diseño es un proceso acumulativo. Empieza con un bosquejo y debe terminar con un máximo de detalle. Completado el diseño de las propiedades se recomienda verificar su factibilidad técnica. Por último, el diseño debe ensamblarse e integrarse en un cuadro global y coordinado, una especie de escenario del todo, al cual debe verificársele su viabilidad operativa (Sánchez-Lara).

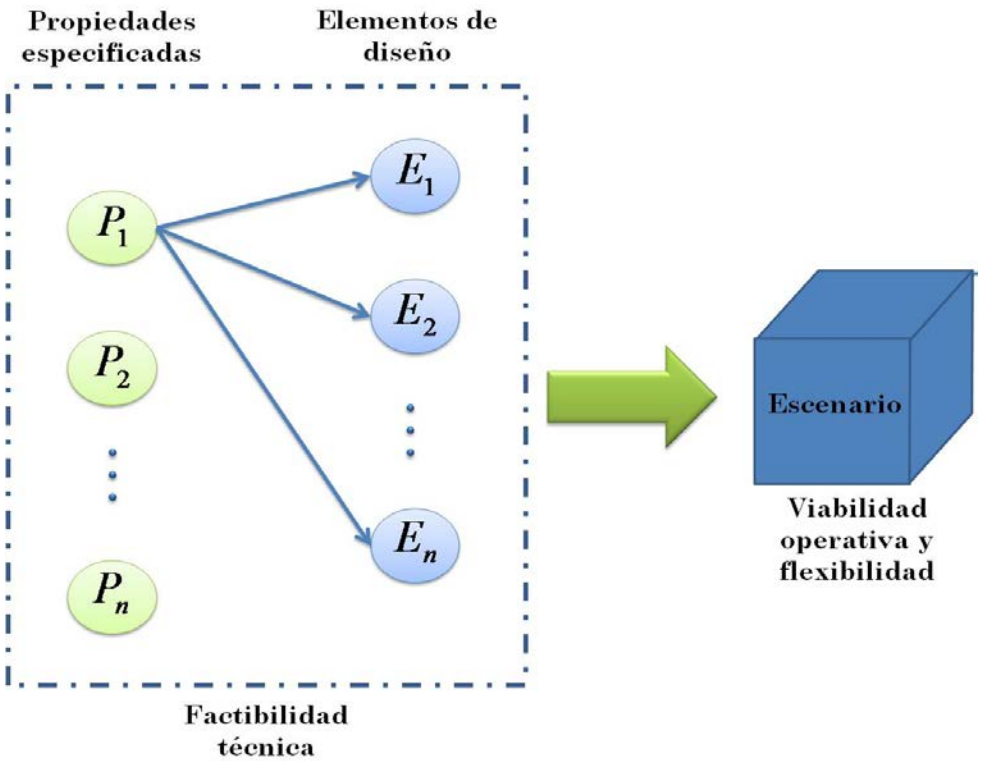

Figura 3. Etapa de diseño del sistema del Diseño Idealizado
Fuente: Sánchez Lara (2007)

En resumen, es evidente que los enfoques de la planeación normativa de Emery y Trist, Ozbekhan y Ackoff afirman enérgicamente que la acción de cambio debe partir de un futuro deseable imaginario, en lugar de partir de un presente fragmentado y problemático. Los enfoques de la planeación normativa alientan a las partes interesadas de un sistema a participar libremente en la creación de estados más deseables del sistema, a través de motivar y movilizar a los interesados a tomar medidas radicales para el cambio.

Como se indica en el inicio de este Capítulo, para lograr el objetivo planteado, se emplea un Rediseño Normativo del Sistema, a partir de tomar de Ozbekhan su tercera fase, Plan estratégico, a partir de extraer del Plan Rector de Petróleos Mexicanos y Organismos Subsidiarios, objetivos generales y específicos, así como líneas estratégicas, planteadas dentro de este documento como el futuro deseado de los sistemas de seguridad en las instalaciones de Petróleos Mexicanos y subsidiarias. Lo anterior en forma de un programa (diseño de la estructura de dicho programa) que lleve a las políticas marcadas en el Plan Rector en actividades específicas, organizadas y programadas. Así como los recursos necesarios para lograrlos.

Del Diseño Idealizado propuesto por Ackoff (2001), en el estudio se utiliza para poder convertir las especificaciones que marca el Plan Rector en acciones o actividades, con un bosquejo de la estructura que es sistema deberá tener. Con lo anterior, se garantiza que el diseño tendrá un enfoque holístico, que tome en cuenta a todas las partes del sistema, pertenecientes los ambientes internos, transaccionales y externos del sistema. Además de que el producto generado no pretende resolver los problemas de seguridad a corto plazo, sino ser capaz de adaptarse a las necesidades del sistema, y perdurar en el mediano y largo plazo.

De ambos autores, la formulación de la problemática (mess o problématique), permitió entender la instalación (sistema u objeto de estudio), definir los riesgos a partir de definir las amenazas y vulnerabilidades e identificar los activos estratégicos o blancos. El escenario de referencia o futuro lógico, esta dado por una análisis de riesgos, mientras que las propiedades deseadas o futuro deseado será extraído de lo contenido dentro del Plan Rector de Petróleos Mexicanos y Organismos subsidiarios.

2.4 Proceso de construcción del sistema por descomposición

Gelman y Negroe (1981), señalan que el enfoque sistémico se desarrolla a través de dos procedimientos de construcción de sistemas: por composición y descomposición; y es este el marco conceptual de estudio y que sirve como herramienta metodológica para conceptualizar una estructura general del proceso de planeación. Este trabajo busca precisamente conceptualizar una estructura general de un SSF para una llamada "infraestructura crítica", a través de un proceso de planeación, que por sus características y necesidades debe ser normativa, interactiva y adaptativa.

Para lograr dicha conceptualización se partió de la construcción de este sistema a partir del proceso de construcción por descomposición planteado por Gelman y Negroe. En este proceso, se parte del sistema hacia sus componentes, y éste basado en la descomposición funcional, que consiste en desmembrar un sistema en subsistemas, cuyas funciones y propiedades aseguren las del sistema en su conjunto, mediante una organización adecuada.

Este proceso se realiza al tomar en cuenta la estructura externa e interna del sistema en consideración. La primera estructura, se establece por medio del papel que juega el sistema en su suprasistema al definir los objetivos y funciones totales y determinar otros sistemas al mismo nivel. La estructura interna, en particular su estructura funcional, se obtiene al considerar un sistema como un agregado hipotético de subsistemas interconectados, de tal forma que garanticen su funcionamiento.

El concepto de Planeación desarrollado por Gelman y Negroe (1982), reconoce la importancia de la toma de decisiones en el proceso de conducción, como una de las funciones básicas de los organismos de la administración pública y privada. Este proceso de conducción consiste en un proceso de cambio controlado del objeto conducido, según cierto objetivo, a través de actividades que lo garanticen, y sirve para seleccionar y realizar la trayectoria de cambio adecuada.

Finalmente, resulta evidente que los actuales sistemas de seguridad física contemplan acciones de prevención, disuasión, evaluación y reacción de forma desagregada, que no aprovechan ni comparten sus recursos de forma apropiada, y con un énfasis en la parte técnica-económica. La complejidad de las grandes infraestructuras criticas requiere de una visión integral y multidisciplinar que permita establecer un sistema que tenga en cuenta no sólo

variables técnicas y normativas, sino también variables económicas, organizacionales, sociales, políticas, o de cualquier otro tipo, con un enfoque integral, e incluyente de las relaciones con el contexto, y que permitan contribuir a mejorar la efectividad de la gestión e identificar y priorizar medidas factibles y eficientes para la reducción del riesgo en este tipo de infraestructuras; dentro de un marco normativo, que haga explícito los fines que este sistema persigue y con un diseño adaptativo e interactivo que permita un postura proactiva en busca de generar las condiciones que contribuyan coadyuvar a las medidas y acciones en materia de seguridad que fortalezcan la capacidad de supervivencia de la organización y ayuden a reducir las pérdidas potenciales.

Capítulo 3 Rediseño del sistema de seguridad física para una LCCI

En este Capítulo, como ya se ha explicado, se emplearon algunos de los conceptos de Planeación Normativa de Ozbekhan, así como de la Planeación Interactiva y Diseño Idealizado de Ackoff, con la finalidad de rediseñar el SSF del objeto de estudio, a través de estructurar las actividades en una propuesta de estructura de un sistema de seguridad física. De igual manera, se tomó como apoyo la estructura sugerida Lynn García (2008), del proceso para diseño y evaluación de un sistema de control, que consta de tres fases: Determinar objetivos, diseñar y analizar el diseño.

3.1 Entendimiento de Sistema de Seguridad Física desde la planeación normativa e interactiva

Tanto Ozbekhan (1977) como Ackoff (2001) proponen establecer la problemática del sistema, la cual permitió tener un entendimiento de la situación actual de este. Esto a través de mapear los vínculos causales entre este conjunto de problemas, en sus tres contextos o ambientes (interno, transaccional y externo, Ozbekhan), además de la descripción detallada de cómo opera el sistema actualmente (Ackoff, 2001).

Ambiente interno

La salvaguarda de los activos estratégicos es el principal motivo y razón de ser de los sistemas de seguridad. Estos activos estratégicos pueden ir desde equipo, instalaciones, información, material, etc. ¿Pero de qué se resguarda a estos activos? Necesariamente, la conformación de un SSF debe partir de la identificación de los riesgos presentes en la organización, y de la identificación de las amenazas (aquello de lo cual se pretende proteger a la organización) y las vulnerabilidades de esta. En el Capítulo 1 estos tres conceptos: riesgo, amenaza y vulnerabilidad, son definidos con cierto detalle, y se hace mención a que una forma de manejar el riesgo es a través de operar sobre la vulnerabilidad (entendiendo amenaza como un factor de riesgo externo del elemento o grupo de elementos expuestos y sobre el cual no es del todo posible operar sobre ella). Es alrededor de estos tres conceptos que se comienza a estructurar el SSF, sus elementos y las interconexiones entre estos, es decir, todos aquellos involucrados de alguna u otra manera en las amenazas o vulnerabilidades de la organización. A partir de lo anterior podemos comenzar a establecer el ambiente interno de la organización.

Anteriormente, en el Capítulo 1 se definió como SSF, al conjunto de principios aplicados a un adecuado sistema de protección. Estos principios son una combinación de elementos de gestión, físico-tecnológicos y humanos. Sin embargo el elemento de gestión, generalmente la seguridad interna de la organización, debe ser quien coordine las actividades en materia de seguridad física con otros grupos involucrados en la seguridad de acuerdo ámbito de seguridad que le confiera.

En las LCCI, la gestión de los sistemas de seguridad física están encargados de la protección de los activos estratégicos de la organización, a través de una figura de gestión de este sistema, y en coordinación con otros grupos de interés para el sistema (protección civil, seguridad industrial, etc.), estructurados bajo una cadena de mando, para poder llevar a cabo las operaciones del sistema de seguridad: aplicación de procedimientos, monitoreo, recorridos, inspecciones, detenciones, labores de investigación, atención a emergencias, etc., y es responsable de llevar a cabo algunas de estas acciones en coordinación con las figuras de seguridad física internas y, de ser necesario, con el personal de seguridad externa, por ejemplo personal de una partida militar de la SEDENA, o fuerzas del orden público locales. Los problemas encontrados en este nivel o ambiento interno, tienen que ver de forma general con un alineación parcial al marco normativo, en cuestiones como equipo (carencia u obsolescencia de este),

falta de procedimientos necesarios, o problemas en la coordinación de las actividades.

Entorno transaccional

El entorno transaccional dentro de una organización está relacionado con el intercambio hacia su exterior, en el cual existe un nivel diferente de intercambio con su exterior entre las diferentes organizaciones. Este intercambio puede darse con proveedores de la organización, otras organizaciones o competidores, la población civil o comunidad aledaña y medio ambiente. En el caso de las LCCI, el ambiente transacción es quizá el más complejo. Las infraestructuras críticas como se menciona en el Capítulo 1, son una red distribuida de procesos repartidos e independientes que trabajan en colaboración y sinérgicamente para producir y distribuir un servicio esencial, y es esta característica la que complica su entorno transaccional al diversificarlo ampliamente. Como se mencionaba, las LCCI proporcionan generalmente un tipo de servicio o producto que resulta esencial para otras organizaciones o sistemas. El caso del sistema de Generación y Trasmisión de Energía Eléctrica es un claro ejemplo. Como LCCI, es vital para prácticamente cualquier otro sistema en cuanto al producto que entrega, la industria en general requiere energía eléctrica para elaborar sus productos, la población civil, los servicios para las zonas de asentamientos humanos (semáforos, alumbrado público, distribución de agua potable, bombeo de aguas residuales, etc.), servicios financieros, de transporte y un largo etc. Pero su relación de intercambio no para ahí, la propia generación y transmisión implica un intercambio con su entorno. La generación de energía genera empleos, lo mismo que un impacto ambiental, y la construcción de esta infraestructura impacta en varios niveles a la zona donde se establece. Lo mismo que la transmisión, tan sólo el derecho de vía de la red de transmisión de energía tiene un impacto transactivo muy significativo. La industria Petroquímica no es la excepción, sus relaciones de transacción no sólo van con la industria que ocupa la materia prima que esta elabora, también es motor económico de la zona, detonador de crecimiento urbano en su región y fuente de un impacto ambiental considerable.

Ambiente externo

En materia de seguridad física en las organizaciones, el ambiente externo está relacionado con las amenazas, que como ya se indicó es un factor de riesgo externo del elemento o grupo de elementos expuestos. Existen diversas formas en las que podemos suscribir los tipos de amenazas. Una clasificación de estas

puede ser de acuerdo con su origen: amenazas naturales y amenazas antrópicas (Cardona, 2001).

Las amenazas de orden natural (fenómenos geodinámicos, hidrológicos, atmosféricos y bilógicos), competen más a protección civil y seguridad industrial, que a la Seguridad física. Las amenazas antrópicas se pueden clasificar de diversas formas. Una de las muchas formas de clasificar los fenómenos o sucesos de origen antrópico que pueden significar o generar amenaza puede ser la siguiente, según su clase: (a) *Sucesos tecnológicos:* eventos relacionados con fallos de sistemas por descuido, falta de mantenimiento, errores de operación, fatiga de materiales o mal funcionamiento mecánico; (b) *Sucesos contaminantes:* relacionados con la acción de agentes tóxicos o peligrosos en términos bióticos para el ser humano y el medio ambiente; y (c) *Sucesos antropogénicos y conflictos:* También se pueden clasificar sucesos que pueden ser provocados accidental o intencionalmente por el ser humano. De estos, la Seguridad física está enfocada primordialmente a los sucesos causados de manera intencional por el ser humano, mientras que el resto son materia de la seguridad industrial y/o protección civil, no obstante se debe tener una coordinación entre dichas partes para atender las situaciones de amenaza.

El riesgo aumenta de acuerdo con los objetivos de dichas amenazas, y las pérdidas potenciales asociadas pueden afectar tan sólo a la organización (a nivel humano, material, económico e imagen), llegar a grados de afectación al área circundante (población civil y medio ambiente), o incluso alcanzar repercusiones que afecten a la sociedad en general y el gobierno (pérdidas económicas, desestabilización social y financiera, costos políticos,). En este sentido, las amenazas definen a los elementos que conforman al ambiente externo. De forma general, las amenazas antrópicas pueden ir desde competidores (en la industria), crimen organizado, delincuencia, vandalismo, etc., además de tener que confrontar a toda la demás gama de amenazas ya explicada.

De acuerdo con el riesgo, el ambiento externo estará compuesto por aquellas figuras que representan una amenaza (delincuentes, crimen organizado, grupos subversivos, competidores), los encargados del ámbito de seguridad (en alguno o todos sus niveles), y los posibles afectados externos (población circunvecina, medio ambiente, etc.). El Capítulo 1 da un detalle de diversas amenazas (antrópicas y naturales) que presenta la zona sur del estado de Veracruz, (lugar donde se encuentra la zona petroquímica más importante del país), y que da un

panorama de los grupos involucrados. Como se señala en ese mismo Capítulo, el ámbito de seguridad (responsabilidad en la seguridad) estará de acuerdo con el nivel de riesgo. Así, según los riesgos que enfrentan las LCCI, la procuración de seguridad llega a nivel a federal, además de existir una coordinación con protección civil de la región en la que se ubique.

Análisis de obstrucciones

El siguiente paso es realizar un análisis de las obstrucciones (Ackoff, 2001), para identificar las características y propiedades de la organización que obstruyen su progreso.

Una de las características que se encuentran de manera general en las organizaciones es la resistencia al cambio de los actuales esquemas de seguridad. El rediseño del sistema implica la adopción de nuevas tecnologías y nuevos procedimientos, y en las organizaciones, sobre todo públicas, existe una resistencia a la adopción de nuevos esquemas y tecnologías. Una manera de motivar al cambio es precisamente por medio de la alineación a un marco normativo con una correspondiente evaluación de nivel de cumplimiento de este.

Otra de las obstrucciones que se presenta en materia de seguridad física en las organizaciones, es que el gasto realizado en medidas de este rubro se considera desde cierta perspectiva, como "un gasto que no se ve". Esto se refiere a que el gasto que representa un SSF (o cualquiera de sus elementos) no es percibido como una inversión, directamente no representa un beneficio económico a la organización o no contribuye a agregar valor utilitario (en la mayoría de los casos). Las medidas en torno a seguridad física son una forma de reducir el riesgo, de reducir el potencial de pérdidas de un evento que se ubica en un tiempo futuro, relacionado con la posibilidad y que no ha sucedió o puede no suceder. Esto lo convierte en un gasto que no genera valor, pero que puede ser justificado para la organización como una forma de aumentar su capacidad de supervivencia, y como parte de las medidas de alineación a un esquema normativo.

Una obstrucción más que se presenta en algunas organizaciones en general (y no sólo en las LCCI), es encontrarse en una posición optimista-pesimista. Si bien los análisis de riesgos tienen como finalidad conocer los riesgos existentes (en función de las amenazas y vulnerabilidades), valorarlos y finalmente proponer las medidas para gestionarlos, asumiéndolos o no y en qué grado, la

falta de una cultura del riesgo, (entendida como el comportamiento que incluye conocimientos, creencias, leyes, costumbres y demás capacidades y hábitos de quien requiere responder asertivamente a las situaciones de peligro que enfrenta), dentro de la organización junto con una posición optimista ante el mismo, del tipo "eso no me va a ocurrir a mí", impide enfrentarse ante ellos. Esta visión optimista generalmente es reforzada con una "limitada" visión de las potenciales amenazas a las que puede hacer frente la organización, generadas (principalmente) de una falta de información o de información parcial, o de plantear las soluciones de acuerdo con las capacidades propias y no de quienes representan la amenaza.

Otro obstáculo, que de igual forma se presenta tanto el sujeto de estudio como en una generalidad de organizaciones, es el entendimiento de que la seguridad física implica un esfuerzo conjunto y coordinado, y no exclusivo del área de seguridad. En este sentido las medidas que se toman en torno a seguridad física pueden "incomodar" al resto de la organización, sin embargo es necesaria la comprensión y participación de todos en estas medidas a fin de reducir los riesgos que enfrenta la organización. Esta situación ha tenido como resultado que algunas de las medidas y acciones que se han implantadas anteriormente en las organizaciones en materia de seguridad, hayan fracasado, sean insuficientes, o sean ejecutadas de manera parcial, situación que implica una vulnerabilidad y por ende sea reflejada en el riesgo.

En algunos otros casos, dentro de las organizaciones existe también una falta de conocimiento cabal de las responsabilidades de los participantes y del papel que cada uno juega en el sistema. Esta situación deriva de no tener una clara definición del papel de cada una de las partes, de cuál es su papel en la seguridad física, lo que resulta crucial para poder establecer una coordinación para llevar a cabo las labores en este rubro.

El rebase tecnológico o la falta de mantenimiento también representa un obstáculo. Algunos de los elementos pertenecientes a los sistemas de seguridad pueden presentar vulnerabilidades para la organización producto de un rebase tecnológico (tecnología en desuso), o que por falta de mantenimiento presente problemas en su operación.

Proyecciones y escenarios de referencia

Por separado, amenazas y vulnerabilidades forman parte del estado actual de la organización (en este caso en términos seguridad física). Al realizar esta

"convolución", es decir identificar y evaluar los riesgos, se realiza una proyección lógica de ese estado. Los riesgos identificados constituyen las situaciones que se presentarán, (en forma de pérdidas ya sea humanas, materiales, ecológicas, materiales y/o económicas), de continuar ambas variables en su estado actual. Estas proyecciones señalan lo que puede ocurrirle a la organización de continuar operando bajo estas condiciones (de amenazas y vulnerabilidades). Sin embargo, no se puede identificar en qué momento del futuro de la organización se presentara esta proyección lógica, pero sí se tiene conciencia de que esta situación, (riesgos identificados) puede presentarse en el futuro de la organización (próximo o no). El motivo de esta incertidumbre, deriva del mutuo condicionamiento de la amenaza y de la vulnerabilidad, entendida esta como la predisposición o susceptibilidad de la organización a ser afectada o sufrir daños en caso de presentarse un fenómeno desestabilizador (natural o antropogénico), dando como resultado que el riesgo sea algo que parece irreal e inasible, ubicado en un tiempo futuro como consecuencia de estar siempre relacionado con azar, con posibilidades, con algo que aún no ha sucedido y que puede no suceder. Como ya se mencionó las proyecciones deben presentar las pérdidas potenciales resultado del estado de vulnerabilidad en concordancia con las amenazas encontradas organización (riesgo), y entregados en forma de un análisis de riesgos, el cual debe describir con cierto nivel de detalle, el grado de pérdidas para cada activo estratégico de la organización.

En el caso de la zona sur de Veracruz, ya en el Capítulo 1 se hace mención al potencial de pérdidas de estas proyecciones. Situaciones que van desde un impacto ambiental (en un ecosistema con una gran riqueza y diversidad en flora y fauna como el de esta zona), provocado por la fuga de sustancia químicas altamente peligrosas no sólo para el ambiente, sino también para trabajadores y población circunvecina. Pérdidas humanas en un radio de afectación que va desde los 8 metros hasta los 7 kilómetros (por cada complejo de la zona sur de Veracruz), en regiones que pueden ir de es poco menos de una decena de trabajadores, hasta regiones que cubren 26 804 habitantes, o incluso hasta los 356 020 habitantes, y que podría elevarse en caso de presentarse una reacción en cadena. Pérdidas materiales para PQ las cuales implicarían la pérdida de activos estratégicos con valores que van desde los 7 a los 25 MDD y cuyo acumulado puede rebasar los 100 MDD, además de las pérdidas económicas derivadas de un paro de operaciones. También están implícitas pérdidas económicas para el estado de Veracruz, así como el gobierno federal, y un consecuente daño a la imagen del gobierno y un alto costo político. Estas

pérdidas potenciales no pueden ser evitadas en su totalidad, pero sí pueden ser disminuidos, o tener una menor posibilidad de presentarse, así como la organización y la región misma estar mejor capacitadas para resistir el impacto de estos eventos. La figura 4 muestra como un evento que desencadene el escenario de mayor magnitud de afectación puede alcanzar no sólo a otro complejo, sino también afectar una parte considerable de la zona urbana de Coatzacoalcos, y en caso del Complejo Cosoleacaque, cubrir en su totalidad la zona urbana de Minatitlán, así como una fuerte afectación a nivel ecológico de la zona.

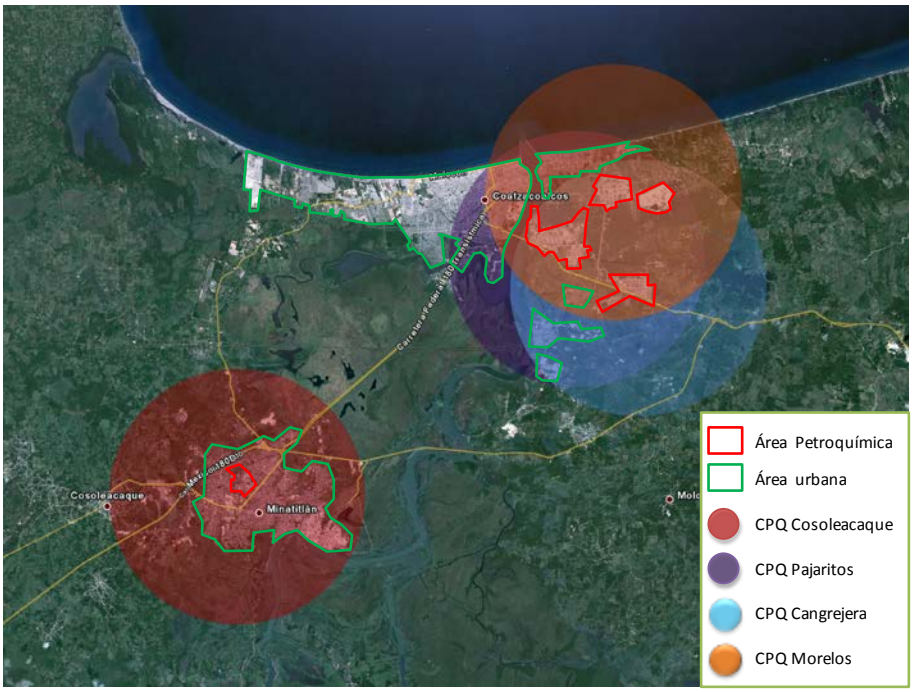

Figura 4: Alcance de los escenarios de mayor riesgo.
Fuente: Elaboración propia

Los escenarios de referencia, describen el cómo y por qué la organización se ve afectada si las suposiciones de las proyecciones referencia fueran ciertas. En términos generales, ¿cuál es el escenario de referencia esperado de acuerdo con las proyecciones de referencia obtenidas que llevará a la organización a su destrucción?

En primer lugar, con referencia al motivo de la existencia de un sistema de seguridad, la pérdida de activos estratégicos compromete seriamente la existencia de la organización. La pérdida de alguno de los activos estratégicos de la organización (humano, tecnológico, de información, etc.), compromete la capacidad de operación de esta, poniéndola a merced de sus competidores, o en

la imposibilidad de cumplir con sus clientes. Esta situación puede ir desde pérdidas económicas para la empresa, hasta demandas judiciales, que llevarían a la organización incluso hasta la bancarrota, y por ende a su extinción. De igual manera, las pérdidas económicas y materiales pueden llegar a tal punto, que se comprometa la solvencia de la organización llevándola al mismo destino.

Otro escenario es el determinado por las pérdidas humanas y el impacto ambiental provocado. En este caso, si el número de pérdidas o el nivel de impacto ambiental derivado de presentarse alguna de las proyecciones de referencia son considerables, tendrán una consecuencia directa en el futuro inmediato de la organización. Una situación de este tipo, generaría una gran presión social sobre la organización, así como en el gobierno, para detener de forma definitiva las operaciones de la organización, por ser consideradas un peligro manifiesto para la sociedad civil y el medio ambiente (se tienen antecedentes de este tipo). De igual manera, las repercusiones de índice jurídico derivadas de estas pérdidas, pueden llevar también a la organización a dar fin con sus operaciones. El costo político de no actuar "ejemplarmente" en situaciones de esta naturaleza, llevan al gobierno a actuar, generalmente, en pro de la presión social y estricto apego al orden jurídico.

Generalmente, las LCCI son capaces de soportar los impactos económicos y financieros que se presenten en caso de presentarse algún evento que atente contra su seguridad (no sólo por su tamaño y capacidad económica, sino también al apoyo que reciben por parte del Estado), sin embargo, la presión social y el alto costo político que representaría un evento que implique pérdidas humanos y/o un fuerte impacto ambiental, llevarían tanto al órgano administrativo de la LCCI, como al Gobierno Federal a detener de forma "indefinida" las operaciones. Esta situación ya tiene antecedentes dentro de esta organización, donde después de haber ocurrido algún accidente de no grandes repercusiones, la presión social y política ha llevado a detener de forma parcial o total las actividades por un tiempo "indefinido". Una vez analizada la situación de las proyecciones y escenarios de referencia, se formula la siguiente misión:

Estructurar un sistema que permita coordinar las acciones que realizan los diferentes grupos involucrados en la seguridad física en las LCCI, con la finalidad de salvaguardar la integridad física del personal y de las instalaciones, así como atender con mayor eficiencia emergencias o actos hostiles provocados por el hombre (fugas, incendios, sabotajes, explosiones, bloqueos, robos y otros); a través de establecer estrategias preventivas y

disuasivas, procedimientos operativos orientados a atender las emergencias, los recursos materiales y humanos pertinentes para su ejecución, así como los mecanismos de colaboración con el personal de apoyo externo y los lineamientos que la permitan, con el propósito de neutralizar, minimizar y controlar los efectos de actos ilícitos o situaciones de emergencia.

Especificación de las propiedades deseadas

La especificación de las propiedades deseadas (del Diseño Idealizado de Ackoff), va de la mano con lo planteado por Ozbekhan en su fase 2 de su Planeación Normativa, el Plan Normativo. Se trata del diseño (o rediseño) del futuro de la organización a partir de lo que es deseable para esta. Ackoff menciona que estas propiedades deberán estar ligadas a la misión del sistema, y se recomienda que sea producto de una lluvia de ideas. Por su parte Ozbekhan señala que este estado normativo se logra mediante la visualización de los "fines" que los actores son capaces de concebir en forma de ideales a los que se puede aproximar constantemente, pero nunca se logran del todo, y “objetivos” que son los estados más valorados futuro y que pueden derivar de tales fines. En este sentido, el Plan Rector de Petróleos Mexicanos y Organismos Subsidiarios define cuales son estos objetivos que PEMEX pretende como institución para el resguardo de su infraestructura, y es el marco normativo. Por otra parte, ya se ha mencionado que el objetivo de un SSF es resguardar físicamente la seguridad patrimonial o activos estratégicos de las personas, comunidades y organizaciones, con la finalidad de reducir la pérdidas asociadas a los riesgos, sin embargo, no obstante las medidas y acciones implementadas, estas pérdidas no pueden ser evitadas, ya que ningún sistema de seguridad es capaz de evitar la ocurrencia de un evento, sólo permite a la organización estar mejor preparada para ello, lo que ayuda a reducir la pérdidas. A partir entonces de este marco normativo y del proceso sugerido por Ackoff, se especifican a continuación las propiedades del SSF propuesto.

Las propiedades deseadas en un sistema de seguridad están dadas en virtud a cinco funciones básicas que debe desempeñar el sistema: disuadir, prevenir, detectar, evaluar, y reaccionar. Por lo tanto, las propiedades deseadas del sistema deben de ayudar a la realización de estas funciones, y deben ser además congruentes con los elementos sugeridos en el Capítulo 1: coordinación con otros organismos, delimitación de responsabilidades, estructuras instrumentadas para el desarrollo de las actividades, planeación de recursos, respuestas a emergencias, cadenas de mando y comunicaciones. Lo anterior enmarcado por la figura normativa correspondiente, que establecerá el cómo

debe ser el sistema. Las propiedades aquí presentadas se proponen como extensivas a las LCCI.

- Alinear a la normatividad o políticas en materia de seguridad física de la organización.
- Integrar por componentes propios y de apoyo capaces de dar una respuesta rápida y oportuna ante amenazas (especialmente antropogénicas como actos terroristas, de sabotaje, robos), que afecten a la operación normal de la organización, que permitan reducir sus efectos y con apoyo de las autoridades competentes para proceder en contra de los infractores, en forma de elementos físico-tecnológicos: barreras perimetrales, circuitos cerrados de televisión, controles de acceso, centros de mando; y actividades humanas: vigilancia y patrullaje.
- Mantener y fortalecer una coordinación, colaboración e intercambio de información, con las instancias competentes, al interior y exterior de la organización, que atiendan asuntos vinculados a la seguridad física, así como con aquellas dependencias de la administración pública de los tres niveles de gobierno que tengan injerencia en la seguridad, a través de establecer los mecanismos necesarios para dicha coordinación.
- Planear y proveer de recursos humanos suficientes y de tecnología de avanzada a los responsables de la gestión interna de la seguridad física de la organización, permitiendo innovar y mejorar continua y permanentemente el sistema de protección (elementos físico-tecnológicos) y los procesos administrativos y operativos que se requieran, e incentivar la profesionalización del personal, con la finalidad de cumplir con la normatividad requerida por la organización.
- Contemplar la modernización de las tecnologías de los sistemas de información para mejorar la toma de decisiones, permitiendo emplear estos como palanca para el apoyo para las acciones en materia de seguridad por parte de los responsables internos de la seguridad física.
- Coordinar las acciones de seguridad física a través de considerar las medidas certificadas, normalizadas o de tendencia en los organismos de mayor reconocimiento a nivel internacional, en materia de seguridad física, industrial, protección civil y preservación del medio ambiente, a fin de crear un clima de confianza que permita a la organización el desarrollo normal de sus actividades.
- Contar con procedimientos específicos de seguridad física que requiere la organización (control de acceso, atención a emergencias como amenaza de artefacto explosivo, actos de sabotaje, bloque a instalaciones, etc.), los

cuales le permitan responder de forma oportuna ante las emergencias y permitan minimizar las pérdidas potenciales, coordinado conjuntamente su elaboración con otras dependencias internas y externas que permitan un mejor producto.

- Identificar las responsabilidades y obligaciones de los niveles o cadenas de mando en la organización encargados de la seguridad física, y de todos aquellos involucrados directamente en la seguridad física, así como los medios que permitan medir el desempeño de estos.
- Coordinar oportunamente el despliegue de las fuerzas de reacción en atención de emergencias en materia de seguridad física, y en coordinación para el apoyo de emergencias industriales o de protección civil, en auxilio al personal y a la sociedad civil de las poblaciones cercanas al centro de trabajo de la organización.

3.2 Diseño del sistema

A partir de las propiedades ya especificadas, se plantea la estructura del SSF que se propone, a partir del proceso de construcción por descomposición propuesto por Gelman y Negroe (1982), en el cual se propone una construcción a través de una descomposición funcional, y que consistente en la desmembración del sistema en subsistemas cuyas funciones y propiedades aseguren las del sistema en su conjunto mediante una organización adecuada. Esta construcción considera en primer lugar el papel que desempeña el sistema en el suprasistema, al definir los objetivos y funciones totales. En este caso, el SSF es un subsistema perteneciente a un suprasistema determinado, es este caso en un subsistema de la Infraestructura Petrolera, considerada como LCCI, encargado de la protección y resguardo de dicha infraestructura.

Como ya se mencionó, Un SSF tiene por objetivo fundamental el resguardar físicamente la seguridad patrimonial o de activos estratégicos de las personas, comunidades y organizaciones de las amenazas físicas (producidas tanto por la naturaleza como por hombre, accidental o deliberadamente) que atenten en su contra, permitiendo reducir la pérdidas potenciales asociadas a los riesgos existentes, aumentar su capacidad de supervivencia, y mantener la continuidad operacional y la propiedad intelectual. Para ello, el sistema debe realizar una serie de funciones que en conjunto logren este objetivo. La diversa literatura alrededor del tema de seguridad lleva al autor a la proponer las siguientes funciones: prevenir, disuadir, detectar, evaluar y responder. Estas actividades conforman el SSF, y la figura muestra la estructura propuesta en un primer nivel de análisis.

Figura 5: Sistema de Seguridad Física y sus funciones, prevención, disuasión, detección, evaluación y respuesta.

Ahora, ¿cómo estas actividades permiten llegar a lo establecido en las propiedades deseadas del sistema? Analicemos una a una.

Señala el Diccionario de la RAE que disuadir es inducir, mover a alguien con razones a mudar de dictamen o a desistir de un propósito, mientras prevenir es preparar, aparejar y disponer con anticipación lo necesario para un fin, evitar, estorbar o impedir, advertir, informar o avisar a alguien de algo. ¿Cómo se relaciona esto con la seguridad?

En seguridad física, el futuro deseado es un ambiente en el cual la organización se encuentre en un estado libre de vulnerabilidades (o con las menos posibles), ante las amenazas que presenta su entorno, con la finalidad de mitigar los riesgos. Un paso para lograr esta situación, es precisamente hacer desistir a quien amenaza a la organización de perpetrar dicha acción. La disuasión pretende erradicar o desaparecer aquella situación que genera vulnerabilidad a la organización o sujeto ante una amenaza, poniéndola en riesgo, la prevención se anticipa a ello.

Existen diferentes actividades que son consideradas de disuasión y prevención que ayudan a llegar al estado deseado, y que aquí llamaremos actividades no directas de fortalecimiento a la capacidad disuasiva y preventiva, las cuales tienen que ver más con el aspecto que guarda la organización u objeto, que con aspectos técnicos o de gestión, y que generalmente no competen directamente al personal encargado de la seguridad física de la organización. Existe una gran cantidad de teorías en torno a esta situación, de la cual el autor considera

destacable la llamada “Teoría de las ventanas rotas”, Wilson y Kelling (1982), la cual señala que una vez que se empiezan a desobedecer las normas que mantienen el orden en una comunidad, tanto el orden como la comunidad empiezan a deteriorarse, a menudo a una velocidad sorprendente, a consecuencia que las conductas incivilizadas o incívicas se contagian. Esta teoría contempla el siguiente ejemplo:

"Consideren un edificio con una ventana rota. Si la ventana no se repara, los vándalos tenderán a romper unas cuantas ventanas más. Finalmente, quizás hasta irrumpan en el edificio, y si está abandonado, es posible que sea ocupado por ellos o que prendan fuego adentro. O consideren una acera o banqueta. Se acumula algo de basura. Pronto, más basura se va acumulando. Eventualmente, la gente comienza a dejar bolsas de basura de restaurantes de comida rápida o a asaltar coches."

Una buena estrategia para prevenir el vandalismo, dicen los autores de esta teoría, es arreglar los problemas cuando aún son pequeños. Repara las ventanas rotas en un período corto, digamos un día o una semana, y la tendencia es que será menos probable que los vándalos rompan más ventanas o hagan más daños. Limpiar las banquetas todos los días, y la tendencia será que la basura no se acumulará (o que la basura acumulada sea mucho menor). Los problemas no se intensifican y se evita que los residentes huyan del vecindario.

Entonces, la teoría hace dos hipótesis: que los crímenes menores y el comportamiento anti-social serán disminuidos, y que los crímenes de primer grado serán, como resultado, prevenidos. Las críticas a la teoría tienden a enfocarse únicamente en la segunda hipótesis. Sin ánimo de entrar en discusiones sobre esta teoría, los resultados que se han visto de situaciones como la recuperación de espacios públicos son visibles.

Ahora bien, aplicado a un SSF, las actividades no directas de fortalecimiento a la capacidad de disuasión están relacionadas con actividades que creen o generen las condiciones óptimas para la disuasión, es decir aquellas que de alguna forma signifiquen un obstáculo o dificultad para la realización de un delito, ya que generalmente, quienes comenten un ilícito, buscan una situación que les de mayores posibilidades de éxito y menor dificultad. Algunas de estas actividades pueden no estar directamente asignadas al personal de seguridad física, pero sí es de su interés el que se lleven a cabo lo más pronto posible y de la mejor forma. Actividades como mantener el perímetro de la organización limpio (libre de grafitis, maleza, basura), en conjunto con un alumbrado

perimetral óptimo y en buenas condiciones son situaciones que crean un ambiente que propicio a la disuasión de los infractores, así como también facilita a las actividades del personal de seguridad física. Es necesario coordinar las llamadas actividades de fortalecimiento a la capacidad disuasiva y preventiva, con aquellas áreas de la organización encargadas directamente de labores como el mantenimiento y limpieza, a fin de crear un ambiente dentro de la organización que sea propicio para la disuasión de los delitos. Lo anterior cumple con la propiedad enunciada que busca coordinar las acciones de seguridad física a través de considerar las medidas certificadas, normalizadas o de tendencia en los organismos de mayor reconocimiento a nivel internacional, en materia de seguridad física, a fin de crear un clima de confianza que permita a la organización el desarrollo normal de sus actividades.

Por otra parte, existen elementos dentro del SSF que explícitamente tienen un carácter disuasivo. Dentro de un SSF existen elementos y medidas que se ocultan, para así actuar, sorprender, y conservar la libertad de maniobra (elementos de repuesta o reacción), y otros que de forma premeditada se busca que sean fácilmente identificables a cualquier persona a fin de servir como una medida de disuasión. Dentro de estas medidas de disuasión comenzamos ver los elementos que conforman la parte física-tecnológica del sistema, y que como fue especificado en las propiedades deseadas, deberán alinearse con la normatividad o políticas en materia de seguridad física de la organización, y ser capaces de dar una respuesta rápida y oportuna ante amenazas que afecten a la operación normal de la organización, reduciendo sus efectos y con apoyo de las autoridades competentes para proceder en contra de los infractores. Dichos elementos son los siguientes:

- Barrearas perimetrales. Estas tienen como objeto delimitar y resguardar una zona específica, y existen una gran variedad y tipo de ellas (bardas, canales, mallas, cercas, etc.), pero básicamente lo que pretenden es presentar un obstáculo que disuada a quien se encuentra fuera de la zona delimitada de ingresar a la zona "asegurada".
- Circuitos cerrados de televisión (CCTV). Un CCTV es una aplicación tecnológica diseñada para vigilar y monitorear una determinada actividad. Básicamente lo constituye un medio de captación (cámaras), uno de observación (monitores), y uno de grabación (dvr´s, computadoras, etc.), interconectados por una red de comunicación. Además de permitir vigilar y monitorear, constituye

también una fuente de evidencia de los sucesos que registra. Generalmente, el saberse "observado" disuade a la personas de cometer actos ilícitos, de ahí que un CCTV sea un medio de disuasión.

- Controles de acceso. Un control de acceso es una actividad que tiene por objeto llevar a cabo una labor de reconocimiento o identificación para permitir o no la entrada a una zona restringida. En función del tipo de riesgos y de la naturaleza de la zona restringida, esta labor tiene puede tener como fin autenticar la identidad de quien pretende ingresar, o controlar aquellos objetos o materiales que pretendan ingresar o salir de la zona asegurada. Existen diferentes tipos de control de acceso que van desde actividades humanas (revisiones por parte del personal de seguridad), o automatizados (detectores de metales, rayos x, etc.). La existencia de estos controles disuade a las personas (la mayor parte del tiempo), de ingresar objetos prohibidos o entrar a una zona a la que no se tiene autorización para entrar.
- Patrullaje. El patrullaje en términos de la seguridad física, es una labor de vigilancia, llevada a cabo en la organización, por parte de las fuerzas o elementos de seguridad física. La presencia de un cuerpo de vigilancia que realice recorridos al interior y exterior de la organización, permite al sistema prevenir y disuadir algunas de las posibles amenazas que enfrenta la organización.

Los elementos hasta aquí descritos tienen un carácter disuasivo al ser elementos plenamente visibles pero también son preventivos en el sentido de que generan la capacidad de disminuir las pérdidas asociadas a los riesgos, al disponer con anticipación o prever los posibles eventos que puedan ocurrir y así fortalecer a la capacidad de respuesta del sistema. No obstante, cabe señalar que ninguna medida que se tome en materia de seguridad es capaz de evitar en su totalidad el daño a la organización u objeto. Lo único que se pretende lograr es disminuir las pérdidas potenciales (es decir disminuir los riesgos), a través de disuadir, y tener una capacidad de reacción adecuada y oportuna.

A partir de lo anterior, se puede disgregar el subsistema disuasión y prevención en las siguientes funciones básicas; resguardo perimetral, por medio de barreras perimetrales y rondas de patrullaje; control de accesos, entendido como la actividad de filtro de reconocimiento o identificación para permitir el ingreso o salida a una zona restringida (con apoyo de elementos tecnológicos y humanos); vigilancia y monitoreo por medio personal de vigilancia y con apoyo tecnológico (sistemas de CCTV); y las actividades no directas de fortalecimiento a la capacidad disuasiva y preventiva, como es la coordinación con las áreas de

mantenimiento y limpieza a fin de generar las condiciones necesarias para la disuasión. Estas actividades quedan sintetizadas en la siguiente figura, y que es un segundo nivel se análisis del subsistema disuasión y prevención. El control de accesos, la vigilancia y monitoreo, y el resguardo perimetral son un conjunto de actividades que actúan en un ciclo constante cuyo objetivo además de disuadir y prevenir es servir de apoyo a las actividades de detección y evaluación, mientras que las actividades no directas no pertenece a este ciclo, ya que estas actividades no son capaces de detectar y ubicar una amenaza, pero si sirven como apoyo en la disuasión y prevención.

Figura 6. Subsistema de Prevención y Disuasión

En lo que respecta a las actividades de detección, algunas de estas están ligadas a los elementos disuasivos. La detección es descubrir algo que no era evidente o visible, lo cual permite ubicar e identificar el tipo de evento. En ese sentido gran parte de los elementos disuasivos permiten al SSF detectar eventos.

En el caso de las barreras perimetrales por si solas no pueden llevar a cabo una detección, pero en conjunto con sensores y/o alarmas de intrusión, los cuales permiten "detectar" cuando algo o alguien pretende ingresar (con o sin autorización) a una zona restringida, son capaces de indicar y ubicar un intrusión.

De igual manera, los CCTV permiten llevar un monitoreo a distancia de puntos específicos de la organización que permiten detectar en tiempo real (o con un retraso de escasos segundos) la ubicación e identificación de los eventos que atenten contra la seguridad de la organización. Actualmente los CCTV pueden

ser configurados para llevar a cabo detecciones automáticas específicas que van desde paquetes abandonados, ingreso a una zona, reconocimiento facial, etc., y que facilitan y fortalecen la capacidad de detección y ayudan a agilizar la respuesta.

Por su parte, los controles de acceso permiten identificar y detectar eventos, al fungir como un filtro en el acceso a las instalaciones de la organización Estos filtros permiten detectar el ingreso y/o salida de personas, objetos o materiales no autorizados a una zona restringida (ya sea por medios automatizados o por personal humano). De igual manera, las labores de vigilancia y patrullaje permiten detectar no sólo eventos en flagrancia, sino también la detección de posibles vulnerabilidades al complejo a través de la realización de rondines de patrullaje.

Una vez detectada la actividad, (ingreso indebido, portación de objetos prohibidos, etc.), se procede a evaluar la respuesta pertinente, en función de la naturaleza de la amenaza o evento suscitado. La evaluación del evento reportado por los sistemas de detección, deberá permitir a los encargados de seguridad tener la información necesaria para saber de qué manera proceder. En primer lugar la evaluación del evento tiene por objetivo confirmar o descartar dicho evento, ¿se trata de una alerta real o es una falsa alarma? Ante la detección de un evento no se deben entrar en actuación los elementos de seguridad a menos de que este sea confirmado. En segundo lugar, si se ha confirmado una alarma, se debe proceder a evaluar la naturaleza del evento suscitado. ¿Qué está ocurriendo?, ¿de qué tipo de evento se trata? Una vez respondido esto, se deberá actuar conforme a la naturaleza del evento lo requiera. Esta evaluación debe ser llevada a cabo el personal encargado de la administración de la seguridad física de la organización (a través de un Centro de Mando), con apoyo de los medios detección que actúen en conjunto (por ejemplo, si el sistema de detección de intrusión capta una señal de alarma de invasión, esta debería ser confirmada por medio redundante, como una cámara de CCTV que permita al usuario confirmar o descartar de forma inmediata dicha alarma)

El Centro de Mando y Control (CMC), es el sitio en el cual, las redes de comunicaciones y los elementos tecnológicos del SSF, interactúan para concentrar la información y asuntos relacionados con la seguridad física; además, es el lugar donde se monitorean, activan y se envían alertas de reacción para controlar aquellos incidentes que atenten contra la seguridad física de las personas o los bienes de la organización. Dentro de su

infraestructura reúne los espacios, servicios y recursos, tanto técnicos como administrativos y financieros, necesarios para supervisar y proteger la seguridad física de las personas e instalaciones que protege. La parte medular del CMC es el Cuarto de Control (CC). El Cuarto de Control, es el sitio en el cual se supervisan y alojan los elementos de supervisión, control, detección y reacción del SSF, como el monitoreo del CCTV, control de accesos, detección de intrusiones, detección de sustancias y objetos prohibidos o peligrosos, alarmas de diferentes tipos, y registros de eventos, entre otros. También es considerado como el espacio físico, donde se toman las medidas necesarias para responder a sucesos y/o acontecimientos que atenten contra la seguridad física de las personas e instalaciones que protege.

Así, el subsistema de Detección y Evaluación está encargado de las funciones de: ubicación e identificación de eventos, a traces de los elementos de control de acceso, resguardo perimetral, y vigilancia y monitoreo; y confirmación y evaluación del evento, llevada a cabo en el centro de mando y control a través del personal encargado de la administración de la seguridad de la organización. Estas actividades quedan sintetizadas en la siguiente figura, las cuales conforman un ciclo, donde primeramente se realiza la ubicación e identificación del evento, para posteriormente una etapa de confirmación y evaluación a cargo del órgano de gestión del SSF; de ser confirmado se procede de acuerdo con el procedimiento correspondiente y de ser descartado regresa a la etapa de ubicación e identificación en espera de un nuevo evento.

Figura 7. Subsistema de Detección y Evaluación

Por último, el Subsistema de respuesta o reacción es el encargado de ejecutar y responder de acuerdo con lo que los otros dos sistemas le comuniquen a este. De la definición que se daba de seguridad en el Capítulo 1, en la que se señala que la seguridad es vista como el conjunto de principios aplicados a un adecuado sistema de protección (SSF), unidos a una actitud de obrar en forma lógica y razonable para generar una situación o estado de tranquilidad real, y a su vez es un conjunto de normas adoptadas para prevenir un peligro, riesgo o amenaza, y que es por estas características, de generar una situación, obrar de forma lógica y razonable, y la adopción de medios para lograr dicha situación, donde esta actitud debe ser encausada por un proceso de Planeación, para poder asegurar mayores probabilidades de éxito, tanto de la operación en condiciones normales, como en su respuesta ante eventos de emergencia.

Para poder llevar a cabo esta respuesta, este subsistema deberá constar de dos elementos, uno de gestión y el otro de ejecución. El elemento de gestión es el encargado de coordinar la respuesta inmediata ante un evento, además de responder ante estos eventos no sólo en tiempo real, sino a mediano y largo plazo, realizado las actividades de planeación del SSF, mientras que el elemento de ejecución se trata de una fuerza de reacción ante los eventos, que responde de forma inmediata ante la ocurrencia de un evento. Estas actividades quedan sintetizadas en la figura 8.

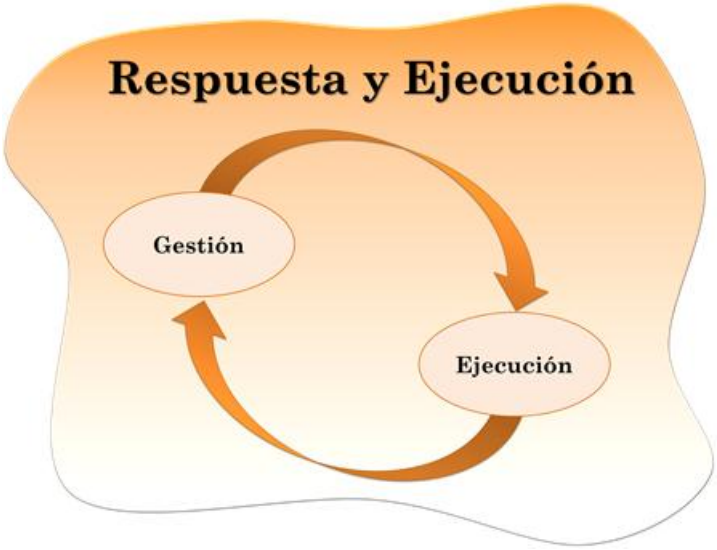

Figura 8. Subsistema de Respuesta y Ejecución

Ahora, ¿Cuáles son las tareas que debe llevar a cabo la parte de gestión? La parte de gestión conduce a los demás elementos del sistema, es quien dice que hacer y cómo hacerlo, por lo cual deben ser los encargados del CMC, ya que este

es el lugar donde converge la información en tiempo real generada por los elementos tecnológicos del SSF y son los responsables directos de la evaluación de la amenaza y del consecuente proceder. Y es aquí donde entra el proceso de planeación.

Este proceso de planeación necesariamente debe apoyarse en un análisis de riesgos que el órgano de gestión del SSF debe programar de manera periódica (anualmente, dada la cantidad y complejidad de la información manejada), ya que este le permite conocer los blancos potenciales y las vulnerabilidades de la organización, así como las amenazas que la rodean. Como ya se ha mencionado, el análisis de riesgos deberá ser congruente con el contexto y tener en cuenta todos los aspectos no sólo de pérdidas económicas, humanas, ambientales y materiales, sino también aspectos, sociales, organizacionales, culturales y todo aquel que sea relevantes para el SSF.

Como ya se advertía, la mejor manera de responder ante un evento es a través de tomar anticipadamente las decisiones de que hacer en caso de un evento. Para ello es necesario prever los escenarios de emergencia posibles a fin de determinar cuál es la mejor forma de proceder de acuerdo con el tipo de evento (¿qué elementos son necesarios?, ¿a quién se debe recurrir?, ¿qué se debe de hacer?) y aprovechar así los recursos disponibles, y que se sintetizan en la forma Procedimientos de Operativos de Emergencia. Estos procedimientos deben contemplar la mayor gama posible de emergencias que puedan ocurrir y no ser limitados por las capacidades de la organización, sino por las capacidades de quien representa la amenaza, y que permitan no sólo responder, sino prevenir y establecer las medidas de recuperación después de un evento.

Ahora bien, para poder responder adecuadamente a las emergencias es necesario contar con los elementos de reacción necesarios y acorde a la naturaleza de la amenaza, sin embargo no siempre es posible tener a total disposición a los elementos necesarios para cubrir todas las posibles emergencias que pudieran suscitarse. Para ello es necesario contar con Mecanismos de Coordinación que permitan compartir los recursos de respuesta emergencia de los agentes tanto internos como externos a la organización, y que permitan una adecuada atención de la emergencia. De acuerdo con lo ya señalado es el Capítulo 1, sobre coordinación con otros organismos.

Esta coordinación se debe hacer extensiva a las labores de Generación e Investigación de Información Estratégica en materia de seguridad física que debe coordinar los encargados de la gestión del SSF de la organización, con los

elementos de seguridad e inteligencia externos que apliquen (en el caso de las infraestructuras críticas México deberá ser con el Centro de Investigación y Seguridad Nacional, CISEN). A través de estas labores se deberá obtener información estratégica para el SSF en relación a su entorno: índices delictivos, antecedentes de sabotaje y/o terrorismo, desastres naturales, información de socioeconómica, política, cultural y ambiental de la zona, con la finalidad de integrar una gama lo suficientemente basta de información que pueda servir de apoyo en las labores del SSF. Las amenazas en la zona sur de Veracruz descritas en el Capítulo 1 de este trabajo es un ejemplo de esta información estratégica. El dotar al SSF con esta información permite a los encargados de la gestión contar con elementos de apoyo para poder realizar el proceso de planeación del sistema, y es además una medida preventiva que amplía el horizonte de conocimiento del entorno de la organización lo cual le permite una mejor base para establecer las posibles amenazas que pueden suscitarse y que es primordial en los análisis de riesgos.

Una respuesta acertada ante las emergencias, (es decir, aquella que genere menos pérdidas) se logra estando preparado para ellas, por medio de los simulacros. Y a su vez, en conjunto con la existencia de los procedimientos de emergencias que pauten el modo de operar ante un evento. La parte de gestión del SSF debe programar, conjuntamente con protección civil y seguridad industrial de la organización, la elaboración de simulacros de emergencia en materia de seguridad física.

La gestión del SSF deberá ser la responsable de programar y presupuestar los gastos y elementos necesarios para llevar a cabo las labores del sistema por medio de programas de adquisición y asignación de recursos. Así mismo es responsable de proponer y revisar los elementos de evaluación y control del sistema, y de generar y revisar los indicadores de desempeño del sistema.

De igual manera los encargados de la gestión del SSF, deben realizar actividades que fortalezcan la capacidad preventiva, disuasiva y de reacción del SSF, a través de programas de modernización tecnológica en materia de seguridad física, actividades de actualización y profesionalización del personal de seguridad, y a través de coordinar las actividades no directas de fortalecimiento a la capacidad disuasiva y de prevención con los correspondientes órganos internos y externos de la organización.

La figura de gestión, debe coordinar las actividades inmediatas de los elementos de reacción del SSF para responder ante un evento. Estos elementos

de reacción deben estar conformados por los elementos internos de seguridad de la organización, así como por aquellos elementos de organizaciones externas, y cuya coordinación deberá estar dada en virtud de la naturaleza de la emergencia a tratar, a través de una adecuada cadena de mando que identifique las responsabilidades y funciones de cada uno de los elementos involucrados.

Así mismo, la parte de gestión de este subsistema deberá estar encargada de la elaboración de un Programa Integral de Seguridad Física (PISF), el cual deberá ser congruente con en el marco normativo que aplique a la organización, lo cual dependerá de la naturaleza del objetivo de la organización. En el caso de la LCCI de la industria petrolera del país, el Plan Rector es el marco normativo y se apoya en la Política General de seguridad física de PEMEX, así como de las normas mexicanas e internacionales que se apliquen. En el caso de los aeropuertos, estos se deben atener a la normatividad que señala la Organización de la Aviación Civil Internacional (OACI), o der ser necesario Conferencia Europea de Aviación Civil (CEAC) o la Transportation Security Administration (*TSA*). Dicho Programa se debe recoger los elementos aquí señalados, es decir debe contemplar información estratégica para el sistema, las actividades contempladas en materia de materia de: modernización tecnológica, adquisición y asignación de recursos; debe contener también los simulacros de emergencia, procedimientos operativos de emergencias, mecanismos de coordinación, así como identificar claramente las cadenas de mando bajo la que rige el SSF, a partir de definir las responsabilidades, funciones y alcances de los elementos del sistema.

La parte de ejecución como se mencionó es una fuerza de reacción ante los eventos, que responde de forma inmediata ante la ocurrencia de un evento. En el SSF debe ser una fuerza de seguridad de reacción encargada de atender dichos eventos por medio de personal de la organización y/o personal de seguridad de aquellas organizaciones o entidades con las que se tengan mecanismos de coordinación, en virtud de la evaluación del evento que se esté suscitando.

Finalmente, el SSF debe contemplar un Sistema de Información Intensiva (SII), que permita coordinar a todos los elementos del SSF que proporcionen información que ayude al sistema a adaptarse al escenario cambiante y ser capaz de responder y sobrevivir en su entorno. Así, las actividades propuestas que conforman el SSF propuesto quedan representadas en la siguiente figura.

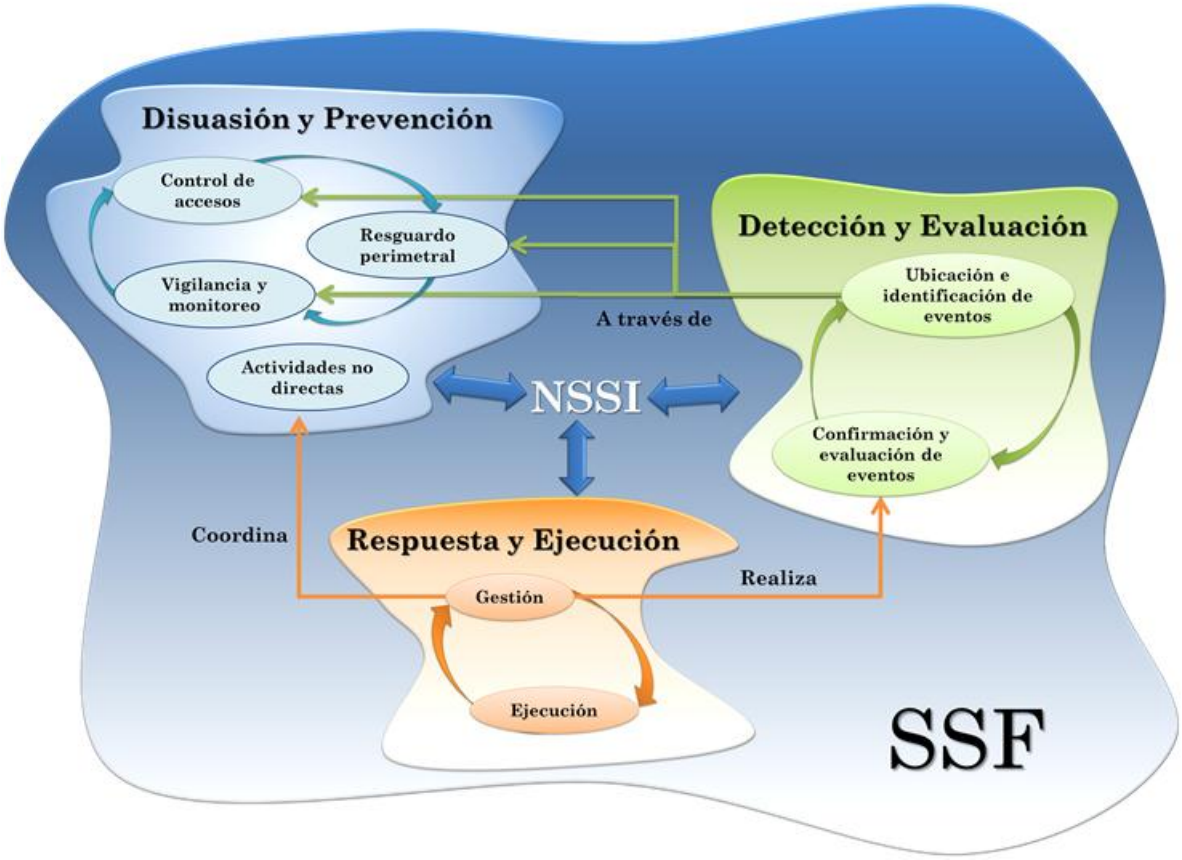

Figura 9. Estructura propuesta de las funciones de un SSF

Integración de la información en materia de seguridad física a través de una Red de Sistemas de Información Intensiva.

El diseño, estructura y creación de una Red de Sistemas de Información Intensiva de seguridad física en la organización permite la integración de la información estratégica del área, lo cual facilita una mejor explotación de los recursos disponibles.

Es importante contar con información de Recursos Humanos y de Seguridad Industrial entre otros. Esta información del personal no puede ser actualizada por el personal de Vigilancia o seguridad física, esta debe ser actualizada por Recursos Humanos y llegar a un acuerdo con el área de IT para obtener las actualizaciones de la Base de Datos de personal, de manera periódica, de acuerdo con las necesidades de operación.

Según el nivel de riesgos en la organización y de la manera en la que esta se encuentra estructurada, el compartir información con el exterior puede resultar

necesario. En el caso de las LCCI´s, esto podría permitir intercambiar información y recursos que permitan atender de mejor manera las emergencias o preverlas. De igual manera, de acuerdo con el nivel de riesgo de la organización, la formalización de la estructura de colaboración puede requerir el intercambio de información en materia de seguridad, de conformidad con la Ley del Sistema Nacional de Seguridad Pública (SNSP), que indica que las instalaciones estratégicas del país deben compartir información de seguridad con "Plataforma México".

En este tenor, es una responsabilidad del área de seguridad física de la organización, el llevar el registro de los datos y eventos relacionados con su actividad. La importancia de llevar estos registros de una manera sistematizada, ofrece la oportunidad de qué a través de su análisis, poder planear, controlar y evaluar las actividades del área de seguridad física, concretamente a través de realizar un análisis de los ilícitos ocurridos en la organización y que permite un bucle de retroalimentación en el sistema. Lo anterior hace indispensable la conformación de un Sistema de Información.

Para crear la Red de Sistema de Información Intensiva de seguridad física, se deben analizar los datos de mayor uso en la materia y la manera en que pueden ser explotados para llegar a un diseño de cómo capturarlos, almacenarlos, administrarlos y explotarlos.

A continuación se presenta de manera general una propuesta de diseño conceptual de la Red a partir de las condiciones de operación encontradas en la infraestructura crítica de PQ y las necesidades identificadas para el mejor desempeño de las áreas de seguridad.

Componentes de la Red de Sistema de Información Intensiva:
Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad (objetivo). Dichos elementos formarán parte de alguna de estas categorías:

- Personas.
- Datos.
- Actividades o técnicas de trabajo.
- Recursos materiales en general (típicamente recursos informáticos y de comunicación, aunque no tienen por qué ser de este tipo obligatoriamente).

Todos estos elementos interactúan entre sí para procesar los datos (incluyendo procesos manuales y automáticos) dando lugar a información más elaborada y distribuyéndola de la manera más adecuada posible en una determinada organización en función de sus objetivos.

Algunos de los componentes identificados (en forma de datos e información) para integrar el Sistema de Información en materia de seguridad física y su descripción se presentan a continuación:

- Control de Acceso de Personas, Vehículos, Equipos y Materiales
- Registro de eventos relacionados con la Seguridad
- Labores de vigilancia y patrullaje
- Consignaciones
- Información de inteligencia

Contenido del Sistema de Información

Una vez que se han definido los componentes del Sistema de Información, se definen los grupos datos que se van a guardar. A manera de propuesta y sin ser limitativo, se mencionan algunos de estos grupos o tablas. Éstos podrán ser complementados o eliminados de acuerdo con las condiciones específicas del momento en que se desarrolle e implante el sistema.

1. Identificación de Personas
    a. Personal de la organización
    b. Personal de fuerzas de seguridad
    c. Personal de proveedores
    d. Personas implicadas en incidentes
    e. Personas consignadas
2. Reporte Diario de Actividades de Vigilancia
    a. Lista de asistencia
    b. Reporte de vehículos
    c. Patrullaje
    d. Eventos
3. Parte Informativo para eventos significativos
    a. Personas involucradas
        i. Presunto delincuente
        ii. Presuntos cómplices
        iii. Personal de vigilancia o Fuerzas de Reacción que detuvieron a los implicados
    b. Reporte de los hechos

c. Parte médico
d. Autoridades que intervienen
e. Formato oficial para consignación
f. Seguimiento del caso
g. Componente espacial
    i. Lugar de los hechos
    ii. En caso de tratarse de robo:
        1. Lugar de la extracción
        2. Lugar de la detección
        3. Lugar de la intrusión (si fueron externos)
        4. Lugar por donde querían extraer lo robado

4. Información estratégica de inteligencia
    a. Antecedentes delictivos de la zona
    b. Antecedentes de sabotaje y terrorismo de la zona
    c. Información general de la zona
        i. Geográfica
        ii. Social
        iii. Ambiental
        iv. Desastres naturales
        v. Infraestructura de respuesta a emergencias.

A su vez, los grupos de datos y el conocimiento de su uso y explotación permiten definir el detalle de los elementos que requiere el SI. A partir de los datos e información ingresada al SI se está en la capacidad de generar información que sea útil para el SSF de seguridad física, como estadísticas de eventos, reportes e indicadores de evaluación del sistema. Esta información permite al sistema responder instantáneamente ante los eventos, y planificar las acciones a mediano y largo plazo.

Mecanismos de coordinación

Para salvaguardar la integridad física del personal, instalaciones, bienes y activos estratégicos de la organización, es necesario robustecer el campo de protección y capacidad de respuesta ante la ocurrencia de una emergencia. Esto, a través de establecer mecanismos de coordinación con los ámbitos de seguridad externos (Gobierno Federal, Estatal, Municipal o instituciones privadas) en forma de convenios de coordinación, a fin de la integrar los recursos técnicos, humanos y materiales de los que estos disponen. El grado de compromiso y formalización de estos convenios está determinado por los riegos identificados en la organización. Como se mencionó en el Capítulo 1, entre

mayor sea el impacto de estos riesgos al país, gobierno y sociedad, mayor formalidad y compromiso requerido por estos convenios. Los aspectos que se deben considerar en los convenios de coordinación se presentan a continuación.

Objetivo

El objetivo principal de un convenio de coordinación es indicar que "servicios" prestará a la organización la entidad con que se efectué el convenio de colaboración, que pueden ir desde intercambio de información estratégica en cuestiones de seguridad, servicios de protección, vigilancia, patrullaje e inteligencia y de apoya en la respuesta a emergencias.

Marco legal y normativo

El marco legal y normativo proporciona las bases sobre las cuales las instituciones construyen y determinan el alcance y naturaleza de la participación política en el convenio. En este regularmente se encuentran las provisiones regulatorias y normativa, así como leyes interrelacionadas entre sí en materia de seguridad.

Responsabilidades y compromisos de la organización

El se deberá nombrar a un representante, el cual debe conocer el convenio de coordinación, normas y especificaciones que aplican, además de tener la facultad para supervisar las actividades a realizar contenidas en el convenio. Debe plasmar también las responsabilidades a las que deberá comprometerse la organización para que los representantes del Gobierno Federal, Estatal o Municipal, puedan dar cumplimiento a sus funciones acordadas en el convenio de coordinación.

Responsabilidades y compromisos de los ámbitos externos de seguridad

Deberán nombrar a un responsable, el cual debe conocer el servicio, normas y especificaciones del convenio de coordinación; además de tener facultad para controlar y supervisar a los grupos que realizan los servicios acordados en los convenios de coordinación. Este apartado debe definir claramente las responsabilidades que la entidad con la que se efectúa el convenio, asume a favor de la organización, así como las tareas necesarias que deberá llevar a cabo para realizar lo planteado en los objetivos del convenio.

Compromisos conjuntos

Deben ser los acuerdos a los que deben llegar ambas partes para poder llevar a cabo los objetivos planteados en el convenio, como acuerdos de la entrada en vigor y de modificaciones al convenio.

Suspensión de los servicios

Motivos por los cuales a su vez con quien se efectúa el convenio (ámbitos de seguridad externos), se reserva el derecho de suspender el servicio, para cumplir con otros compromisos constitucionales y legales, lo cual hará con previa notificación a la organización.

Relación laboral

En este apartado se deberá definir bajo la dirección de quien trabajara el personal tanto de la organización, como de aquella entidad con la que se efectúa el convenio. Es recomendable que quien esté a cargo sea personal de la organización, ya que el ceder esta dirección ante una entidad externa a la organización, puede ser interpretado como manipulación.

Confidencialidad de los servicios

La información que reciba la entidad o entidades con la que se tenga efectuado el convenio, por razones de la prestación de los servicios establecidos en el convenio, así como la información resultado del trabajo conjunto de entre estas y la organización, no debe ser divulgada ni transferida a terceros, sin el acuerdo previo y por escrito de las partes involucradas.

Vigencia

La vigencia de los convenios será acordada entre quienes suscriban el acuerdo, el cual se podrá revisar, modificar o adicionar, previo acuerdo de las partes. Se debe incluir un apartado que determiné los motivos de la conclusión anticipada convenios, por causas justificadas de cualquiera de las partes que lo suscriben.

Procedimientos operativos de emergencias

Los Procedimientos Operativos de Emergencia permiten establecer las medidas preventivas y acciones de respuesta y recuperación para atender aquellas emergencias que, de presentarse, podrían causar serios estragos no sólo en Organización, sino en las zonas aledañas a éste, como empresas y población civil y medio ambiente.

Es importante que en estos procedimientos se identifique claramente al coordinador general de la emergencia; a los coordinadores de contingencia entre los cuales se realicen las labores de coordinación para atender a la emergencia; las acciones preventivas, para el caso en que apliquen, que

permitan tomar previsiones contra algún tipo de incidente, como pueden ser simulacros; acciones iniciales, que incluyen labores de coordinación y preparación de recursos humanos y materiales para el ataque a la emergencia; acciones de respuesta que permitan atacar directamente la emergencia; acciones de recuperación para volver lo más rápido posible a las actividades normales del Complejo; y, de ser necesario, acciones de control para mantener la Seguridad física de las instalaciones de la organización. Los aspectos que se deben considerar en los procedimientos operativos de emergencias deberán ser: objetivos, alcance, marco legal y normativo, y el desarrollo del procedimiento (con la estructura que ya se ha mencionado).

Es imprescindible diseñar un escenario por cada uno de los procedimientos a elaborar, a través de definir un conjunto de supuestos acerca de las posibles amenazas a las que está sujeta la organización (de origen natural o antropogénico), con el objeto de responder de manera adecuada ante una situación lo más cercana a la realidad. Se deben considerar las experiencias anteriores, acerca de los fenómenos que con mayor incidencia han ocurrido en el área geográfica, o bien, los incidentes que han ocurrido históricamente en la organización o en organizaciones aledañas. A continuación se enuncian los procedimientos que se proponen dentro de una estructura general de un SSF.

- Procedimiento de Emergencia de supuesto de robo.
- Procedimiento de emergencia por Supuesta amenaza de artefactos explosivos.
- Procedimiento de Emergencia por atentados terroristas y actos de sabotaje.
- Procedimiento de Emergencia por ataque de personal armado.
- Procedimientos de Emergencia por siniestros y daños intencionales.
- Procedimiento de Emergencia por daños causados por fenómenos naturales

Adicionalmente a estos procedimientos, los cuales deben ser procedimientos que permiten establecer medidas de prevención, reacción y recuperación a eventos que se manifiestan de manera común, se deben establecer procedimientos a realizar de manera cotidiana y que sirvan también para establecer tareas de prevención, detección y reacción a emergencias. Estos son algunos de estos procedimientos cotidianos a considerar.

- Procedimiento para el control de acceso y salida peatonal y vehicular.
- Procedimiento para el control de personas y vehículos dentro de las instalaciones.

- Procedimiento para el ingreso y salida de materiales, armas, objetos no autorizados.
- Procedimiento para el cuidado y vigilancia de las áreas críticas (de alto riesgo o donde se encuentran los activos estratégicos)
- Procedimientos para patrullaje de las instalaciones.

Elaboración de simulacros en materia de seguridad física

Una manera eficaz de combatir un estado de emergencia es a través de la planeación de actividades de apoyo para el ataque a estos estados de emergencia, y dentro de esta, la difusión y realización de simulacros es una herramienta que permiten establecer un ensayo acerca de cómo se debe actuar en caso de que se presente la emergencia, a través de seguir un programa previamente establecido basado en procedimientos de seguridad y protección. El ensayo o simulacro pone a prueba la capacidad de respuesta, y su ejercicio permite evaluar y retroalimentar los programas. Adicionalmente, los simulacros sirven para acostumbrar al personal a adoptar las rutinas de acción más convenientes para reaccionar de manera más fluida en caso de una emergencia.

Ya sea dentro del programa de simulacros con el que cuente la organización, o que sea necesario crear un, se debe contemplar la realización de simulacros en materia de Seguridad física. En él se debe explicar cuáles son las actividades previas y las acciones a aplicar para poder difundir y realizar con éxito un simulacro en materia de seguridad, con la finalidad de inhibir o mitigar las consecuencias de un accidente, atentado o fenómeno natural potencial o real, interno o externo, que pueda afectar al personal, instalaciones o al medio ambiente de la organización y/o a la comunidad circundante.

Algunos de los elementos que se deben considerar en la organización de los simulacros en materia de seguridad son los siguientes: responsables de la organización de las brigadas internas (rescate, primeros auxilios, etc.) por parte de cada sección de la organización, brigadistas, observadores, evaluadores y controladores.

Sobre los escenarios para los simulacros, necesario apegarse a las condiciones reales en que pueda ocurrir un desastre, realizar recorridos de reconocimiento por las áreas de operación del simulacro, consultar planos, elaborar croquis y determinar zonas que representen menores posibilidades de rescate.

Programas de modernización tecnológica

Es recomendable que los programas de modernización tecnológica consideren los siguientes puntos:

- Elaboración de un diagnóstico de las necesidades tecnológicas de la organización en materia de seguridad física.
- Investigar la tecnología de punta y analizar su aplicación a las condiciones de la organización.
- Prever recursos financieros y elaborar un programa de adquisiciones para cubrir las necesidades de equipo de acuerdo con el diagnóstico, así como aplicar un programa de mantenimiento de equipos.

Para coadyuvar a la realización de estas actividades es necesario considerar los siguientes elementos:

- Fecha del último diagnóstico de necesidades tecnológicas
- Determinar si este diagnóstico de necesidades es producto de un análisis de riesgos y vulnerabilidad
- Considerar los siguientes elementos para el diagnostico de modernización tecnológica:
  - Centro de control y mando
  - Perimetrales
  - CCTV
  - Control de accesos
  - Procedimientos y organización
- Generar documentación de los resultados obtenidos
- Establecer recomendaciones tecnológicas producto del diagnóstico
- Determinar el porcentaje de las recomendaciones convertidas en proyectos en forma, para ser utilizado como parámetro en estudios posteriores.
- Determinar si existen proyectos en marcha derivados de esos resultados
- Determinar si existen proyectos completados derivados de estos resultados
- Definir si existe un presupuesto preestablecido destinado a la adquisición y modernización tecnológica
- Determinar si existe un programa de adquisición y modernización tecnológica
- Determinar si existe un programa de mantenimiento de los componentes tecnológicos del sistema de seguridad en los siguientes rubros:

- Centro de control y mando
- Perimetrales
- CCTV
- Control de accesos
- Procedimientos y organización

Indicadores de desempeño del sistema de seguridad física

Los indicadores de desempeño del sistema son elementales para evaluar, dar seguimiento y medir el grado de compromiso de la organización con un objetivo en particular, es este caso la seguridad física. Para ello es necesario seleccionar las métricas adecuadas y utilizar datos objetivos, garantizando que se puedan comparar, obtener y repetir en el tiempo y que permitan establecer una medida del desempeño del sistema. De acuerdo con el tipo de infraestructura u organización que se trate se deberán emplear las normas y estándares que permitan evaluar las medidas particulares de seguridad para la organización.

Sin embargo, un punto en común entre las diferentes organizaciones son los sistemas de información. En el Capítulo 1 se indica que las LCCI's poseen un Sistema de Información Intensiva (NIIS) el cual tiene a su cargo la operación del sistema (LCCI). La norma ISO/IEC 17799 (denominada también como ISO 27002) es un estándar para la seguridad de la información, con el título de Information technology - Security techniques - Code of practice for information security management. Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información, definida en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".

La versión de 2005 del estándar incluye las siguientes once secciones principales:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.

5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

Independientemente de los elementos establecidos por la ISO/IEC 17799, se pueden establecer indicadores específicos en materia de seguridad física. Los responsables de la gestión del SSF y los elementos de las fuerza de reacción (encargados de la ejecución) deberán establecer conjuntamente los indicadores que permitan medir desempeño del sistema. Algunos de los posibles indicadores que el autor considera relevantes y que se proponen son:

Cumplimiento a la normatividad de seguridad específica.

Este indicador tiene como propósito evaluar el nivel de cumplimiento de las actividades contempladas dentro de la normatividad específica que aplique a la organización. En el caso de PEMEX PQ, este indicador se desarrollará de acuerdo con lo especificado dentro del Plan Rector de Seguridad Física de PEMEX.

Este indicador mide la eficacia ya que se evalúa las actividades de seguridad física presentados en la organización y permite verificar la ejecución apropiada. De igual forma al comparar datos históricos se podrá medir el comportamiento de los controles existentes.

La normatividad establece los parámetros para la seguridad de la organización, pero cada una de estas los adapta a sus necesidades. Esta revisión se recomienda sea anual y la información generada debe ser entregada al órgano administrativo superior del encargado de la gestión del SSF de la organización. En el caso de los complejos de PEMEX PQ por ejemplo, esta información se deberá entregar al órgano de control interno de PEMEX PQ.

Incidencias de inseguridad presentadas en la Entidad

El propósito de este indicador es minimizar la frecuencia de los acontecimientos que afecten la seguridad de la organización, permite medir la eficiencia del SSF ya que evalúa el comportamiento histórico de los casos de inseguridad presentados en la organización y permite verificar si los controles existentes son apropiados.

La manera de medir este indicador es a través de los informes y registros de los eventos (robos, actos mal intencionados de terceros, etc.) presentados y que permitan llevar una estadística de incidencias. Se recomienda que se realice con una frecuencia mensual.

Estudios de seguridad

El propósito de este indicador es verificar los estudios de seguridad elaborados en la organización y mide la eficacia del sistema ya que se evalúa la realización de los estudios de seguridad presentados en la organización y permite verificar si los controles existentes y recursos son apropiados. Se recomienda realizar de forma anual. Para ejemplificar esto, en el caso de PEMEX PQ, cada Complejo debe de elaborar estudios de seguridad física de manera periódica (anualmente cada complejo debe realizar un análisis de riesgos), sin embargo es necesario enviar a la dirección Administrativa de PEMEX PQ, un oficio con las novedades presentadas y la información obtenida en estos estudios con la finalidad de verificar las medidas de seguridad que se están llevando a cabo dentro de los complejos.

Integridad de los elementos del SSF

El propósito de este indicador es verificar la integridad del SSF que sean susceptibles de fallas físicas o de operación y mide la eficacia de los elementos ya que se evalúa que cumplan con su objetivo o el efecto deseado. Un ejemplo de esto es medir la integridad de la barda perimetral, del 100 por ciento de la barda ¿Cuáles son las condiciones que esta guarda? (por porcentaje). Así con los diferentes elementos como cámaras, arcos detectores, y demás equipo.

Indicadores específicos

Cada organización puede tener indicadores específicos determinados por un órgano interno del suprasistema al que pertenece. En el caso de PEMEX PQ por ejemplo, existen siete indicadores que la Dirección Corporativa de Administración a través de la Gerencia de Servicios de Seguridad Física

entregará a la Comisión Asesora Interorganismos de seguridad física, mismos que se reproducen a continuación.

Indicador	Formula
Seguridad física a instalaciones	(*Servicios de seguridad física realizados x* 100) /(*Servicios de seguridad física programa*
Protección a Funcionarios	(*Servicios de protección realizados x* 100)/(*Servicios de*
Protección al personal	(*Servicios de protección realizados x* 100)/(*Servicios de*
Patrullajes a la red de ductos	(*Patrullajes para la seguridad física realizados x* 100) /(*Patrullajes para la seguridad física pro*
Investigaciones de hechos delictivos en contra de la Institución	(Acciones de Investigación realizadas x 100)/(*Acciones de Inve*
Peritajes	(*Peritajes programados x* 100)/(*Peritajes realizados*)
Información relacionada con Petróleos Mexicanos y Organismos Subsidiarios	(*Acciones de información Realizadas x* 100)/(*Acciones d*

Hasta aquí la descripción de los elementos propuestos para el SSF. Cada uno de ellos ha sido revisado de forma general con la finalidad de que sean adaptables a LCCI's diferentes a la empleada como ejemplo.

Capítulo 4. Conclusiones y discusión de resultados

El actual clima de preocupación alrededor a la seguridad a nivel mundial ha llevado a los gobiernos a tener una mayor preocupación sobre los niveles de seguridad de los sistemas que resguardan a su infraestructura crítica. Esta infraestructura por sus características de complejidad en sus relaciones ha sido llamada como Infraestructura Crítica Larga y Compleja, LCCI, y es un blanco ideal para quienes buscan causar daños que desestabilicen fuertemente a los gobiernos y sociedad en general. Los sistemas de seguridad física de estas infraestructuras tienen como propósito el resguardar físicamente la seguridad patrimonial o de los activos estratégicos de estas organizaciones de las amenazas (naturales y antropogénicas) que atentan contra ellas, a través de actuar directamente sobre las vulnerabilidades de la organización, y de generar la capacidad y adquirir los recursos que permitan el combate a estas amenazas, con la finalidad de reducir las pérdidas potenciales asociadas a los riesgos (establecidos por la relación de las amenazas y vulnerabilidades), aumentar su capacidad de supervivencia y mantener la continuidad operativa. No obstante, gran parte de estos sistemas dan un fuerte peso a la implementación de medidas de apoyo tecnológico para el combate a eventos, incluso la oferta de sistemas integrales de seguridad física hace referencia a integrar los elementos tecnológicos de este sistema. Si bien sistemas de estas características permiten

a la organización tener la capacidad de detectar e identificar un evento, no garantizan que el sistema tenga la capacidad de responder a estos eventos en forma que las pérdidas sean las menos posibles.

El problema principal es que los sistemas de seguridad, en algunas ocasiones, no cumplen (o lo hacen de manera parcial) con la alineación al marco normativo correspondiente, y las medidas tomadas lejos de ser integrales, son acciones aisladas o insuficientes que no permiten una explotación adecuada de los recursos con los que cuenta el sistema, lo que vuelve a la organización vulnerable ante las amenazas potenciales, lo cual compromete el futuro de la organización. Un acercamiento holístico al diseño de los sistemas de seguridad física, permite a la organización tener un mayor control sobre su futuro, a partir de acciones en materia de seguridad producto de un proceso de planeación.

La propuesta de SSF contempla tres grupos de actividades:

- Disuasión y prevención
- Detección y evaluación
- Respuesta y ejecución

En el subsistema de disuasión y prevención está conformado por cuatro actividades: control de accesos, resguardo perimetral, vigilancia y monitoreo, y actividades no directas de fortalecimiento a la capacidad disuasiva y preventiva. Las tres primeras actividades contienen una fuerte componente tecnológica en la actualidad, y constituyen el principal componente de los sistemas de seguridad física que cotidianamente se encuentran. El incluir actividades no directas permita al sistema crear un ambiente que favorece a la capacidad disuasiva y preventiva a través de medidas que no pertenecen estrictamente al área de seguridad física, pero que ayudan al sistema a cumplir de mejor forma su objetivo.

El subsistema de detección y ubicación tiene a su cargo la tarea de ubicar e identificar los eventos que atenten contra la seguridad física en el momento que se están suscitando o que tienen una fuerte posibilidad de ocurrir en un corto plazo, apoyados de los elementos de control de accesos, resguardo perimetral, y vigilancia y monitoreo. La confirmación y evaluación permite descartar falsas alarmas, y generar una respuesta que sea acorde al tipo de evento que se está suscitando.

Finalmente la etapa de respuesta y ejecución es la encargada de responder a los eventos de forma inmediata a través de un elemento encargado de la ejecución y de la respuesta a mediano y largo plazo por parte de un órgano de gestión. Dicha respuesta a mediano y largo plazo es dada en forma de un proceso de planeación el cual debe de generar, entre otras, las siguientes actividades: procedimientos operativos de emergencias; simulacros en materia de seguridad física; programas de adquisición y asignación de recursos, de modernización tecnológica y de profesionalización del personal; elaborar mecanismos de coordinación; y proponer y revisar elementos de evaluación y control del sistema así como de indicadores del desempeño del sistema. Está a su cargo también la coordinación de la respuesta ante los eventos por conducto del elemento de ejecución, así como coordinar las actividades no directas de fortalecimiento a la capacidad disuasiva y preventiva con los responsables de mantenimiento, seguridad industrial o con quien corresponda.

Estas actividades buscan lograr el objetivo del sistema desde varias perspectivas, no sólo basadas en la capacidad tecnológica, a través de dotar al SSF de mayor capacidad para dar una respuesta que reduzca las pérdidas, fortalezca la capacidad de supervivencia y mantenga la continuidad operativa de la organización.

BIBLIOGRAFÍA

[1] Ackoff, Russell [1981], *Rediseñando el Futuro,* Ed. Limusa, México.

[2] Ackoff, Russell [1999], *Un Concepto de Planeación de Empresas*, Ed. Limusa.

[3] Ackoff, Russell [2001], *Guía breve de la Planeación Interactiva y el Diseño Idealizado*.

[4] Anderson, M. y P. Woodrow [1989], *Rising from the Ashes: Development Strategies in Times of Disaster*, Westview Press/UNESCO, Paris.

[5] Alarcón Olguín, Víctor y Bermúdez, Ubléster Damián (1988). *Orden jurídico y seguridad nacional*. Crítica jurídica. N° 9. Puebla: Universidad Autónoma de Puebla.

[6] Balducelli C., Bologna S., Dipoppa G. y Vicoli G. [2003], *Lecture notes in Computer Science*, Dependability and Survivability of Large Complex Critical Infrastructures, Vol. 2788, pp. 342-353.

[7] Banfield, Edward C. [1959], *International Social Science Journal*, Ends and Means in Planning, Vol. XI, No.3.

[8] Campelo, De Melo María Ángela y G. A. Miguel Domingo [2004], *Anais da III Conferencia Internacional de Pesquisa em Emprendedorismo na América Latina (CIPEAL),* Planificación interorganizacional y desarrollo emprendedor: un caso de estudio, Rio de Janeiro.

[9] Cardona, Arboleda Omar Darío [2001], *Estimación holística del riesgo sísmico utilizando sistemas dinámicos complejos*, Tesis de doctorado, Universidad Politécnica de Cataluña.

[10] Checkland, Peter B. [1999], *Systems thinking, System Practice*, Ed. Wiley, UK.

[11] Comité Conjunto de Estándares Australia / Nueva Zelanda [1999], *Administración de riesgos,* Estándar AS/NZS 4360:1999.

[12] Cordero, Mayorga Alfonso [2010], *Notas sobre el Curso de Seguridad Física*.

[13] Cruz, Serrano Noé y Otero Silvia [2007], *Pemex admite que es frágil ante sabotajes,* Nota periodística, El Universal, en http://www.eluniversal.com.mx/nacion/154143.html

[14] Delgado, R. y Serna N. [1977], *Cuadernos Prospectivos (11-A)*, Procedimientos de Planeación Normativa, Fundación Javier Barros Sierra, México.

[15] Diccionario de la Real Academia Española, en línea en http://www.rae.es/rae.html

[16] Diu, Antonio [2007], *Lectura en el Instituto de Ingeniería y Tecnología (IET)*, Large and Complex Critical Infrastructure Protection (LCCIP).

[17] Emery, F. E. y Trist E. L. [1965], *Human Relations*, The causal textures of organizations environments, Vol. 18, pp. 21-32.

[18] Fuentes, Zenón Arturo [2000], *Cuadernos de Planeación y Sistemas*, Metodología de la Planeación Normativa, DEPFI, UNAM, México.

[19] Gelman O., Negroe G. [1982], *La planeación como un proceso básico en la conducción*. Revista de la *Academia Nacional de Ingeniería, México, Jun, 1982, Vol 1, No. 4, 253-270*

[20] González, Miguel Ángel [2010], *Ajse World (Revista de Seguridad)*, Decálogo de Principios Fundamentales en la Protección de Instalaciones, España.

[21] Instituto Nacional de Administración Pública (I.N.A.P.) [2005], *IV Curso de directivos públicos locales*, Gestión de riesgos, México.

[22] Kelling, G. L. y Wilson James Q [1982], *Broken Windows.*

[23] Lynn, García Mary [2001], *The design and Evaluation of Physical Protection Systems*, Ed. Butterworth-Heinemann, USA.

[24] Mitroff, Ian I. y Alpaslan Murat C. [2003], *Harvard Business Review,* Preparing for evil, pp. 109.115.

[25] Ozbekhan, Hasan [1977], *Philosophical Transactions of Royal Society publishing*, The Future of Paris: A Systems Study in Strategic Urban Planning. Vol. 287, No. 1346, pp. 523-544.

[26] Petróleos Mexicanos [2005], *Plan Rector de Seguridad Física de Petróleos Mexicanos y Organismos Subsidiarios*, México.

[27] Portal de PEMEX *Petroquímica, www.ptq.**pemex**.com/*.

[28] Portal de la Secretaría de la Seguridad Pública, *www.ssp.gob.mx/*.

[29] Programa Sectorial de Desarrollo Económico 2005-2010, Secretaria de Desarrollo Económico, Gobierno del Estado de Veracruz.

[30] Rodríguez, Contreras Carlos [1998], *La conferencia de búsqueda en el contexto organizacional mexicano: reunión de reflexión y diseño,* Tesis de maestría, UASLP, México.

[31] Sánchez, Lara Benito [2007], *Notas del Curso de Enfoque de Sistemas*, Posgrado en Ingeniería, UNAM.

[32] Velazco, Gamboa Emilio [2004], *Fundamentos de la Seguridad Privada: Una Percepción Criminológica,* Revista en línea Latino Seguridad, en http://www.latinoseguridad.com/LatinoSeguridad/SPX/SPX30.shtml

[33] Zavaleta, Betancourt José Alfredo [2010], *La seguridad pública en Veracruz*, Nota periodística en Servicios Profesionales de Información, http://www.spiveracruz.info