VNIVERSIDAD NACIONAL AVTNOMA DE MEXICO

PROGRAMA DE MAESTRIA Y DOCTRADO
EN INGENIERIA

FACVLTAD DE INGENIERIA

EVALUACIÓN DE RIESGOS EN PROYECTOS DE SEGURIDAD FÍSICA: UNA PROPUESTA METODOLÓGICA PARA EL CENTRO DE INVESTIGACIÓN Y DESARROLLO DE TECNOLOGÍA PARA SEGURIDAD DE LA UNAM

TESIS

QUE PARA OBTENER EL GRADO DE

MAESTRO EN INGENIERÍA

INGENIERÍA DE SISTEMAS – PLANEACIÓN

PRESENTA:

ING. JUAN JACOBO SALAZAR AGUIRRE

TUTOR:

DR. BENITO SÁNCHEZ LARA

2011

JURADO ASIGNADO

Presidente:	**Dr. Sánchez Guerreo Gabriel De Las Nieves**
Secretario:	**Dr. Bautista Godínez Tomás**
Vocal:	**Dr. Sánchez Lara Benito**
1er Suplente:	**Dra. Monroy León Cozumel Allanec**
2º Suplente:	**M.I. Soler Anguiano Francisca Irene**

Lugar donde se realizó la tesis:

CIUDAD UNIVERSITARIA, MÉXICO D.F.

TUTOR DE LA TESIS

DR. BENITO SÁNCHEZ LARA

_____

FIRMA

Agradecimientos

A Dios por regalarme la oportunidad de compartir este tiempo y espacio con quienes han hecho posible este éxito académico.

A mi querida UNAM, por permitirme ser parte de su inmensa familia; en especial a la Facultad de Ingeniería, que me ha formado como profesionista.

A mis sinodales: la Dra. Cozumel Allanec Monroy León, la Mtra. Francisca Irene Soler Anguiano, el Dr. Tomás Bautista Godínez y el Dr. Gabriel de las Nieves Sánchez Guerrero; por sus aportes para mejorar la tesis.

A mi tutor, el Dr. Benito Sánchez Lara, por guiar la elaboración de este trabajo, por alentar en todo momento su culminación, por su dedicación y gran paciencia, en realidad las palabras no alcanzan para agradecerle todo el apoyo que mostró hacia mi persona en este logro profesional.

Al CONACYT, por la beca que me otorgó para realizar mis estudios de maestría

Al CIDETES, y al M.I. Alberto Lepe Zuñiga, por permitirme desarrollar este trabajo de investigación.

Dedicatorias

A mis padres, por el inmenso amor con el que a cada momento me han impulsado para alcanzar esta meta. A Alicia Aguirre, mi madre, el pilar y gran motor de la familia, quien me ha guiado y acompañado en cada peldaño escalado, siendo mi soporte. A mi padre, Juan Salazar, cuyos consejos me han permitido superar adversidades y enfocarme en una superación constante. Mis respetos y admiración.

A Cristina Cortés, esposa y amiga, quien me ha acompañado en esta travesía mostrando su amor y comprensión, en los momentos difíciles. A ese pequeño engrane que mueve todo mi ser, mi hija: Alexa Berenice, quien con una sola sonrisa cambia el rumbo de la vida. Las amo.

A quienes desde ese lugar especial me acompañan en un nuevo triunfo: María Castañeda, Claudio Aguirre, Dolores Casas y José Salazar.

A mis hermanos de alma: Mirna Morones y Ricardo Briceño (ahora compadres), Erika Villalba, Diana Gudiño, Joseba Andoni, Luis Méndez y Enrique Espinoza, a quienes me une un lazo que va más allá de la amistad.

A mis hermanos de maestría: Alberto Sánchez, Erik Bárcenas y Ricardo Gines, con quienes he compartido esta aventura académica, algunas desventuras profesionales, pero sobre todo, momentos alegres, motivo de nuestra gran amistad.

A las familias Cortés Miranda, López Aguirre, Aguirre Medrano, Salazar Tello y García Rojas quienes con sus comentarios siempre me han demostrado su interés y aprecio.

¡GOYA! ¡GOYA! ¡CACHUN CACHUN RA RA! ¡CACHUN CACHUN RA RA! ¡GOYA! ¡UNIVERSIDAD!

Índice de contenido

Índice de tablas

Índice de figuras

Cuadros comparativos

Resumen

Actualmente la seguridad es un tema de interés general para todo el mundo, eventos relacionados con el terrorismo o el narcotráfico, a nivel mundial y nacional, han transformado su percepción y es visualizada como un problema de gran magnitud, del cual se buscan permanentemente soluciones, entre las que destacan el uso de tecnología. Bajo este contexto la Universidad Nacional Autónoma de México, a través de su Centro de Investigación y Desarrollo de Tecnología para Seguridad, persigue el objetivo de dar solución a problemas relacionados con los riesgos asociados a eventos no deseados de seguridad y con el análisis, obtención, selección, adquisición y desarrollo de tecnología como respuesta, esto a través de proyectos de seguridad física, para los cuales, la evaluación de riesgos representa un insumo importante que es obtenido de una metodología de desarrollo propio. En este trabajo de investigación, con la finalidad de contar con una metodología sólida, robustecida en su teoría y práctica como instrumento de planeación, cuyos resultados proporcionen sustento a la toma de decisiones orientadas a la reducción y mitigación del riesgo, dicha metodología fue tomada como objeto de estudio. Se realizó un análisis comparativo tomando como referencia otras metodologías alternas de la misma naturaleza, y utilizando las bases cognoscitivas del enfoque sistémico y cibernético, al proceso de conducción, a la planeación como un proceso básico en la conducción y a la Investigación Interdisciplinaria de Desastres, se establecieron propuestas expresadas en adecuaciones y recomendaciones a nivel estructural y funcional. De esta manera, se re-estructuró la metodología en una etapa de preparación y siete etapas principales, que son: caracterización del sistema afectable; caracterización del sistema perturbador; caracterización del sistema de gestión; evaluación del riesgo; propuestas para el tratamiento del riesgo; construcción del plan para la reducción de riesgos; y control.

Abstract

Today the security issue is a topic of interest for everyone, the global and national events, related to terrorism or drug trafficking, have transformed their perception and it´s viewed as a major problem, which is constantly looking for solutions, emphasizing the use of technology. In this context the National Autonomous University of Mexico, through its Centre for Research and Development of Technology for Security aims to provide solutions to problems related to the risks associated with unwanted security events and analysis, procurement, selection, acquisition and development of technology as an answer, through physical security for which the risk assessment represents an important input that is derived from a methodology developed in-house. In this research, in order to have a solid methodology, strengthened in its theory and practice as an instrument for planning whose results provide support to the decision-making aimed at reducing and mitigating risk, this methodology was taken as object of study. A comparative analysis was performed with reference to other alternative methodologies of the same nature, and using the cognitive basis of systemic and cyber approach, the process management, the planning as a basic process in the process management, and the Interdisciplinary Research of Disaster, set out proposals expressed in adaptations and recommendations at the structural and functional level. Thus, it restructured the methodology in a preparation stage and seven main stages, namely: characterization of the affected system; characterization of the perturbed system; characterization of the management system; risk assessment; proposed for the management of risk; construction plan for risk reduction; and control.

Introducción

El tema de seguridad, hoy en día, representa un interés generalizado a nivel mundial y nacional, los actos terroristas perpetrados a las torres gemelas el 11 de septiembre de 2001 en Estados Unidos, o el fenómeno desencadenado por el narcotráfico en el país, son hechos que han marcado la forma en que es percibido, tomando relevancia como un problema que crece de forma importante. Por ejemplo, internacionalmente se han tomado un sin número de medidas de prevención en aeropuertos, como respuesta a este problema, en este sentido, el papel de la tecnología en materia de seguridad es un aspecto de llamar la atención, puesto que empresas que se dedican a su desarrollo y comercialización han sacado provecho de ello. En México, se ha creado una necesidad por este tipo de tecnologías y en general por los servicios de seguridad.

Bajo este contexto, en 2005 el Centro de Investigación y Desarrollo de Tecnología para Seguridad (CIDETES) fue creado por la Universidad Nacional Autónoma de México con el objetivo de aportar soluciones prácticas en materia de seguridad física dirigidas a las diferentes entidades gubernamentales, así como a la industria pública y privada del país; la reducción de riesgos asociados eventos no deseados de seguridad y el análisis, obtención, selección, adquisición y desarrollo de tecnología como respuesta, a través de proyectos de seguridad física, representan entonces, su principal actividad, la cual encuentra en la evaluación de riesgos, su principal insumo.

Las metodologías de evaluación de riesgos representan una herramienta necesaria en el ámbito de la seguridad física, puesto que permiten identificar y determinar los elementos relacionados con los eventos no deseados de seguridad, como son las amenazas, las vulnerabilidades, así como los posibles daños que generan impactos de diversa naturaleza, en un determinado sistema, y con base en ello, establecer las medidas que permitan reducir las condiciones que favorecen a esos elementos. Es por esta razón que el CIDETES ha desarrollado una metodología como producto de la necesidad por contar con una herramienta que permita diagnosticar y evaluar el riesgo, y que establezca además, un puente hacia las propuestas tecnológicas y normativas que hagan posible su reducción.

Por otro lado los proyectos en los que participa el CIDETES, dirigidos a importantes empresas transnacionales, exigen instrumentos de trabajo sólidos, es por ello que surge la inquietud de revisar su metodología para evaluación de riesgos, con la finalidad de robustecerla en su teoría y práctica como instrumento de planeación, cuyos resultados proporcionen sustento a la toma de decisiones orientadas a la reducción y mitigación del riesgo. Una observación en este punto, es que la reducción de riesgos, puede ser abordada como un problema en el que se desea pasar de un estado actual, en el que existen ciertas condiciones que caracterizan a un sistema con riesgo, a uno deseado, en el que se reducen dichas condiciones, auxiliándose para su solución, en la planeación.

Para este fin, el presente trabajo de investigación se estructura en cuatro capítulos a través de los cuales aborda los tópicos necesarios. En el capítulo I, se establecen los antecedentes que permiten construir al objeto de estudio, en este caso, la metodología CIDETES.

El capítulo II, aborda los conceptos de la Investigación Interdisciplinaria de Desastres, utilizada como marco teórico para la evaluación de riesgos, ya que al tomar como fundamento las bases cognoscitivas proporcionadas por el enfoque sistémico y cibernético, permite conceptualizar a los elementos asociados a eventos no deseados de seguridad, de esta manera a través del proceso de conducción es posible ubicar al sistema perturbador, que es capaz de originar calamidades (amenazas), al sistema afectable, en el que pueden materializarse los desastres, y al sistema regulador, que busca reducir los riesgos, o bien, restablecer la situación normal del sistema afectable. Otro aspecto abordado, es el papel que la planeación desempeña, como instrumento de apoyo al proceso de conducción en la toma de decisiones, a través de cuatro etapas interrelacionadas: diagnóstico, prescripción, instrumentación y control. Así, estos rubros permiten: sentar las bases teóricas que fortalecen a la metodología; enmarcarla como un instrumento de planeación; y establecer los criterios de comparación que se utilizarán en el capítulo III.

Para alcanzar el objetivo de este trabajo de investigación, en el capítulo III se caracterizan estructural y funcionalmente tres metodologías, además de la utilizada por el CIDETES: la metodología SVA desarrollada por el American Petroleum Institute (API) y la National Petrochemical and Refiners Association (NPRA), para la industria petrolera y petroquímica; la metodología MOSLER; y la metodología RAM desarrollada por los laboratorios Nacionales Sandia. Posteriormente, con la finalidad de establecer sus diferencias y similitudes, se realiza un análisis comparativo, con base en los criterios: estructura, funcionalidad, evaluación de riesgo y, alcances y resultados. Y al final del capítulo, se establecen las propuestas valoradas como elementos que enriquecen y fortalecen a la metodología CIDETES.

Finalmente en el capítulo IV se presentan los resultados y conclusiones que abarcan 5 puntos: el análisis comparativo entre las metodologías; las fortalezas y debilidades de la metodología CIDETES; las propuestas de adecuación a la metodología CIDETES; la forma en que la metodología CIDETES es robustecida en su teórica y práctica; y sobre el alcance del trabajo investigación.

ANÁLISIS DE RIESGOS EN PROYECTOS DE SEGURIDAD FÍSICA

CAPÍTULO 1

1.1 Situación actual de la seguridad en México

A nivel mundial, el evento que ha marcado la pauta en la percepción sobre seguridad, es el atentado a las torres gemelas del 11 de septiembre de 2001 en Estados Unidos, debido al cual comenzaron a establecerse una serie de medidas, sobre todo en aeropuertos de todo el mundo. Ahora bien, después de esa fecha, el terrorismo tomó relevancia en todos los planos de seguridad, aunque existían antecedentes como los atentados de la ETA (Euskadi Ta Askatasuna) en España o la propia Al Qaeda en Afganistán, es a partir de esa fecha que se crea un parte aguas en este tema. En el plano nacional, las múltiples ejecuciones del narcotráfico, secuestros, así como escándalos por corrupción, han llevado a considerar a México como un "Estado fallido" o fracasado, al borde del caos, en el cual el gobierno al perder el control, utiliza las fuerzas armadas como último recurso. Sin embargo, analistas mexicanos piensan que en realidad se trata de un "Estado parcialmente fallido", en el que sólo las instituciones encargadas de la seguridad son las que han fracasado (Benitez Manaut, 2009).

El concepto de seguridad, en la actualidad es ampliado con una transición sobre su objetivo, dejando de estar centrado exclusivamente en la defensa territorial y las instituciones del estado (seguridad nacional), para abarcar también a la sociedad e individuos (seguridad humana/seguridad ciudadana) (Chanona, 2007). Es una de las funciones principales del Estado, representa un aspecto crítico y ocupa un lugar de interés nacional; es abordada desde muchas perspectivas, la principal y que en es cada vez más representativa ante ciudadanos, empresas y autoridades, es que se trata de un problema que toma forma no solo a través de la alta incidencia con una delincuencia cada vez más organizada y violenta, sino además con una respuesta evidentemente insuficiente por parte del estado, y que aunado a las múltiples relaciones de corrupción entre autoridades y delincuentes, ha crecido importantemente con el paso del tiempo.

La sociedad, al ser una de las partes más vulnerables, ha demandado una participación más activa, creando diversas asociaciones e institutos que brindan apoyo en materia de seguridad, como son: el Colectivo de Análisis de la Seguridad con Democracia (CASEDE); el Sistema de Observación para la Seguridad Ciudadana (SOS); México Unido Contra la Delincuencia (MUCD); o el Instituto Ciudadano de Estudios Sobre la Inseguridad (ICESI); entre otros. Este último, con apoyo del Instituto Nacional de Estadística y Geografía (INEGI) realizó la sexta Encuesta Nacional Sobre Inseguridad (ENSI-6) en las 32 entidades federativas y 16 zonas urbanas (ciudades o zonas metropolitanas) [1].

[1] Se omitieron los resultados correspondientes a los estados de Tabasco y Tamaulipas, y a las ciudades de Villahermosa y Nuevo Laredo, al presentarse condiciones irregulares en el levantamiento de información, relacionadas con la seguridad de los encuestadores. Las 16 zonas fueron: 1) Acapulco, Guerrero; 2) Cancún, Quintana Roo; 3) Ciudad Juárez, Chihuahua; 4) Chihuahua, Chihuahua; 5) Cuernavaca, Morelos; 6) Culiacán, Sinaloa; 7) Distrito Federal; 8) Guadalajara, Jalisco; 9) Monterrey, Nuevo León; 10) Mexicali, Baja California; 11) Nuevo Laredo, Tamaulipas; 12) Oaxaca, Oaxaca; 13) Tijuana, Baja California; 14) Toluca, Estado México; 15) Villahermosa, Tabasco;16) Zona conurbada al DF del Edo. México.

Esta encuesta, con base en delitos del fuero común (95% del total de la delincuencia) cometidos en 2008, trata de estimar: el total de personas que fueron víctimas de uno o varios delitos (prevalencia delictiva), que se expresa como un porcentaje de las víctimas; el total de los delitos cometidos a dichas personas (incidencia delictiva), que se expresa en tasas por cada 100 mil habitantes; la tasa de delitos no denunciados y no registrados; las características y magnitud de la victimización; así como la percepción de las personas sobre la inseguridad y la forma en la que actúan las autoridades[2]. Algunos de los resultados que arrojó esta encuestan son descritos en los siguientes párrafos.

Uno de los principales resultados de la encuesta, es el termómetro del delito o índice nacional de inseguridad, que se obtiene de tres indicadores: la incidencia delictiva – tomada de la ENSI – , el porcentaje de delitos cometidos a mano armada – tomada de la ENSI – y la tasa de homicidios dolosos en 2008 — tomada de la estadística oficial —. En este se muestra a Chihuahua como la entidad más insegura, seguida de Sinaloa, Baja California, el Distrito Federal y Guerrero, debido principalmente a las cifras referentes a los homicidios dolosos que han tenido un ascenso notable en sólo un año, colocando a las primeras dos, en rangos similares de países como Sudáfrica o Venezuela, con tasas muy altas de homicidios. Por otra parte la entidad más segura del país sigue siendo Yucatán, presentando cifras cercanas a las de las naciones más seguras del mundo. En la figura 1 se muestra esta gráfica, presentando la cifra obtenida para 2008 y entre paréntesis la del estudio anterior, correspondientes 2007.

De acuerdo con el Sistema Nacional de Seguridad Pública, los estados de Sinaloa, Chihuahua, Guerrero, Durango y Baja California presentan graves tasas de homicidios dolosos por cada 100 mil habitantes: 43.7, 42.1, 30.2, 27.8 y 27.7 respectivamente.

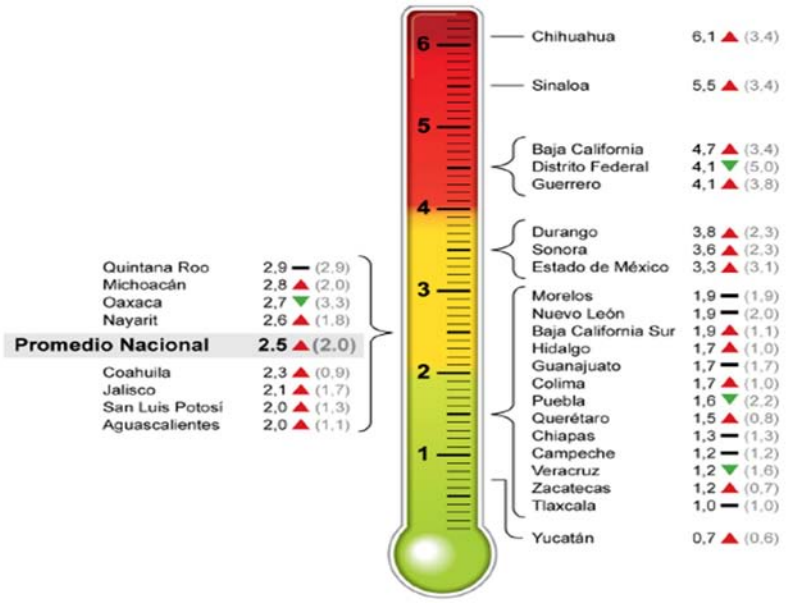

Figura 1. Termómetro del delito o índice nacional de inseguridad.
Fuente: Encuesta ENSI-6 2009

[2] La encuesta ENSI-6 fue llevada a cabo en marzo de 2009 con un periodo de referencia del 1 de enero y el 31 de diciembre.

Con relación a la prevalencia, las entidades federativas de Guanajuato, Nuevo León y Nayarit se encuentran dentro del promedio nacional (11%); el Distrito Federal, Aguascalientes, Sonora, Estado de México, Coahuila, Baja California, Chihuahua, Michoacán, Colima, Jalisco, Baja California Sur, Querétaro y Quintana Roo, se encuentran por encima del promedio nacional, siendo las dos primeras las de mayor prevalencia (19% y 16% respectivamente); Aguascalientes, Sonora, Coahuila, Michoacán, Colima, Baja California Sur, Querétaro, Nayarit, Hidalgo y Zacatecas presentaron un incremento en este rubro, destacándose las primeras tres, que no habían figurado entre las más altas, también cabe mencionar que ninguna presentó un decremento en sus cifras respecto a las encuestas anteriores de 2004 y 2007. Por otra parte, todas las zonas urbanas o metropolitanas se encuentran por encima del promedio nacional, siendo la ciudad de Chihuahua la de mayor prevalencia (20%), creciendo significativamente en 10 unidades porcentuales con respecto a la encuesta de 2005, contrario al comportamiento del Distrito Federal[3] y la Ciudad de México[4] que presentaron un decremento de 10 y 5 unidades porcentuales respectivamente. Algunos datos referentes a la prevalencia son:

- A nivel nacional el 13.1% de los hogares presentaron víctimas de algún delito, mientras que en las zonas metropolitanas fue de un 21%;

- El 11.46% de la población adulta fue víctima de algún delito, a nivel nacional, y el 17% en las zonas metropolitanas;

- Con relación al entorno de los encuestados el 22% aseguran la existencia de narco-tiendas cerca de su hogar, a nivel nacional, y un 32% en zonas metropolitanas, mientras que el 31%, a nivel nacional, asegura que se dan disparos de arma de fuego cerca de su hogar, y un 41% en las zonas metropolitanas. Este dato proporciona una idea de la variación en la victimización, ya que el vivir en estos entornos aumenta la probabilidad de ser víctima de algún delito. De esta manera, el 19.5% de las personas que afirmaron la existencia de narco-tiendas fueron víctimas, mientras que sólo el 8.9% de las que aseguraron lo contrario lo fueron; por otro lado el 18% de las personas que viven en lugares con disparos de fuego fueron víctimas y sólo el 8.5% de las que no viven en estos lugares lo fueron;

- Los delitos en agravio de personas que se cometen principalmente son: robo a transeúnte – delito con mayor prevalencia –, robo relacionado a cajero, secuestro, lesiones, sexuales, otros delitos, fraude y extorsión;

- Los delitos que afectan al hogar que se cometen principalmente son: robo parcial de vehículos (autopartes, herramientas, etc.) – delito con mayor prevalencia –, robo de vehículos y robo a casa habitación.

[3] Analizado como zona urbana o metropolitana.

[4] Para efectos de esta encuesta, la Ciudad de México es considerada como el Distrito Federal en conjunto con la zona conurbada del estado de México.

En lo referente a la incidencia delictiva se mostró primeramente la tasa general de incidencia, en la que se expresa por cada 100 mil habitantes, el número de delitos ocurridos con respecto a la población total del país, estado o ciudad, según sea el caso de análisis. En esta tasa se encontró un incremento significativo entre 2007 y 2008 en estados que tradicionalmente presentaban niveles de delincuencia bajos o moderados como: Aguascalientes, Baja California Sur, Coahuila, Colima, Hidalgo, Michoacán, Nayarit, Querétaro, Sinaloa, Sonora y Zacatecas; en el otro extremo, las entidades que normalmente presentan nivel altos se han mantenido altas pero estables, como son: el Distrito Federal y el Estado de México. En 2007 la tasa de incidencia del Distrito Federal no era comparable a la de ningún otro estado, para 2008 Chihuahua, Mexicali y la zona del Estado de México conurbada con el D.F. se encuentran en los mismos niveles, por arriba de los 20,000 delitos; por otro lado las ciudades de menor incidencia fueron Cuernavaca y Culiacán con 11,707 y 12,341 delitos respectivamente, valores que se ubican dentro del rango promedio nacional, mientras que el resto de las ciudades se encuentra por arriba del promedio.

Tomando en cuenta los delitos de robo a transeúnte, robo relacionado a cajeros, otros robos, secuestro, lesiones, sexuales, otros delitos, fraude y extorsión, se construyó la tasa diferenciada de delitos en agravio a las personas. En esta tasa se indica el número de delitos por cada 100 mil habitantes, encontrando un incremento notable en más del 300% en estados como Coahuila, cuya tasa subió de 2,027 a 8,201, o Colima que registró un cambio en su tasa de 1,413 a 6,379, sin embargo, la entidad que presentó una mayor incidencia a nivel nacional es el Distrito Federal, a pesar de que su tasa descendió de 21,405 a 16,840; en contraparte la entidad con la tasa más baja es Zacatecas con 1,153; el análisis de las zonas metropolitanas reveló que el Distrito Federal, la zona conurbada del estado de México y la conjunción de ambas zonas tienen las tasas más altas superando los 15,000 delitos, mientras que la de menor tasa es Monterrey con 4,950 delitos. Cabe mencionar que ningún estado sufrió un cambio a la baja. A nivel nacional y metropolitano, el delito de mayor incidencia fue el robo a transeúnte, aunque descendió de 5,932 a 4,092, en el primero y de 10,023 a 7,715 en el segundo, siguiéndole la extorsión con 1,291 y 1,325 respectivamente, de los cuales el 80% fue vía telefónica, siendo un delito que impacta de forma importante en la población, al igual que lo es el secuestro y secuestro exprés, que se presentaron en un promedio de 76 secuestros de cualquier tipo.

La otra tasa que se construyó, fue la tasa de delitos al hogar, que indica el número de delitos a dicho patrimonio por cada 1,000 hogares, considerando el robo total de vehículo, robo parcial de vehículo y robo a casa habitación. Aquí se estimaron 137 delitos a nivel nacional, encontrando un incremento importante entre 2007 y 2008, desde un 90% hasta un 95% en: Aguascalientes, Baja California Sur, Coahuila, Guanajuato, Hidalgo, Michoacán, Querétaro, Sonora y Zacatecas, siendo Aguascalientes la entidad con mayor incidencia con 301.7 delitos. En lo referente a las zonas metropolitanas se estimaron 183.1 delitos: Chihuahua, Guadalajara, Mexicali, Tijuana, Ciudad Juárez, Monterrey y el Distrito Federal presentan una incidencia mayor a esta cifra, siendo la ciudad de Chihuahua la de mayor incidencia con 306.9 delitos. Tanto a nivel nacional como metropolitano el delito de mayor incidencia fue el robo parcial de vehículo con 95 y 136.4 respectivamente. El lugar con mayor incidencia en donde ocurrieron delitos fue la vía pública con un 52% a nivel nacional y 58% a nivel metropolitano, seguido del hogar con un 28% y un 23% respectivamente.

La percepción que se tiene sobre la inseguridad es un factor que proporciona una idea del impacto que genera este problema en la población. De acuerdo a la consulta SIMO-CASEDE[5], la población consideró que las principales amenazas internas que atentan contra la seguridad del país son: la delincuencia organizada (33.9%), la inseguridad pública (18.5%), los grupos armados (9.6%), la corrupción (7.5%), el terrorismo (7.3%) y el secuestro (5.8%); mientras que las principales amenazas externas consideradas son: el tráfico de drogas (49.4%), el tráfico de armas (17.2%) y una crisis financiera internacional (10.6%).

Siguiendo con la encuesta ENSI-6 se encontró que en promedio, un 65% de la población a nivel nacional se siente insegura en su estado, y un 49% en su municipio o delegación, además un 58.8% considera que los delitos en su municipio o delegación aumentaron, lo que ha llevado a que el 72% de las personas, en promedio, haya dejado de hacer actividades como permitir que sus hijos menores salgan, usar joyas, salir de noche, llevar tarjetas de crédito y/o débito, o incluso, salir a caminar. Con relación a los lugares en los que se sienten más inseguros, se encuentra el transporte público, con un 64.5%, y en general en la calle, con un 61.6%, por otro lado, aunque el hogar es el lugar en dónde se sienten menos inseguros, con un 12.4%, en el 45% de éstos se tomaron medidas de seguridad. El Distrito Federal y Chihuahua son las entidades en las que sus habitantes se sienten más inseguros, siendo Chihuahua la que ha presentado un incremento importante respecto a la encuesta anterior.

De esta manera, la población se siente cada vez más desprotegida y ha perdido la confianza en la justicia, la policía y sus gobernantes, lo que ha provocado por un lado, que no se denuncien los delitos, y por otro, que se recurra cada vez más a la autoprotección, que se ha convertido en una necesidad, en la que diversas empresas han sacado provecho. Dicho en otras palabras, la seguridad en México, representa un mercado que ha crecido notoriamente, en el que se ofrecen diversos servicios y productos que buscan reducir este problema. Algunos datos que refuerzan esta idea indican que: para 2007, en la última década, según cifras del Sistema Nacional de Seguridad Pública, el mercado de la seguridad privada creció un 400% [6]; por su parte el Consejo Nacional de Seguridad Privada estimó que en 2010 existían más de 10,000 empresas de seguridad privada en el país, las cuales facturaron alrededor de 28,000 millones de pesos al año, aunque sólo aproximadamente el 20% se encontraban registradas ante la Secretaria de Seguridad Pública Federal, y de ésas, solo el 2.5% contaban con alguna certificación, mientras que el resto ofrecían sus servicios de forma irregular [7].

Estas empresas ofrecen diversos productos y servicios entre los que destacan:

- Guardias de seguridad. De acuerdo con la Sociedad Mexicana de Guardaespaldas, en el país hay aproximadamente 18,000 escoltas y 127,000 guardias intramuros registrados ante las autoridades federales[8]; el Consejo Nacional de Seguridad Privada afirma que

[5] Encuesta sobre Seguridad Nacional realizada por "Sistemas de Inteligencia en Mercado y Opinión" en conjunto con el "Colectivo de Análisis de la Seguridad con Democracia" realizada entre septiembre de 2008 y agosto de 2009"

[6] Tomado del Plan Nacional de Desarrollo 2007-2012, p. 73

[7] Tomado de la revista Proceso, 15 julio de 2010, http://www.proceso.com.mx/rv/modHome/detalleExclusiva/81429

[8] Tomado del periódico "El Universal", lunes 24 de mayo de 2010, http://www.eluniversal.com.mx/nacion/vi_177912.html

existen en promedio 400,000 elementos que desempeñan esta actividad, ofreciendo entre los servicios más demandados, la custodia en el traslado de valores y mercancía, y el uso de tecnología para monitorización[9];

- Ropa blindada. En México se estableció la primer empresa dedicada a la fabricación de ropa blindada a nivel mundial, el dueño y diseñador de estas prendas asegura que sus ventas se han incrementado de forma importante principalmente en el sector privado.

- Vehículos blindados. México ocupa el primer lugar en Latinoamérica en blindaje de vehículos [10];

- Diversos equipos electrónicos. Entre los que se pueden mencionar los microchips de localización, alarmas, cámaras, equipos de control de acceso, equipos de radiocomunicación, equipos de detección de intrusos, entre otros.

En este contexto la Universidad Nacional Autónoma de México, como una institución con gran influencia en el desarrollo del país, ha fomentado una participación más activa en relación con el tema de seguridad, ya sea fuera de la UNAM, formando parte en la creación y funcionamiento del ICESI, o bien, dentro, creando el Centro de Investigación y Desarrollo de Tecnología para Seguridad (CIDETES), que desde de 2005 tiene la importante tarea de generar investigación y desarrollo de tecnología en materia de seguridad.

1.2. El Centro de Investigación y Desarrollo Tecnológico para Seguridad (CIDETES)

El Centro de Investigación y Desarrollo Tecnológico para Seguridad (CIDETES), nació como un compromiso de la UNAM por aportar soluciones prácticas en materia de seguridad. De esta manera el 24 de enero de 2005, después de tres años de haber realizado trabajos de investigación y desarrollo de tecnologías para instituciones públicas y privadas, se creó el CIDETES como un órgano adscrito a la Secretaría de Posgrado e Investigación de la Facultad de Ingeniería, con el propósito de apoyar a las entidades federativas del país en sus tres niveles (Federal, Estatal y Municipal), así como a la industria pública, privada y social, en lo relacionado con el análisis, obtención, selección, adquisición y desarrollo de tecnología en materia de seguridad, además de proporcionar asesoría sólida y transparente, así como formar cuadros de recursos humanos especializados que cubran las necesidades de dichas entidades o sectores.

La determinación para la creación del centro recae en el hecho de que la inseguridad es uno de los problemas nacionales más importantes, sin menospreciar la situación internacional que exige una mayor atención a esta problemática en aeropuertos, puertos y zonas fronterizas, y en donde además el uso de tecnologías ha tomado gran relevancia, por ende, la importancia de desarrollar

[9] Tomado de la revista en América, número 61, p 72
[10] Tomado del periódico "El Universal" , miércoles 26 de mayo de 2010, http://www.eluniversal.com.mx/nacion/177956.html

tecnología, ya que en la actualidad, la mayoría proviene de otros países, y en consecuencia, es escaso el número de especialistas nacionales que la evalúan y emplean.

De acuerdo con lo anterior, el CIDETES tiene por objeto:

- Realizar estudios e investigaciones;
- Desarrollar soluciones tecnológicas;
- Formar y capacitar personal en materia de seguridad;
- Evaluar lo relacionado con las condiciones de seguridad en instalaciones;
- Documentar y recopilar información en la materia y;
- Difundir los trabajos de investigación de sus miembros.

La forma en la que lo realiza es a través de la participación, desarrollo o ejecución de proyectos, los cuales pueden ser patrocinados o propios, los patrocinados son aquellos en los cuales la UNAM recibe una remuneración económica a cambio, y los propios, aquellos subsidiados con los recursos del propio Centro. Los proyectos que se pueden promover son:

- Estudios e investigaciones;
- Soluciones tecnológicas;
- Servicios:
  - ✓ Formación y capacitación de personal en materia de seguridad;
  - ✓ Evaluaciones sobre condiciones de seguridad en instalaciones;
  - ✓ Opinión y evaluaciones técnicas sobre tecnologías;
  - ✓ Evaluación de confianza de personal.

Para que un proyecto patrocinado o propio pueda ser promovido por el CIDETES debe cumplir con al menos una de las siguientes características:

- Tener en su objetivo una connotación de Seguridad;
- Promoverse para un patrocinador relacionado con Seguridad;
- Que como consecuencia de su realización, el CIDETES incremente su acervo de habilidades y conocimiento en ciencias y tecnologías relacionadas con la Seguridad.

1.3 Conceptos Básicos en Proyectos de Seguridad Física

1.3.1 Riesgo

Antes de definir el concepto de riesgo resulta conveniente entender dos elementos asociados a este: las amenazas y la vulnerabilidad. Las amenazas son los posibles eventos, actos o condiciones (por sí mismos o encadenados a otros), que de suceder o materializarse, pueden ocasionar daños tangibles o intangibles a los elementos de un sistema físico, como pueden ser los activos (intelectuales y materiales) de una organización, impactando de tal manera que alteren o interrumpan sus objetivos. La vulnerabilidad, por su parte es la mayor o menor facilidad que

presenta el elemento de un sistema (que puede ser un activo de una organización, y que representa un blanco u objetivo) para la ocurrencia de una amenaza.

El riesgo se encuentra asociado prácticamente con todas las actividades que se pueden imaginar, cuando se habla de riesgo se hace referencia a la incertidumbre sobre una pérdida, a variaciones entre resultados esperados y los que se dan en forma real, a la probabilidad de que una amenaza se materialice y se tenga una perdida, o bien, a la posible aparición de un acontecimiento indeseable. A continuación se muestran algunas definiciones sobre el riesgo tomadas principalmente de estándares internacionales:

- ✓ ASIS internacional (2003) define el riesgo como la posibilidad de pérdida resultante de una amenaza, incidente de seguridad, o de un evento.

- ✓ De acuerdo con el estándar australiano AS/NZS 4360:2004 el riesgo es definido como la posibilidad de que ocurra algo (un evento) que tendrá un impacto sobre objetivos y que es medible en términos de consecuencias y probabilidades.

- ✓ En el vocabulario de la ISO/IEC Guide 73:2002 se define al riesgo como la combinación de la probabilidad de un evento y sus consecuencias, especificando que es usado solamente cuando al menos existe la posibilidad de consecuencias negativas, y que en algunas situaciones los riesgos surgen de la posibilidad de una desviación de un resultado o evento esperado. Por otro lado, en su versión 2009 (ISO 31000:2009) es definido como *el efecto de la incertidumbre sobre objetivos*, entendiendo como *efecto* a la desviación de lo esperado, ya sea positivo o negativo, caracterizándose por referirse a eventos potenciales, consecuencias o una combinación de ambas, y cómo pueden afectar al logro de objetivos; se expresa en términos de una combinación de consecuencias de un evento o cambio de circunstancias, y la probabilidad de ocurrencia.

- ✓ El Instituto Americano del Petróleo (2004), establece que el riesgo es una expresión de la probabilidad de que una amenaza ataque con éxito la vulnerabilidad de un activo crítico o conjunto de ellos, que sea su objetivo y cause un conjunto determinado de consecuencias, determinando dicha probabilidad en función del grado de atracción para el adversario, el grado de amenaza, y el grado de vulnerabilidad.

Estas definiciones nos muestran que el concepto de riesgo ha ido cambiando, ha pasado del evento al efecto, de considerarlo exclusivamente negativo a incluir la parte positiva, y se han creado debates sobre si se trata en realidad del efecto producido por la incertidumbre o si es en sí la incertidumbre, que de ocurrir tendría un efecto[11]. Para el CIDETES, dentro de sus proyectos de seguridad física, el riesgo se presenta cuando un elemento crítico (o conjunto de ellos) del sistema de estudio (pueden ser activos materiales o intelectuales de una empresa) se convierte en el objetivo de una amenaza, teniendo en ese momento un autor motivado, y que debido al menor o mayor grado de vulnerabilidad de dicho elemento, puede ser alcanzado y causar una

[11] Dr. David Hillson, Risk Doctor Briefing, diciembre 2009, http://www.risk-doctor.com/pdf-briefings/risk-doctor52s.pdf

serie de daños en el sistema que se ven reflejados en impactos económicos. Su cálculo resulta de la convolución de:

- La probabilidad de ocurrencia de la amenaza;
- El grado de atracción del activo por parte de la amenaza,
- El grado de vulnerabilidad del activo, y;
- Los impactos económicos que se pudieran presentar si la amena alcanza al activo.

1.3.2 Seguridad

Definir el concepto de seguridad es complejo debido al amplio carácter con que es manejado, es aplicado de diversas formas que dan lugar a diferentes ramas, como lo son la seguridad social, la seguridad industrial, la seguridad informática, la seguridad física, entre otras.

La palabra seguridad tiene diferentes acepciones, dependiendo del contexto en el que se utiliza, una percepción importante es lo que hace sentir: certeza, confianza, protección, o el saber que no se corre peligro. Etimológicamente, proviene del latín securitas, -atis, (seguro), y su adjetivo securus, -a, -um, formados por los vocablos: se (sin) y cura (cuidado), que significa "sin cuidado", "descuidado" o "despreocupado". Un elemento relevante para su conceptualización es su relación con el riesgo, la seguridad es inversamente proporcional al riesgo, a mayor seguridad menor riesgo y a menor seguridad mayor riesgo. En función del riesgo se puede considerar lo siguiente:

1. El riesgo se presenta bajo un conjunto de condiciones o circunstancias, internas o externas a un sistema, es decir, bajo una situación determinada;

2. El objetivo o propósito es reducir el riesgo que puede presentarse;

3. Para alcanzar dicho objetivo, se requiere un conjunto de pasos o acciones que permitan pasar de una situación actual (con un nivel determinado de riesgo) hacia una situación deseada (con una reducción de dicho nivel de riesgo), es decir, puede ser conceptualizada como un proceso;

4. Para llegar a la situación deseada, con una reducción en el riesgo, se generan programas, políticas, recomendaciones, etc.

De acuerdo con esto, la seguridad puede definirse como un proceso cuyo objetivo es la reducción de riesgos a los que está sujeto un determinado sistema debido a sus condiciones o circunstancias internas y externas, a través de la generación de estrategias, programas, políticas, uso de tecnologías, etc.

En estos términos, la reducción de riesgos se puede tratar como un problema, puesto que se tiene una discrepancia entre lo que se tiene y lo que se desea, buscando pasar de un extremo a otro haciendo uso eficiente de los recursos con los que se cuenten.

1.3.3 Seguridad Física

Existen dos conceptos que no pueden escaparse de una revisión: "Security" y "Safety". La idea básica de ambos es la protección de elementos o activos; security, se refiere a la protección contra incidentes previstos, deliberados y planeados, principalmente actos maliciosos o malintencionados, que a menudo son el resultado de una persona o grupo de personas, con el deseo de causar impactos o consecuencias en un sistema físico; mientras que safety, se refiere a la protección contra incidentes casuales como resultado de una o más coincidencias, que rara vez son maliciosos o malintencionados, y que a menudo son el resultado del comportamiento humano en combinación con el medio en el que se desenvuelve, sin un deseo de causar consecuencias; security, se enfoca en las amenazas (threats) que son rastreables a incidentes humanos, y que no siempre son visibles o tangibles, pueden ser internas o externas al sistema, estás últimas con un grado de incertidumbre sobre su manifestación y control, su relevancia confiere a un amplio rango de empresas o compañías; por su parte safety, se enfoca en los peligros (hazards), los cuales se manifiestan en el riesgo a la salud o el medio ambiente, siendo de carácter interno al sistema, observables y tangibles, siendo más relevante a cuestiones industriales.

La seguridad física o "security", se puede definir como aquella parte de la seguridad relacionada con las medidas diseñadas (como evitar accesos no autorizados a instalaciones o uso de equipo restringido) para proteger los elementos de un sistema físico (personal, instalaciones, materiales, documentos -activos tangibles e intangibles-) en contra de cualquier amenaza (espionaje, sabotaje, daños, robos, etc.) que tenga una probabilidad de ocurrencia y que comprometa su integridad, permitiendo de esta manera, reducir el riesgo al que está sujeto dicho sistema debido a las condiciones o circunstancias bajo las que se encuentra.

Un sistema se puede ver comprometido por un acto ilícito, de acuerdo con Cornish y Clarke (1986), cuando se presentan 3 factores o elementos:

1) Un autor motivado;
2) Un blanco o víctima accesible, y;
3) La ausencia de un vigilante capaz.

Como respuesta, se han desarrollado enfoques que buscan generar ambientes seguros. El "Crime Prevention Through Environmental Design" (CPTED), desarrollado por Ray Jeffery, criminalista de la Universidad Estatal de Miami, trata de reducir el crimen y el miedo al crimen al genera un clima de seguridad y tranquilidad, dentro de espacios diseñados bajo cinco premisas:

1) Vigilancia natural (diseñar una visibilidad adecuada);
2) Control natural de accesos (delimitar y conocer los puntos de acceso al espacio);
3) Reforzamiento del territorio (delinear de forma clara el espacio privado);
4) Mantenimiento del territorio (diseñar programas que mantengan la integridad del espacio), y;
5) Actividades de apoyo (de diversa naturaleza, que coadyuven a las anteriores).

Otro enfoque es el "Environmental design", desarrollado por Oscar Newman, el cual plantea la optimación de las oportunidades de disuasión y aprehensión al contar con:

1) Mayor tiempo de perpetración (provocar el retraso en la consumación del delito);
2) Mayor tiempo de detección (contar con los medios necesarios que faciliten la identificación de los actos delictivos);
3) Menor tiempo de reporte (contar con una observación global que permita percibir más detalles);
4) Menor tiempo de respuesta por las fuerzas de seguridad (planear las acciones a tomar).

Bajo este enfoque, un concepto importante es "Defensible Space", que hace referencia a un entorno cuyas características físicas (construcción y distribución de edificios) y funcionales permiten que el elemento humano sea pieza fundamental para garantizar su propia seguridad, a través de cuatro características:

1) Territorialidad (actitud de pertenencia y responsabilidad);
2) Vigilancia natural (capacidad de observación continuamente las áreas propias);
3) Imagen y medio (capacidad de diseñar una percepción de que el área no está aislada y no es vulnerable) y;
4) Área segura (contar con el resguardo y observación de fuerzas de seguridad).

Siguiendo principios como los que manejan estos enfoques, la seguridad física se puede valer de elementos, como un sistema de seguridad, para garantizar la protección y salvaguarda de instalaciones de diversa naturaleza, como pueden ser: empresas, escuelas, cárceles, etc.

1.3.4. Sistemas de seguridad física

Un sistema de seguridad física, se puede entender como un conjunto de elementos interrelacionados que tiene como finalidad proporcionar protección a las instalaciones de una empresa u organización, principalmente a sus activos (intelectuales y materiales). Sus principales funciones, son:

1) Disuadir;
2) Detectar;
3) Retardar y;
4) Responder.

Un sistema de seguridad eficaz debe ser capaz de disuadir, detectar a tiempo al adversario, retardarlo el tiempo suficiente para que las fuerzas de respuesta de seguridad puedan llegar y neutralizar al adversario antes de que se lleve a cabo el acto malintencionado.

La función de disuasión del sistema de seguridad consiste en inducir al posible adversario a que desista sobre su posible ataque, es decir, prevenir los actos malintencionados.

La detección, es la función requerida para el descubrimiento de la acción del adversario, e incluye acciones encubiertas o manifiestas. Para descubrir una acción adversaria, primeramente un sensor o conjunto de sensores (equipo o personal) reacciona ante un acontecimiento anormal e inicia una alarma, después la información del sensor y la evaluación del subsistema es reportado y mostrado, y finalmente alguien evalúa la información y determina si la alarma fue válida o no. Los métodos de detección incluyen una amplia gama de tecnologías y de personal, por ejemplo: el control de accesos, que es un medio que permite la entrada de personal autorizado, así como la detección de entrada o intento de entrada de personal no autorizado y el contrabando; los bloqueos, que también se puede considerar un factor de retraso (después de la detección); la búsqueda de metales y explosivos, a través de detectores de metales, rayos X (para paquetes), y detectores de explosivos; o, el personal de seguridad, que puede realizar la detección, equipado con medios de alerta y comunicación con las fuerzas de seguridad. En la evaluación de la detección se debe informar si la alarma es válida o no, y detallar la causa de la alarma (qué, quién, dónde, o cuántos).

El retardo del adversario, es la función que busca impedir el progreso de las acciones de éste, puede ser logrado por obstáculos fijos o activos (por ejemplo, puertas, bóvedas o cerraduras) o por barreras activadas por sensor (por ejemplo, aspersores líquidos o de espuma). Los elementos de seguridad pueden ser considerados como elementos de retardo, si se encuentran en posiciones fijas y protegidas.

La respuesta, comprende las medidas adoptadas por los elementos de seguridad (policía o agentes del orden) para evitar el éxito del adversario o de la amenaza. La respuesta consiste en la interrupción y neutralización. La interrupción se da cuando la fuerza de respuesta llega a la ubicación apropiada para detener el progreso del adversario. La neutralización es el acto de detener al adversario antes de que alcance su objetivo.

La acción de un adversario, desde su inicio hasta su fin, puede ser medida como una función del tiempo, en dicho periodo el sistema de seguridad física tiene como finalidad evitarla, la figura 2 muestra la secuencia que seguirían sus funciones, cuya eficiencia puede determinarse de la siguiente manera:

- Disuasión. Al lograr que la acción malintencionada no inicie, de no conseguirlo e iniciar dicha acción, el adversario se enfrentará a la siguiente función;

- Detección. Por la probabilidad de identificar la acción del adversario, así como el tiempo requerido para reportar y evaluar la alarma;

- Retardo. Por el tiempo requerido por el adversario (después de la detección) para eludir cada elemento destinado a esta función;

- Respuesta. Por el tiempo entre la recepción del comunicado de las acciones del adversario, la interrupción y la neutralización de la acción.

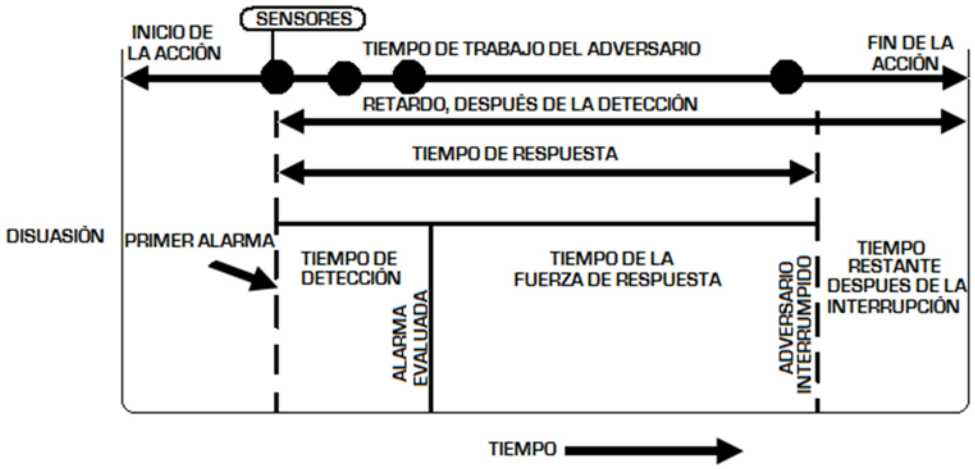

Figura 2. Tiempo de trabajo del adversario vs sistema de protección física
Fuente: Presentación sobre la metodología de evaluación de riesgos de los laboratorios Sandia, 2006

La eficiencia del sistema de seguridad física es determinada por los elementos que lo conforman, de sus características, su buen funcionamiento y operación. Algunos de estos elementos son:

- Barreras física
- Cerraduras con llave
- Sistemas de alarma local
- Alumbrado de vigilancia
- Sistemas de CCTV
- Sistemas de control de acceso
- Sistemas de alarma con monitoreo remoto
- Barreras físicas anti-vandalismo y protección perimetral con guardias
- Guardias con equipos de comunicación
- Alarmas perimetrales
- Guardias armados y entrenados con equipos de comunicación avanzados
- Planes de contingencia
- Fuerza de respuesta armada interna

1.3.5 La administración de riesgos

Retomando el concepto del riesgo, se trata de un hecho que no puede ser evitado o negado, y entenderlo, en el sentido de cómo es causado e influenciado, puede permitir cambiarlo. Para esto se cuenta con un proceso denominado *administración de riesgos*, acerca del cual se han creado estándares, principalmente el Australiano Neozelandés AS/NZS 4360:2004 y recientemente la ISO 31000:2009 emitida por la Organización Internacional de Normalización, en el que se dan importantes avances en el sentido de su definición, tratándolo como un efecto de la incertidumbre en lugar de un evento y, además considera necesarios, elementos como la planeación, para su manejo.

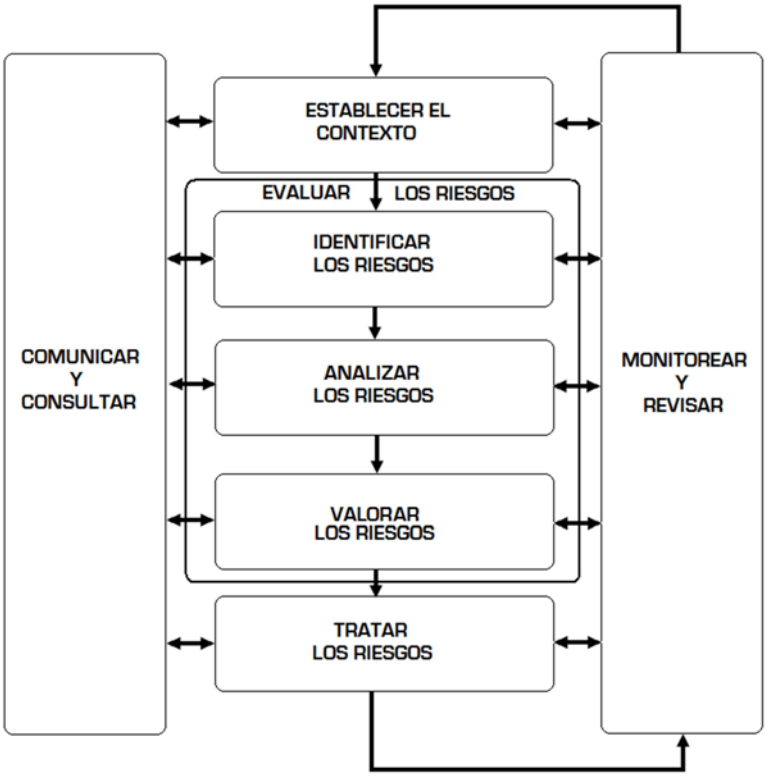

Figura 3. Proceso de Administración o gestión de riesgos
Fuente: ISO 31000, 2009.

En la figura 3 se muestra el procedimiento de gestión o administración del riesgo, que se conforma por cinco actividades:

- *Comunicación y consulta* entre los stakeholders o partes interesadas (internas y externas) y los responsables de la aplicación del proceso en cada etapa del mismo, a través de un plan y con la finalidad de que las partes comprendan la base sobre la cual se toman decisiones, así como la razón por la cual se requieren acciones concretas.

- *Establecer el contexto*, en donde se definen los parámetros internos y externos que deben tenerse en cuenta, se establece ambiente externo, el interno y el del proceso de administración, definiendo sus alcances, objetivos y criterios para medir el riesgo.

- *Evaluación de riesgos*, que se realiza en tres instancias: 1) la *identificación del riesgo*, en donde se listan las fuentes de riesgo, las posibles zonas de impacto, accidentes, sus causas, y sus posibles consecuencias, con base en los eventos asociados que podrían desencadenarlos; 2) *análisis de riesgos,* se consideran las causas y fuentes del riesgo, sus consecuencias positivas y negativas, así como la probabilidad de que pueden ocurrir, teniendo en cuenta la interdependencia de dichas causas y fuentes en su totalidad, así como la información disponible, puede realizarse a diferentes grados de detalle mediante una combinación cualitativa, semi-cuantitativa o cuantitativa, dependiendo de las circunstancias y

los criterios de riesgo definidos, y; 3) la *valoración del riesgo*, en donde se compara el nivel de riesgo que se encuentra en la instancia anterior mediante los criterios establecidos en el establecimiento del contexto, y se establece la priorización para el tratamiento de los riesgos.

- *Tratamiento de los riesgos,* que consiste en seleccionar y aplicar una o más opciones para modificar los riesgos; implica un proceso cíclico de evaluación de riesgos con la finalidad de saber si los niveles residuales del riesgo son tolerables o no. Las opciones del tratamiento de riesgos no necesariamente son mutuamente excluyentes o apropiadas en todas las circunstancias, algunas pueden ser: evitar el riesgo; eliminación de la fuente del riesgo; cambiar la naturaleza y la magnitud del riesgo; cambiar sus consecuencias; compartir el riesgo; aceptar el riesgo; entre otras opciones. Básicamente se presentan dos instancias: 1) la *selección de las opciones de tratamiento del riesgo*, que busca equilibrar costos y esfuerzos frente a los beneficios, tomando en cuenta los requisitos involucrados; 2) la *elaboración y aplicación de planes de tratamiento de riesgos*, que considera y define, entre otros aspectos: el beneficio a obtener, las acciones propuestas, los requisitos de control, los requisitos necesarios, etc., así como a los responsables de su aprobación y ejecución.

- El *monitoreo y revisión,* que es una parte planeada, en donde se abarcan aspectos como la detección de cambios en el contexto externo e interno, incluyendo los cambios en el propio riesgo, que pueden requerir la revisión de las prioridades y tratamientos, o bien, la identificación de riesgos emergentes. Se proporciona una medida del rendimiento del proceso a través de la aplicación de planes en lo que se registra el progreso.

1.3.6 Metodologías para la evaluación de riesgos en proyectos de seguridad física

Es importante distinguir entre un proceso de gestión o administración del riesgo, abordado en la sección 1.3.5, y una metodología para determinar el riesgo, el primero es el marco de referencia del segundo; una metodología para determinar o evaluar el riesgo es una herramienta de análisis para integrar datos e información, y ayudar a comprender la naturaleza y ubicación de los riesgos de un sistema. Por otro lado, un aspecto importante de estas metodologías es el papel que desempeñan en el desarrollo o ejecución de un proyecto de seguridad física.

Un proyecto se puede definir como un conjunto de actividades interrelacionadas, programadas y coordinadas, que son planeadas para alcanzar objetivos específicos aprovechando los recursos disponibles en un tiempo determinado; surge como respuesta a la búsqueda de soluciones de un problema (reemplazo de tecnología obsoleta, equipamiento especializado de tecnología, desarrollo de software, inversiones en negocios, etc.). El Project Management Institute (2000) en su PMBOOK GUIDE define un proyecto como una tarea temporal (tiene un inicio y un fin – cuando se logran los objetivos o se hace evidente que no se cumplirán, o cuando ya no existe la necesidad de llevarlo a cabo) que se asume con la finalidad de crear un producto, servicio o resultado único, a través de una elaboración progresiva. Existen diversas formas de clasificar a los proyectos, de acuerdo a su carácter, al sector económico en el que se desarrolla, según los objetivos, según su tamaño, según el tipo de productos o servicios generados, entre otras.

Los proyectos de seguridad física podrían ser enmarcados por su objetivo y por el tipo de productos o servicios generados, ya que en un proyecto de esta naturaleza se busca diagnosticar, evaluar y manejar los riesgos asociados a sistemas físicos, generando normas y políticas que garanticen la disminución de esos riesgos así como el uso eficiente de las tecnologías disponibles para esos fines, evitando que sus activos o bienes (físicos e intelectuales) se vean comprometidos.

En un proyecto de seguridad física se pueden abordar aspectos relacionados con: investigación (diagnósticos, evaluación de riesgos, propuestas tecnológicas, capacitación, desarrollo de políticas y procedimientos); atención de emergencias; administración de desastres; desarrollo e implantación de sistemas de seguridad, entre otros.

1.4 La metodología empleada por el CIDETES para la evaluación de riesgos en proyectos de Seguridad Física

El CIDETES utiliza un conjunto de procedimientos a través de los cuales busca determinar los medios de protección (tecnológicos y normativos) requeridos para garantizar la seguridad de un sistema bajo estudio, así como la programación para su implantación y presupuesto, con base en la obtención de un "mapa de riesgos" resultado de la evaluación del riesgo al que se encuentra sujeto dicho sistema[12]. La metodología CIDETES tomó como base la metodología de evaluación para la protección de puertos (EPP), para la realización del proyecto "Alternativas tecnológicas para la protección del puerto de Veracruz" en 2006.

Los resultados que se obtienen de esta metodología se encuentran sustentados por el trabajo en campo (recolección de información) y la experiencia, en materia de seguridad, de los investigadores. A continuación se describen brevemente las etapas o pasos por los que se encuentra integrada dicha metodología, en el capítulo 3 de este trabajo de investigación se hace un análisis estructural y funcional de la misma.

Como se puede ver en la figura 4, se constituye por 9 etapas o pasos, que son:

1) Definición del Universo o sistema objeto del estudio de riesgo;
2) Identificación y definición de amenazas;
3) Determinación del grado con el que los elementos representan un objetivo para las amenazas
4) Determinación del grado de vulnerabilidad de los elementos con respecto de las amenazas
5) Determinación del impacto en caso de pérdida de los elementos
6) Cálculo del riesgo
7) Obtención del mapa de riesgo
8) Equipamiento
9) Diseño del programa de presupuesto

[12] Desarrollado por el M.I. Alberto Lepe Zuñiga

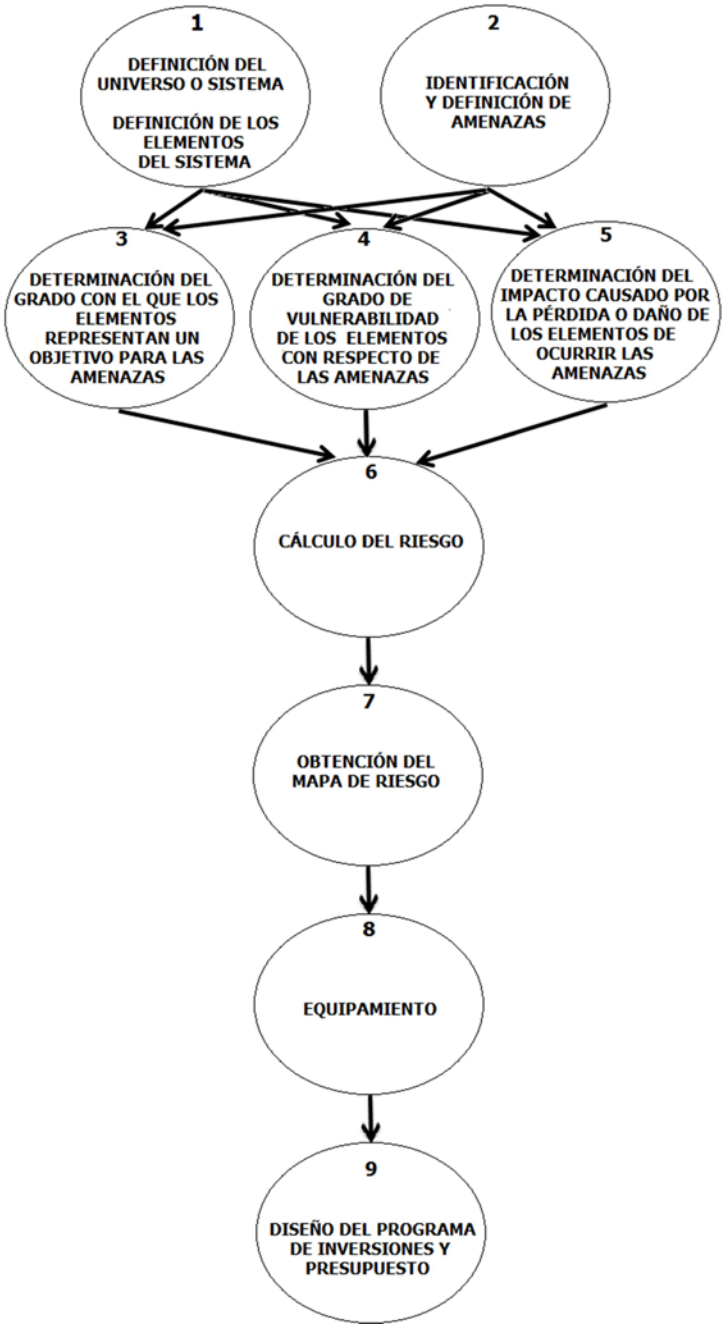

Figura 4. Etapas de la metodología empleada por el CIDETES
Fuente: Elaboración propia, 2010.

1) Definición del universo o sistema objeto del estudio de riesgo.

En este primer paso se identifican los elementos que conforman el sistema en estudio con base en criterios de agregación definidos por los expertos, de esta manera se listan y describen los elementos que conforman al sistema.

Elementos (E)= {elemento1, elemento2, elemento3 …… elementoN}

2) Identificación y definición de amenazas.

En esta fase, con base en el trabajo de campo y la experiencia de los investigadores, en materia de seguridad, se identifican las amenazas que en un momento determinado se pudieran presentar y afectar al sistema en estudio y sus elementos, tomando como referencia su entorno (situación socio-económica, socio-política, el medio ambiente, etc.), y estimando a su vez la probabilidad de ocurrencia de dichas amenazas.

Amenazas (A) = {amenaza1, amenaza2, amenaza3 … amenazaN}

Probabilidad de ocurrencia (Pa) = { p1, p2 , p3 … pN}

Los resultados obtenidos en estas primeras dos etapas o pasos, alimentan las tres siguientes, en las que se relaciona a cada amenaza con cada elemento para valorar el grado con el que los elementos representan un objetivo para las amenazas, el grado de vulnerabilidad de los elementos con respecto a cada amenaza y el impacto en términos económicos causado en cada elemento si cada amenaza se materializara. Generándose de esta manera una matriz de valores en casa paso.

	amenaza1	amenaza2	amenaza3	…	amenaza N
elemento1	Ve1,a1	Ve1,a2	Ve1,a3		Ve1,aN
elemento2	Ve2,a1	Ve2,a2	Ve2,a3		Ve2,aN
elemento3	Ve3,a1	Ve3,a2	Ve3,a3		Ve3,aN
.....					
elementoM	VeM,a1	VeM,a2	VeM,a3		VeM,aN

3) Determinación del grado con el que los elementos representan un objetivo para las amenazas

Aquí el grupo de expertos se pone de acuerdo y asignan un valor entre 0 y 100 que represente el grado con el cual la amenaza se dirigiría al elemento con la finalidad de causar un daño. Esto se hace para cada elemento con respecto a cada amenaza. El producto o resultado de este paso es la matriz "O", en donde el elemento "$O_{m,n}$" representa el grado con que el elemento "m" es atractivo para la amenaza "n".

$$\text{Objetivo (O)} = f(A,E) = \begin{pmatrix} O_{1,1} & O_{1,2} & O_{1,3} & O_{1,N} \\ O_{2,1} & O_{2,2} & O_{2,3} & O_{2,N} \\ O_{3,1} & O_{3,2} & O_{3,3} & O_{3,N} \\ O_{M,1} & O_{M,2} & O_{M,3} & O_{M,N} \end{pmatrix}$$

4) Determinación del grado de vulnerabilidad de los elementos

De la misma manera que en el paso anterior el grupo de expertos se pone de acuerdo y asignan un valor entre 0 y 100 que represente el grado de vulnerabilidad de cada elemento, evaluando la potencialidad de cada amenaza. El producto o resultado en este

paso es la matriz "V", en donde el elemento "$V_{m,n}$" representa el grado de vulnerabilidad del elemento "m" con respecto a la amenaza "n".

$$\text{Vulnerabilidad (V)} = f(A,E) = \begin{pmatrix} V_{1,1} & V_{1,2} & V_{1,3} & V_{1,N} \\ V_{2,1} & V_{2,2} & V_{2,3} & V_{2,N} \\ V_{3,1} & V_{3,2} & V_{3,3} & V_{3,N} \\ V_{M,1} & V_{M,2} & V_{M,3} & V_{M,N} \end{pmatrix}$$

En esta etapa el principal insumo es el estudio que se realiza acerca del sistema de seguridad, en el que se levanta información sobre:

- El sistema de CCTV
- Control de Accesos
- Perimetrales (Bardas y caminos)
- Centro de Mando de Control
- Áreas Críticas
- Organización y Procedimientos

5) Determinación del impacto en caso de pérdida de los elementos

Se parte de la consideración de que las amenazas alcanzan sus objetivos, entonces el grupo de expertos determinan el impacto causado por la pérdida o daño de los elementos, analizando las posibles consecuencias que se presentarían y traduciéndolas a un valor económico. El producto o resultado de este paso es la matriz "I", en donde el elemento "$I_{m,n}$" representa el impacto económico (valor absoluto de los costos implicados) causado por la pérdida o daño del elemento "m" causado por la amenaza "n".

$$\text{Impacto (I)} = f(A,E) = \begin{pmatrix} I_{1,1} & I_{1,2} & I_{1,3} & I_{1,N} \\ I_{2,1} & I_{2,2} & I_{2,3} & I_{2,N} \\ I_{3,1} & I_{3,2} & I_{3,3} & I_{3,N} \\ I_{M,1} & I_{M,2} & I_{M,3} & I_{M,N} \end{pmatrix}$$

6) Cálculo del riesgo

El riesgo asociado a cada elemento con respecto de cada amenaza, se calcula multiplicando la probabilidad de ocurrencia de las amenazas por cada valor asignado en la relación elemento-amenaza de los pasos anteriores, es decir, la probabilidad de ocurrencia "Pa_n", de la amenaza "n", por el elemento "$O_{m,n}$", obtenido en el paso 3 (grado con el que los elementos representan un objetivo para las amenazas), por el elemento "$V_{m,n}$", obtenido en el paso 4 (grado de vulnerabilidad de los elementos con respecto de las amenazas), por el elemento "$I_{m,n}$", obtenido en el paso 5 (impacto económico que se tendría si las amenazas alcanzaran sus objetivos), cuyo resultado genera al elemento "$R_{m,n}$", que conforma, entonces, la matriz "R" y en donde dicho elemento representa el riesgo asociado al elemento "m" con respecto a la amenaza "n".

$$R = f(O, V, I)$$

$$R = \begin{pmatrix} O_{1,1} * V_{1,1} * I_{1,1} * Pa_1 & O_{1,2} * V_{1,2} * I_{1,2} * Pa_2 & O_{1,3} * V_{1,3} * I_{1,3} * Pa_3 & O_{1,N} * V_{1,N} * I_{1,N} * Pa_N \\ O_{2,1} * V_{2,1} * I_{2,1} * Pa_1 & O_{2,2} * V_{2,2} * I_{2,2} * Pa_2 & O_{2,3} * V_{2,3} * I_{2,3} * Pa_3 & O_{2,N} * V_{2,N} * I_{2,N} * Pa_N \\ O_{3,1} * V_{3,1} * I_{3,1} * Pa_1 & O_{3,2} * V_{3,2} * I_{3,2} * Pa_2 & O_{3,3} * V_{3,3} * I_{3,3} * Pa_3 & O_{3,N} * V_{3,N} * I_{3,N} * Pa_N \\ O_{M,1} * V_{M,1} * I_{M,1} * Pa_1 & O_{M,2} * V_{M,2} * I_{M,2} * Pa_2 & O_{M,3} * V_{M,3} * I_{M,3} * Pa_3 & O_{M,N} * V_{M,N} * I_{M,N} * Pa_N \end{pmatrix}$$

$$R = \begin{pmatrix} R_{1,1} & R_{1,2} & R_{1,3} & R_{1,N} \\ R_{2,1} & R_{2,2} & R_{2,3} & R_{2,N} \\ R_{3,1} & R_{3,2} & R_{3,3} & R_{3,N} \\ R_{M,1} & R_{M,2} & R_{M,3} & R_{M,N} \end{pmatrix}$$

Una vez que se tiene el valor del riesgo asociado a cada elemento con respecto de cada amenaza, se obtiene el riesgo acumulado para cada elemento, sumando sus valores asociados, es decir, el riesgo asociado al elemento "m", queda definido por:

$$R_m = R_{m,1} + R_{m,2} + R_{m,3} + \ldots + R_{m,n}$$

Después de esto, se jerarquizan los valores "R_m" con el propósito de expresar de mayor a menor el riesgo de los elementos y clasificarlos como altos, medios o bajos, tratando de construir una idea sobre la prioridad de atención con que dichos elementos pueden ser considerados al momento de establecer las propuestas tecnológicas.

7) Obtención del mapa de riesgo

En esta fase se representa gráficamente, en planos, los elementos del sistema y su riesgo asociado, identificándolos por colores, rojo para los elementos considerados como de alto riesgo, amarillo para los clasificados como riesgo medio, y verde para los de bajo riesgo.

8) Equipamiento

Aquí, una vez construido el mapa de riesgos, los expertos se reúnen y discuten el tipo de tecnologías requeridas y sus características (número de elementos, ubicación, etc.), para cada elemento en función de su valor de riesgo asociado. Al final de esta etapa se tiene la propuesta de las tecnologías a implantar.

9) Diseño del programa de inversiones y presupuesto

En la fase final se realiza una investigación sobre los costos de los equipos y tecnologías propuestas, y se diseña el programa de presupuesto, el cual, en función de la jerarquización del riesgo encontrado, asigna prioridades, en primer instancia, a aquellos elementos en los que el riesgo es alto, después a los de riesgo medio, y finalmente a los de riesgo bajo.

1.5 Problemática entorno a la metodología para la evaluación de riesgos empleada por el CIDETES en proyectos de seguridad física

Las metodologías utilizadas para la evaluación de riesgos representan una parte importante dentro de los proyectos de seguridad física, puesto que permiten estimar el grado con que una o varias amenazas pueden causar pérdidas a una institución o empresa, la facilidad con que lo pueden hacer, así como las consecuencias de esas pérdidas, reflejadas en diversos aspectos, como lo pueden ser el impacto o impactos económicos, sociales, ambientales, psicológicos, etc. De sus resultados, se obtiene la información requerida para la formulación de propuestas tecnológicas y normativas que permiten mejorar las condiciones de seguridad, de dicha institución o empresa.

De esta manera, las metodologías para la evaluación de riesgos permiten tener una idea clara, o bien, sentar las bases sobre cuestiones como:

- ¿Qué proteger?;
- ¿De qué, quién o quienes se tiene que proteger?;
- ¿Qué pasaría si no se protege?;
- ¿En qué beneficia estar protegido?;
- ¿Con qué se tiene que proteger?;
- ¿Cómo se tiene que proteger?;
- ¿Cuánto cuesta estar protegido?.

Por otro lado estas metodologías, presentan cierta subjetividad asociada a la experiencia de las personas que las aplican, sin embargo, un problema mayor, es la ambigüedad que se puede presentar debido a una definición ambigüa o errónea en los elementos de evaluación (criterios, escalas y unidades de medición).

EL CIDETES utiliza la metodología para la evaluación de riesgos presentada en la sección 1.4 dentro de sus proyectos de seguridad física, misma que no se ha utilizado recurrentemente, y que sin embargo, ha sido modificada por sus investigadores con el fin de ofrecer resultados que se apeguen a las necesidades de sus clientes y cubrir las características del entorno de dichos proyectos. Además, las exigencias por contar con instrumentos sólidos, debido a la importancia y magnitud de los proyectos más recientes, han puesto a esta metodología como un elemento de revisión, que necesita ser fundamentado, robustecido y complementado en su estructura y funcionalidad. De esta manera, al hacer una revisión de los problemas que presenta la metodología empleada por el CIDETES se pueden mencionar:

- Está sujeta a cierta subjetividad, al depender de la experiencia de sus investigadores;

- Se presentan ambigüedades al no definir de una forma clara y precisa, las escalas y unidades de medición para evaluar el riesgo, lo que provoca pérdidas de tiempo y sesgos en los resultados obtenidos;

- Una conceptualización parcial o reduccionista del sistema, objeto de estudio, en el que será evaluado el riesgo;

En este sentido, además de buscar una solución para los problemas listados, se busca fortalecer:

- El sustento teórico, con base en elementos cognoscitivos proporcionados por el enfoque de sistemas y el enfoque cibernético;

- La forma en que da soporte a la toma de decisiones, en materia de seguridad, a quienes van dirigidos sus resultados;

- La forma en la que se obtiene el valor del riesgo, puesto que una parte fundamental es el grado de certeza con el que se obtienen los resultados de este tipo de estudios;

- Los mecanismos y herramientas que soportan la recolección de información que sustenta la evaluación de riesgos;

- La validez y sustento de las propuestas tecnológicas como resultado de la evaluación de riesgos, ya que el mercado de tecnología en materia de seguridad en el país se encuentra en manos de los proveedores, y son ellos quienes en la mayoría de los casos terminan realizando recomendaciones sobre qué comprar, aunque no siempre justifican, del todo, dicha compra. Mediante esta metodología se busca fundamentar las razones por las cuales las propuestas establecidas debieran llevarse a cabo;

- La justificación sobre el beneficio económico que se tendría, de invertir en las propuestas tecnológicas, a través de un indicador de rentabilidad;

- La justificación sobre la reducción del riesgo, si se implantan las propuestas establecidas, a través de un indicador;

- La justificación sobre la importancia del valor del riesgo obtenido en comparación con otros sistemas a través de un indicador.

1.6 Definición del Problema

En función de las consideraciones enlistadas en la sección anterior los expertos del CIDETES concuerdan en que la metodología utilizada no considera aspectos importantes de otros metodologías, y por lo tanto requiere ser revisada en su práctica, así como sustentada en su teoría, debido a lo cual, es necesario que la metodología CIDETES sea analizada en su totalidad y comparada con las principales metodologías utilizadas en el ámbito de la seguridad física para la evaluación de riesgos, y de esta manera sustentar, estructurar, definir y complementar cada una de las etapas o fases de dicha metodología, permitiendo considerarla como instrumento de planeación que proporcione apoyo en la toma de decisiones.

1.7 Objetivos

El objetivo principal de este trabajo de investigación es proponer adecuaciones y recomendaciones a la metodología desarrollada por el CIDETES, como resultado de un análisis comparativo, en el que se tomen como referencia otras metodologías utilizadas en la evaluación de riesgos en materia de seguridad física, a fin de robustecer sus bases teóricas y eventualmente su práctica como instrumento de planeación.

El objetivo particular queda establecido por la caracterización de la metodología utilizada por el CIDETES, así como de las metodologías para la obtención del riesgo que se puedan aplicar en el rubro de la seguridad física, realizando un análisis estructural y funcional de ellas con el propósito de conocer cómo son utilizadas y aplicadas, esto desde un enfoque de planeación.

1.8 Justificación

El análisis de riesgos representa el motor en un estudio integral sobre seguridad, ya que es a partir de éste que se determinará la situación actual de un sistema de interés (instalaciones, edificios, etc.), al evaluar los riesgos de dicho sistema se desprenderán las recomendaciones tecnológicas y normativas.

Después de aplicar la metodología CIDETES en un proyecto de seguridad física, enfrentarse a la subjetividad y ambigüedades que generan retrasos y sesgos, así como entender la importancia que tiene la evaluación de riesgos dentro de este tipo de proyectos, resulta necesario robustecer las bases teóricas y prácticas de la metodología, con la finalidad de contar con un instrumento que permita proporcionar sustento sólido a través de resultados que faciliten la toma de decisiones relacionadas con la seguridad física de un sistema específico, y que involucre un proceso de planeación.

Particularmente el CIDETES se encuentra en un una etapa de posicionamiento en el rubro de proyectos sobre seguridad física, por lo que es de su interés realizar un estudio sobre su metodología. De esta manera surge la inquietud de este trabajo de investigación.

1.9 Alcance

Establecer propuestas de mejora, que permitan a la metodología CIDETES robustecer, por un lado, sus bases teóricas, al proporcionar el sustento cognoscitivo para conceptualizar sistémica y cibernéticamente los fenómenos y elementos asociados al riesgo en materia de seguridad física, y por otro, su práctica como instrumento de planeación, a través de adecuaciones y recomendaciones, estructurales y funcionales, a su proceso de aplicación.

1.10 Estrategia de Investigación

La estrategia de investigación permitió definir el rumbo a seguir en la elaboración del trabajo de investigación, y de esta manera alcanzar los objetivos planteados, a continuación en la tabla 1 se presentan las etapas en las que fue dividida:

Etapa	Métodos y herramientas	Actividades	Resultados esperados
Conceptualización	Metodología CIDETES. Revisión de literatura referente a la evaluación de riesgos en materia de seguridad física	Aplicación de la metodología en un proyecto de seguridad física.	Problemática. Objeto de estudio (problema). Objetivos, alcance y justificación de la Tesis.
Investigación	Revisión de literatura sobre la Investigación Interdisciplinaria de desastres	Estructuración del marco teórico.	Elementos cognoscitivos que sustentan la evaluación de riesgos en materia de seguridad física. Criterios de comparación
Análisis	Análisis estructural y funcional de las metodologías	Selección de las metodologías alternas sobre evaluación riesgos en materia de seguridad. Caracterización de las metodologías de referencia y de la metodología CIDETES.	Metodologías de referencia. Características estructurales y funcionales de las metodologías.
	Análisis comparativo entre las metodologías	Comparación entre las metodologías de referencia y la metodología CIDETES.	Cuadros comparativos entre las metodologías Diferencias y similitudes entre las metodologías para la evaluación de riesgos Fortalezas y debilidades de le metodología CIDETES
Síntesis	Recopilación de resultados.	Construcción de las adecuaciones y recomendaciones.	Propuestas de mejora

Tabla 1. Estrategia de investigación.
Fuente: Elaboración propia

LA INVESTIGACIÓN INTERDISCIPLINARIA DE DESASTRES COMO MARCO DE LA EVALUACIÓN DE RIESGOS

CAPÍTULO 2

Fuentes Zenón (1994) considera a la planeación como una herramienta cuyas características dependen de la clase de problema en que es aplicada, de tal manera que existe una metodología o procedimiento para cada una de ellas, y propone un enfoque contingente en el que se tiene como propósito ayudar a definir qué metodología o procedimiento es el que mejor se adecúa. De esta manera, el trabajo de investigación es dirigido, por un lado, con respecto al problema sobre la reducción de riesgos mencionado en la sección 1.3.2, al enfoque de la planeación como un proceso básico en la conducción, establecido por Gelman y Negroe (1982), y por otro, a la Investigación Interdisciplinaria del Desastre (IID) desarrollada por Gelman (1996) en respuesta al sustento teórico que requiere la metodología para la evaluación de riesgos utilizada por el CIDETES.

Así, el marco teórico de este trabajo de investigación queda establecido en primer instancia por el enfoque sistémico y el enfoque cibernético, los cuales representan las bases cognoscitivas del proceso de conducción, que a su vez, sustenta a la Investigación Interdisciplinaria de Desastres "IID", permitiendo sentar las bases metodológicas para la evaluación de riesgos a través de la conceptualización de los sistemas involucrados en este fenómeno del desastre.

Abordar estos conceptos hará posible sustentar teóricamente a la metodología CIDETES, puesto que la IID proporciona una percepción holística de la problemática referente a eventos no deseados de seguridad, aquí llamados fenómenos de desastre, al definir y caracterizar tanto estructural como funcionalmente a cada sistema involucrado en dicho fenómeno. Esto resulta trascendente ya que evitará que el manejo que se da al riesgo, para su obtención, se realice de forma reduccionista al considerar de forma parcial a los elementos involucrados.

Por otro lado el enfoque de planeación como un proceso básico de conducción permitirá conocer las instancias necesarias para enmarcar a la metodología CIDETES como un instrumento de planeación que proporcione sustento a la toma de decisiones del sistema conducente.

La evaluación y reducción del riesgo, como objetivos de la seguridad física, hacen que resalte la importancia de las metodologías que tienen como fin último la obtención del valor de esta variable, debido a lo cual resulta necesario conocer los elementos mínimos que deben contemplar, el apartado sobre "estudios de riesgos" proporcionará una idea clara acerca de estos elementos y de esta manera establecer los criterios bajo los cuales se realizará la comparación de las metodologías en el capítulo 3.

2.1 El enfoque sistémico y el enfoque cibernético

Las bases cognoscitivas que soportan al proceso de la conducción son el enfoque sistémico y el enfoque cibernético. El *enfoque sistémico* permite conceptualizar y diseñar objetos como sistemas, por medio de dos procedimientos: construcción por composición y descomposición funcional. En el primero se parte del elemento y se busca llegar al sistema; se ve al objeto de estudio como un conjunto de elementos interrelacionados, organizados e interconectados, y se concibe como un todo integral, se deducen sus propiedades a partir del estudio de sus componentes, de su comportamiento y las relaciones que los vinculan; sin embargo, existe el riesgo de no comprender su naturaleza integral y tener sólo una noción parcial del sistema, al no descubrir el papel que juega en un sistema mayor (suprasistema) y no contemplar todos los elementos relevantes y sus relaciones. En el segundo, se parte del sistema hacia sus componentes, desmembrándolo en subsistemas, cuyas funciones y propiedades aseguran las del sistema en conjunto, y desmembrando a su vez, sucesivamente cada subsistema; se toma en cuenta la estructura externa (se determina el papel que desempeña en el suprasistema y sus relaciones con otros sistemas) e interna (se considera al sistema como un agregado hipotético de subsistemas funcionales, en tal forma interconectados, que aseguran el cumplimiento de su objetivo en el suprasistema).

El *enfoque cibernético* proporciona una pauta heurística para definir a los subsistemas que integran a un sistema, permite determinar el fenómeno del control en ellos y visualizar sus mecanismos, con la consecuente definición de las estructuras organizativas, procesos de gestión y planeación para su realización. Desde este paradigma, como se muestra en la figura 5, se distinguen dos subsistemas: el subsistema gestor, conducente, de regulación o de control, y el subsistema conducido o focal, así como a sus correspondientes relaciones: de información (del conducido al conducente) y de ejecución (del conducente al conducido).

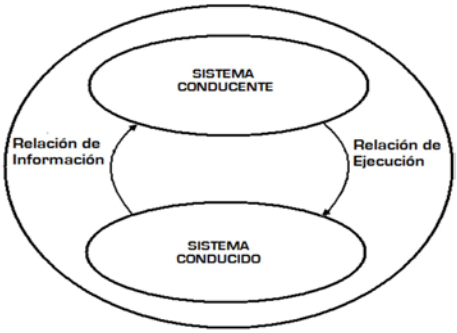

Figura 5. Visualización de un sistema bajo el paradigma cibernético
Fuente: Gelman O. 1996

2.2 La planeación como un proceso básico en la conducción

La *conducción* se presenta al conceptualizar un sistema bajo el paradigma cibernético, se manifiesta como la relación determinante entre dos sistemas: el conducente y el conducido. Se puede definir como un proceso controlado (considera el caso de no cambio del sistema

conducido), en el que en función de cierto objetivo, el sistema conducente traza, realiza y controla la trayectoria adecuada que permite lograrlo, mientras que el sistema conducido es el principal responsable por cumplir con el papel que tiene el sistema en el suprasistema, es decir, proporciona productos, bienes o servicios.

Se distinguen dos modalidades de conducción: la correctiva y la planeada. La correctiva trata de mantener al objeto conducido en un estado dado, o bien, de optimizar su operación, a través de acciones inmediatas, según la situación que se presente. La planeada, se caracteriza por preestablecer un estado futuro deseado del objeto conducido, como objetivo a largo plazo, de modo que se identifican, seleccionan, organizan y realizan las actividades que contribuyan a su logro, a través de la planeación.

En este contexto, la *planeación* bajo el enfoque sistémico (construida mediante el método por descomposición funcional) en el marco del proceso de conducción, es presentada como una actividad adicional a este proceso, que está orientada a la identificación y solución de problemas. Se considera como un instrumento básico que apoya la toma de decisiones, puesto que visualiza y estudia al objeto conducido; proporciona un marco metodológico que en contraposición a la conducción correctiva, permite prever las consecuencias de las acciones actuales y futuras, los posibles problemas futuros y su prevención en caso de su inminente ocurrencia; define objetivos de cambio, políticas y estrategias del proceso de conducción, así como las acciones más adecuadas (inmediatas, a mediano y largo plazo) para determinar y realizar la trayectoria que permita alcanzarlos, de manera directa a través de programas y proyectos, y de manera indirecta mediante criterios generales de selección, contenidos en las políticas, y de soluciones inmediatas, que permitirán generar acciones a ejecutar como resultado de la toma de decisiones.

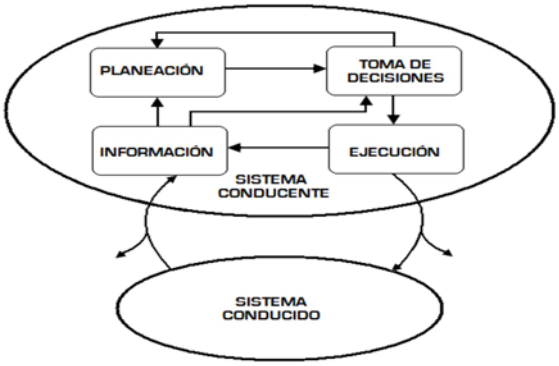

Figura 6. Proceso de planeación desde el enfoque de conducción
Fuente: Gelman O. (1996)

La planeación es ubicada así, dentro del *sistema conducente*, ver figura 6, junto a otros tres subsistemas funcionales:

- Toma de decisiones, en el que se seleccionan las alternativas de acción con la finalidad de optimizar el funcionamiento del sistema o hacer que siga una ruta hacia el cumplimiento de objetivos y metas establecidos por la planeación;

- Información, en el que se proporcionan los elementos necesarios sobre los estados y tendencias del sistema conducido y de su entorno a través de indicadores relevantes que incluyan a otros sistemas vinculados;

- Ejecución, en el que se asegura la realización de las acciones definidas en el proceso de planeación y de las autorizadas por la toma de decisiones, transmitiéndolas del conducente al conducido.

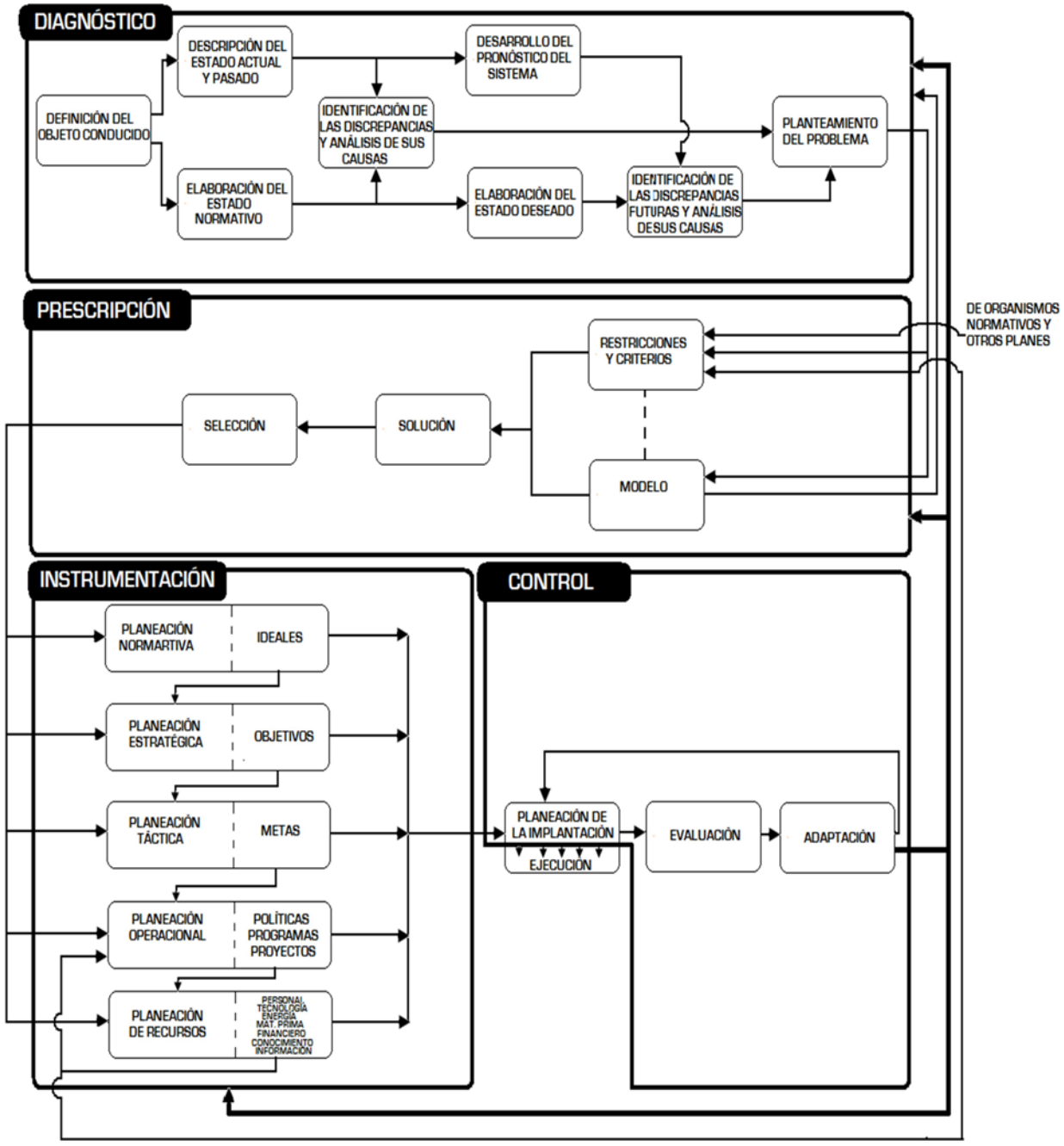

Figura 7. Etapas del proceso de planeación
Fuente: Gelman O. (1996)

El proceso de planeación no es lineal, en la figura 7 se presentan las cuatro etapas que se interrelacionan, las cuales son:

1. Diagnóstico. Se detectan, definen y plantean los problemas (impedimentos y/o conflictos entre los objetivos o funciones del objeto conducido) actuales y futuros que se quieren resolver durante el proceso de conducción. Se conceptualiza al objeto conducido como un sistema, contextualizándolo en el suprasistema, sus interrelaciones con otros sistemas, así como sus propios subsistemas. Se conceptualiza la problemática, al detectar y evaluar las discrepancias, por un lado, al comparar los estados anteriores y actuales con respecto a los estados normativos, y por otro, al comparar los pronósticos de los estados del sistema y su estado deseado.

2. Prescripción. Se trata de dar solución al problema planteado, se construyen modelos con la finalidad de obtener y simular la solución, así como obtener los pronósticos para la etapa anterior; se definen las restricciones, se formulan los criterios para la búsqueda de soluciones y se evalúan las alternativas para seleccionar las factibles y alcanzar un estado deseado.

3. Instrumentación. Se transforma la solución del problema en un conjunto de elementos específicos, formulándose jerárquicamente, en función de los recursos, los ideales, los objetivos, las metas, los programas y políticas, que de acuerdo con Ackoff, se realiza mediante la planeación normativa, estratégica, táctica y operacional, respectivamente.

4. Control. Se busca corregir y mejorar el plan estimando su eficiencia, detectando errores y cambios en el entorno de la conducción. Primeramente en la implantación, se diseñan y organizan los procedimientos para la toma de decisiones, y llevar a cabo el plan (la implantación por sí misma no forma parta de la planeación, es dividida en dos partes, la planeación de la ejecución y la ejecución, únicamente la primera forma parte del proceso); después, de forma continua se detectan errores o fallas del plan con la finalidad de corregirlos, a través de la evaluación y adaptación.

2.3 La Investigación Interdisciplinaria de Desastres (IID)

El Instituto de Ingeniería desarrolló un área interdisciplinaria, que estudia bajo el enfoque sistémico y cibernético el fenómeno de desastre, su principal objetivo consiste en identificar y resolver los problemas de seguridad y salvaguarda de la población, asentamientos humanos, servicios estratégicos, áreas productivas, medio ambiente y obras civiles, a través de la elaboración de metodologías de estimación de riesgos, y de la elaboración de medidas para su reducción, lo que, a su vez conduce al diseño de sistemas de seguridad, y a su instrumentación con planes y programas de acción.

Los problemas surgen como resultado de las discrepancias, desviaciones o conflictos entre los objetivos del objeto conducido, los de su supra-sistema, los del propio sistema, y los de sus subsistemas. En términos generales se pueden visualizar internamente, producidos por las

relaciones entre el sistema conducente y el objeto conducido, o externamente, debido a la relación del objeto conducido con su supra-sistema, con sus subsistemas y con otros objetos, o bien por las relaciones entre el sistema conducente con su supra-sistema y con otros sistemas conducentes.

Para determinar problemas específicos y solucionarlos se requiere precisar los sistemas involucrados, especialmente sus estructuras (interna y externa), así mismo, para su estudio y tratamiento se requiere contar con un paradigma particular. Para entender y controlar el fenómeno de desastre se cuenta con dos paradigmas: el inicial y el fundamental.

2.3.1 Paradigmas que conceptualizan el fenómeno de desastre

En el *paradigma inicial*, se establecen las bases para este fenómeno. Los desastres eran percibidos como eventos que afectaban asentamientos humanos y producían daños, es decir, como una mezcla del evento desequilibrante y los estados del daño, al separar estos dos elementos se plantean dos conceptos relevantes en este estudio:

- La *calamidad*, que se refiere al fenómeno destructivo o suceso que desestabiliza o perturba y puede causar daños a cualquier agente expuesto (asentamiento humano, región política-administrativa, área productiva, obra civil, etc.).

- El *desastre*, por su parte, se refiere a los estados mismos del daño y a todas sus consecuencias, que alteran o incluso rompen el orden normal de las relaciones productivas, comerciales, sociales o políticas.

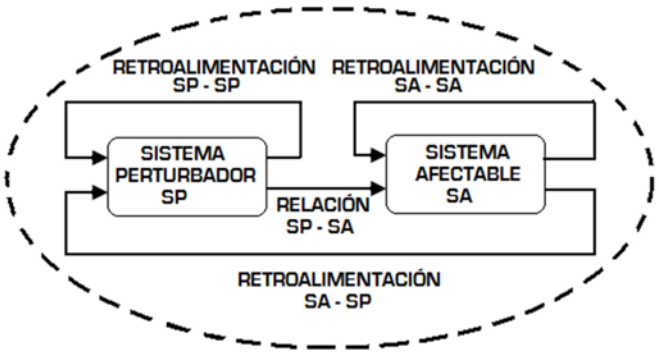

Figura 8. Relaciones entre el sistema perturbador y el sistema afectable
Fuente: Gelman O. (1996)

Estos dos conceptos son a menudo manejados como amenazas en el caso de la calamidad y de un evento no deseado en el caso del desastre. En esta problemática de desastres se definen dos tipos de sistemas que interactúan entre sí: el afectable y el perturbador. El primero, denominado "SA", es el sistema en el que pueden materializarse los desastres debido a la perturbación a la que está expuesto. El otro, denominado "SP", es el responsable de la perturbación, se define como el sistema capaz de producir calamidades. La relación "SP-SA" se da cuando "SP" impacta una calamidad en el sistema "SA" y éste altera su estado normal.

Como se muestra en la figura 8, existen tres retroalimentaciones que pueden agravar o disminuir un desastre: "SP-SP", se manifiesta cuando la ocurrencia y características de una calamidad puede verse modificada, favorecida o inhibida por la acción de otra; "SA-SP", resulta en la activación o detención de la producción de calamidades por el "SP" debido al estado del "SA"; "SA-SA", se da cuando el "SA" influye sobre su propio comportamiento y estado, de tal manera que se agrava o disminuye el desastre, y se abandona o fortalece el estado normal.

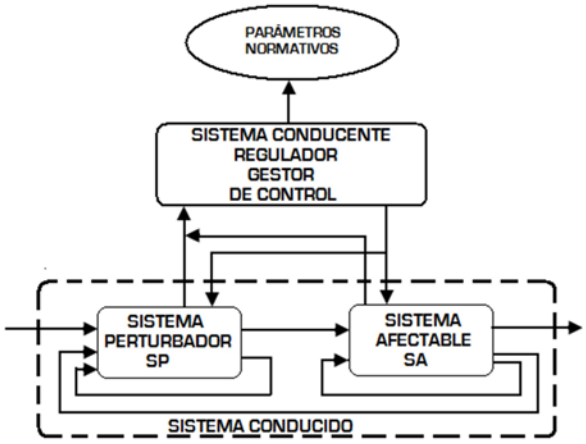

Figura 9. Representación del paradigma fundamental que conceptualiza el fenómeno de desastre.
Fuente: Gelman O. (1996)

En la figura 9, se representa al *paradigma fundamental,* que integra al sistema de control o regulación, el cual persigue dos objetivos: la reducción de riesgos a través de la prevención y la mitigación; y el restablecimiento de la situación normal a través del rescate y la recuperación. De esta manera, el subsistema conducido es el que produce los desastres, mientras que el otro, de conducción, los controla, esto es, busca frenar la producción de desastres. El sistema de conducción tiene que alcanzar los objetivos planteados, apoyándose en la información sobre los estados actual y futuro de los "SP" y "SA", a través del monitoreo, pronóstico, planeación, toma de decisiones y ejecución de una multitud de diversas acciones organizadas en el tiempo y espacio, antes, durante y después del desastre, por medio de los programas correspondientes de gestión, los cuales tienen que ser elaborados, realizados, evaluados y actualizados, por un conjunto de organismos que constituyen la estructura organizativa del sistema conducente.

En las siguientes secciones se detallan los aspectos relevantes de los sistemas que dan explicación al fenómeno de desastre.

2.3.2 El Sistema Perturbador

Como se definió en la sección anterior, el sistema perturbador "SP" es aquel que tiene la capacidad de producir calamidades, así que resulta de especial importancia el estudio de estos fenómenos destructivos. Las calamidades o fenómenos destructivos son determinados e identificados por sus características, que pueden ser de dos tipos:

1) De *identificación*, que permiten realizar un reconocimiento espacial y temporal, a través de su nombre, fecha de ocurrencia, lugar de origen, cobertura, y trayectoria;

2) De *evaluación*, que permiten realizar un reconocimiento de sus particularidades propias por medio de sus *parámetros directos* (miden los factores determinantes como lo son la magnitud, intensidad, velocidad desarrollo y frecuencia), *indirectos* (estiman las manifestaciones de la calamidad a través de sus efectos, los más importantes son los que evalúan los daños producidos), y *particulares* (que caracterizan aspectos específicos de las calamidades).

A continuación se presentan algunas de las calamidades que pueden ser consideradas en un proyecto de seguridad física:

- Terrorismo y acción bélica: el primero, como sucesión de actos de violencia ejecutados para infundir terror, crear un clima de inseguridad o dominar una situación, frecuentemente de carácter político. La segunda, como la lucha armada entre grupos sociales, entre los habitantes de un mismo pueblo o ciudad, o entre bandos de una misma nación o de dos o más naciones, que están en conflicto por intereses o por ideologías opuestas.

- Accidente mayor: acción de origen humano y/o natural que se presenta en forma súbita o inesperada y produce, involuntariamente, aunque muchas veces previsible, daños severos a las personas, cosas, procesos tecnológicos y/o medio ambiente.

- Acto de locura: acción de una o varias personas que pierden la razón en determinado momento, llegando a producir accidentes, delitos u otros actos que atentan contra la sociedad.

- Acto delictivo y sabotaje: acción del hombre que atenta contra la vida, la salud y los bienes materiales de los demás o que impide el normal funcionamiento de un servicio o una empresa, al inutilizar sus equipos o instalaciones, y/o que altera el orden y sistema social, violando la legislación existente.

- Disturbios sociales: acciones originadas por el hombre, por desacuerdo con las disposiciones gubernamentales o patronales, así como por otras razones, frecuentemente, de carácter emocional, reflejadas en manifestaciones, huelgas, revueltas, etc.

- Drogadicción y alcoholismo: introducción al organismo de bebidas alcohólicas o drogas que provocan efectos estimulantes o deprimentes, resultando en accidentes, delitos u otros actos que atentan contra la sociedad.

- Efecto negativo por operar servicios: consecuencias adversas que surgen de la operación normal de algunos sistemas, que perjudican el funcionamiento de otros; por

ejemplo, al operar las industrias o medios de transporte, se emiten gases que contaminan el medio ambiente.

- Envenenamiento: introducción en el organismo de tóxicos de naturaleza química o biológica en cantidades que causan trastornos graves o muerte.

- Explosión: liberación rápida, violenta e irreversible de energía manifestada como el excesivo incremento de presión, por la expansión súbita de sustancias químicas y gaseosas.

- Falla o error humano: acción ocasionada por el hombre, en forma involuntaria, frecuentemente por descuido, que puede alterar los servicios, producir accidentes, resultar en errores de diseño, construcción, mantenimiento y operación, etc., generando lesiones o pérdidas de vida, daños materiales y/o impactos sobre el medio ambiente.

- Fuga y derrame de sustancias peligrosas: desalojo de materiales peligrosos para el hombre y su hábitat, tales como sustancias tóxicas, radiactivas, corrosivas, combustibles, explosivas, contaminantes, bacteriológicas, virulentas y/o cancerígenas, ya sea durante su almacenamiento, transporte, producción, utilización o desecho.

- Incendio: propagación y extensión del fuego no controlado que se produce en industrias, viviendas, bosques, etc., por la ignición de materiales combustibles, en presencia de una fuente de calor y oxigeno u otro material comburente.

- Interrupción de servicios: alteración del servicio que proporciona un sistema al suspender o disminuir sus funciones. Por ejemplo, la interrupción del servicio de agua potable, energía eléctrica, transporte, abastos, etc.

Otro aspecto relevante a considerar es que las calamidades se manifiestan a través de los posibles *impactos* que pueden llegar a causar, por lo que resulta trascendente determinarlos y evaluarlos. Un impacto se puede definir como cualquier incidencia de un agente, elemento o suceso sobre el sistema afectable que produce efectos indeseables (muertes, daños materiales, etc.). Se distinguen dos tipos de impactos:

1) *Primarios o elementales,* que son las manifestaciones propias de la calamidad y se presentan como consecuencia directa de esta;

2) *Agregados*, resultado de integrar y transformar los efectos de impactos anteriores, casi siempre afectando en mayor medida, ya que provocan efectos indirectos.

Por otro lado, conocer los mecanismos de producción de las calamidades hace posible establecer una clasificación y elaborar métodos y modelos de diagnóstico y pronóstico, al mismo tiempo que se favorece el logro del objetivo de prevención, al permitir una oportuna

intervención en ellos. Se distinguen dos mecanismos en la producción de calamidades: interno y externo**.**

El *mecanismo interno* es producido por el sistema perturbador en cinco etapas interrelacionadas:

1) *Preparación* (organización de las condiciones necesarias para su ocurrencia);
2) *Iniciación* (excitación o activación del mecanismo);
3) *Desarrollo* (crecimiento en intensidad y magnitud de la calamidad);
4) *Traslado* (transporte de los elementos impactantes) y;
5) *Producción de impactos* (la manifestación de la calamidad como incidencia de un agente, elemento o suceso sobre el sistema afectable).

El *mecanismo externo* es producido por la compleja red de retroalimentaciones, las cuales pueden iniciar o alterar este proceso de producción, a este fenómeno destructivo se le llama calamidad encadenada, y pueden presentarse tres tipos:

1) *Encadenamiento corto*, producido por una retroalimentación "SP-SP", esto es, cuando la calamidad es iniciada directamente por un impacto primario de un fenómeno destructivo anterior;
2) *Encadenamiento largo*, producido por una retroalimentación "SA-SP", esto es, cuando la calamidad es iniciada por un efecto de un fenómeno destructivo anterior;

3) *Encadenamiento integrado*, producido por una retroalimentación "SA-SA", esto es, cuando la calamidad se presenta a través de impactos agregados de los efectos de un fenómeno destructivo anterior.

De esta manera es posible, entonces, establecer una clasificación que facilite el entendimiento de los fenómenos destructivos y, a la vez, se coadyuve en la realización de los procesos de evaluación y prevención del peligro. Algunos sistemas de clasificación de calamidades pueden ser:

- Por *origen*. Se consideran las fases de preparativos e iniciación de la calamidad, tomando en cuenta el ambiente en el que surge, por ejemplo: socio-organizativas, generadas por actos y errores humanos; de efecto negativo por operar servicios; etc.

- Por *ámbito de desarrollo y traslado*. Se agrupan con relación al crecimiento e intensificación de la calamidad, así como el transporte de los elementos impactantes, por ejemplo: por ámbito social; ámbito tecnológico; etc.

- Por *retroalimentación*. Facilita la elaboración de pronósticos y permite intervenir en las calamidades encadenadas para lograr su prevención y mitigación, los fenómenos destructivos pueden pertenecer a dos tipos de grupos:

- *Directas*, producidas sólo por los mecanismos internos del sistema perturbador;

- *Encadenadas*, iniciadas o alteradas por una o varias retroalimentaciones.

- Por *procedencia*. En función de la ubicación del sistema afectable, siendo:

  - *Internas*, cuando surgen o se generan directamente en el lugar de interés, esto es, en la zona donde está ubicado el sistema afectable, y;

  - *Externas*, cuando se generan fuera del lugar de interés y que pueden impactar sobre éste.

Así mismo, con relación al objetivo de prevención, las estrategias para controlar estos fenómenos destructivos pueden seguir dos caminos de intervención en los mecanismos de producción:

1) *Internamente*, a través de los siguientes lineamientos:

   - Eliminar o impedir la organización y formación de las condiciones favorables para la iniciación y desarrollo de las calamidades, y reforzar las desfavorables;

   - Prevenir la iniciación o activación de los mecanismos productores al identificar los elementos o eventos "disparadores" de la calamidad;
   - Deshabilitar o insensibilizar los elementos partícipes del mecanismo productor y/o sus interrelaciones, en las fases de desarrollo y traslado;

   - Interrumpir los canales de transferencia, al impedir que en la fase de producción de impactos, estos lleguen a incidir sobre el sistema afectable.

2) *Externamente*:

   - En el encadenamiento corto, se trata de disminuir, desviar o interrumpir la retroalimentación "SP-SP", interviniendo en el canal de la transmisión de los impactos.

   - En el encadenamiento largo, retroalimentación "SA-SP", se establecen dos lineamientos:

     1) Reforzar el sistema afectable para disminuir los efectos de impactos anteriores al evitar que la retroalimentación se convierta en el factor iniciador de nuevas calamidades;

2) Disminuir o interrumpir las vías de transmisión de los efectos producidos por la calamidad primaria.

- En el encadenamiento integrado, retroalimentación "SA-SA", se establecen tres lineamientos:

1) Reforzar el sistema afectable para disminuir los efectos de impactos anteriores;

2) Intervenir en la integración de los efectos y su transformación en impactos agregados, e;

3) Interrumpir o disminuir los canales de transmisión de los impactos agregados.

2.3.3 El Sistema afectable

El sistema afectable, definido en la sección 2.1.3 como el sistema en el que pueden materializarse los desastres debido a la perturbación a la que está expuesto, y los subsistemas que lo conforman, representan lo que se quiere proteger. Está integrado, por el medio ambiente y los sistemas de subsistencia, considerados como medios indispensables para el sustento del sistema,

El concepto de desastre se vuelve operativo al visualizarlo como un estado del sistema afectable, es decir, como una característica global del sistema, que se determina por los valores de parámetros relevantes de su funcionamiento en un momento determinado. Puede ser representado por un vector en el espacio multidimensional de estados como se representa en la figura 10.

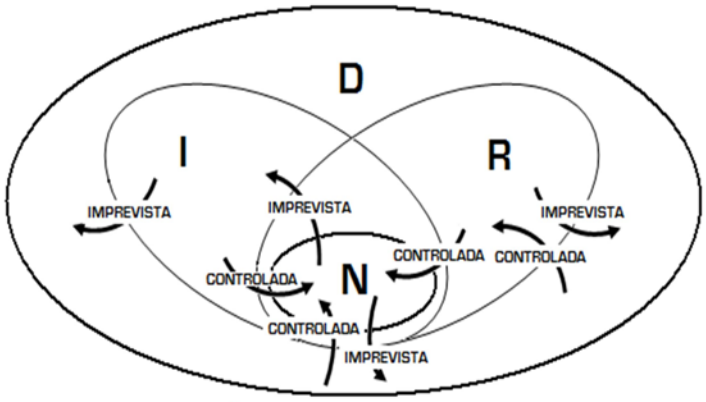

Figura 10. Estados del sistema afectable
Fuente: Gelman O. (1996)

El área de *estados normales*, se refiere a los estados en los que el sistema tiene un funcionamiento normal y estable, y puede lograr sus finalidades. El área de *estados insuficientes* engloba aquellos en los que tiene, todavía, un funcionamiento normal, pero presenta una alteración no significativa (por agentes internos -vejez, deterioro, etc.-; o por los externos -falta de suministro, impacto adverso, etc.-). El área de *estados de desastre* reúne a aquellos en los que el funcionamiento del sistema falla, presentando una alteración significativa y con tendencia a crecer, que no permite al sistema cumplir con sus responsabilidades. El área de *estados de retorno*, incluye todos los estados intermedios entre el área de estados de desastre y el área de estados normales, se caracteriza por la disminución de la alteración y la recuperación progresiva del funcionamiento normal del sistema.

La ubicación del sistema, en una determinada área dependerá de los rangos permisibles para cada parámetro relevante del mismo, así como su monitoreo. Existen transiciones entre las áreas, las cuales implican cambios en las responsabilidades del proceso de conducción:

- *Imprevistas*. Ocurren por el propio desarrollo del sistema o como resultado del impacto de las calamidades, es decir, por causas internas o por la intervención del sistema perturbador.

- *Controladas.* Se refieren a las transiciones realizadas a través de ciertas actividades específicas del organismo conducente.

Por su parte los *sistemas de subsistencia*, contemplan las necesidades y satisfacciones de los elementos y en general del sistema. De acuerdo con su importancia se han clasificado en:

- *Vitales*. Proporcionan el mínimo requerido de bienestar y estabilidad de tal forma que su falla tiene repercusiones inmediatas, como lo es la salud o la seguridad, entre otras;

- *De apoyo*. Dan soporte a los sistemas vitales, y;

- *Complementarios*. Cubren, en forma complementaria, las necesidades y dan soporte al sistema, pero su falla no tiene repercusiones inmediatas.

Determinar la estructura interna y externa de estos sistemas de subsistencia representa un factor relevante que hay que considerar en el mecanismo de la formación de un desastre. En relación con la interna, se busca identificar las consecuencias de los impactos de fenómenos destructivos. Por su parte, en la externa, se busca definir a través de las interrelaciones entre ellos sus contribuciones de subsistencia, las cuales se pueden dar de tres maneras:

- *Interrelación por dependencia*. Cuando están relacionados entre sí, de manera que un sistema se ve afectado cuando otro suspende o disminuye la prestación de sus funciones; su determinación permitirá evaluar los daños encadenados que pueden ocurrir, los daños propios del sistema más los que se pueden provocar en otros

sistemas. Puede ser de cuatro tipos, de acuerdo con el grado de alteración y tiempo que tarda en afectar:

1. *Inmediata*, cuando la falla de un sistema coloca a otro, en un estado de desastre sin dilación.

2. *Directa*, si la falla de un sistema coloca o puede colocar a otro, en un estado de desastre, con retraso en el tiempo;

3. *Indirecta*, cuando la falla de un sistema coloca a otro en un estado de insuficiencia;

4. *Sin relación de dependencia*, si la falla de un sistema no produce alteraciones significativas en otro.

- *Interrelación por efectos negativos*. Se da cuando el funcionamiento normal de un sistema perturba el funcionamiento normal de otro sistema, se pueden diferenciar dos clases:

  1. *Producidos como resultado de un proceso*, ante lo cual basta con suspender la ejecución del proceso en el lugar afectado y realizarlo en otro, y aunque puede ser una solución costosa, la repercusión sólo es económica.

  2. *Producidos por materiales o elementos que son productos o desechos del proceso*, ante lo cual se requiere de una inversión, creación y uso de nuevas tecnologías.

- *Interrelación por peligrosidad*. Se presenta cuando los sistemas manejan equipos y/o materiales que, en caso de una falla, tienen una alta posibilidad de provocar un desastre, ya sea en su propio sistema o en otros, pueden distinguirse dos clases:

  1. *Total*, se da en aquellos elementos o componentes que, en caso de falla, afectan sensiblemente el funcionamiento de su propio sistema y también pueden provocar alteraciones en otros.

  2. *Externa*, se presenta cuando la falla del elemento no afecta de manera sensible a su propio sistema, pero sí altera otros sistemas.

- *Combinación de interrelaciones*. Se presenta cuando existen varios tipos de relación, e incluso todos, además, se considera que una misma falla en un sistema puede impactar por varios caminos a otros sistemas.

2.3.4 Sistema Regulador

El sistema de regulación, gestión o control, a través de una estructura organizativa que opera mediante programas de acción, en función al rol que desempeña en el suprasistema, que en el control de desastres, consiste en cumplir con funciones de integración de actividades que se ejecutan en una situación normal, así como asegurar la eficaz y eficiente realización de la respuesta en el futuro, busca cumplir con dos objetivos:

1) *Reducir los riesgos* de los probables daños que puedan producir las calamidades en un sistema afectable "SA", a través de:

    a) *Prevención*. Antes de la ocurrencia del desastre, implica determinar los fenómenos destructivos, estimar sus características relevantes e intervenir en los mecanismos de producción y retroalimentación del sistema perturbador "SP", ya que permitirá prevenir su ocurrencia y disminuir su impacto;

    b) *Mitigación*. El riesgo depende de la vulnerabilidad del sistema afectable "SA", así, la reducción de riesgos depende de la posibilidad de cambiar la relación entre el sistema perturbador "SP" y el sistema afectable "SA", al impedir o desviar el canal de transferencia de los impactos de las calamidades, y/o de reforzar al sistema afectable "SA", con el fin de disminuir los posibles efectos adversos de dichos impactos y aminorar la intensidad de los daños.

2) *Restablecer la situación normal*, durante y después de la respuesta, que engloba los objetivos de auxilio o rescate y de recuperación:

    a) *Auxilio o rescate*. Se da en la fase de respuesta, y consiste en atender las situaciones de emergencia que ocasiona un desastre, está integrado por funciones basadas en el monitoreo y pronóstico de los sistemas "SA" y "SP", como son: alertar sobre la probable situación de emergencia o su inminente ocurrencia; reconocer los daños para estimar recursos y actualizar los planes de auxilio; concretar los planes de emergencia en busca de respuestas oportunas y adecuadas; coordinar esfuerzos de auxilio, seguridad, rescate, restablecimiento del funcionamiento de servicios básicos, atención médica, aprovisionamiento de elementos que sustentan necesidades básicas y comunicación de emergencia; la reconstrucción inicial y vuelta a la normalidad, que busca recuperar y mejorar las condiciones de bienestar al rehabilitar los sistemas de subsistencia y servicios de soporte de vida, afectados por el desastre.

    b) *Recuperación*. Concluye la fase de emergencia, se da en el control de la transición del estado de retorno al buscar la situación normal. Durante esta fase, se destaca la necesidad de fundamentar, diseñar y organizar el proceso de reconstrucción, así como mejorar sustancialmente el estado de seguridad y salvaguarda de la zona afectada.

Una de las principales funciones del sistema de gestión es el control de transiciones de un estado a otro en el sistema afectable (definidos en la sección 2.3.3) a través de estados propios del sistema y una serie de actividades orientadas a regresar al sistema afectable de un estado de desastre, insuficiente o de retorno, al estado normal:

- Cuando el sistema afectable se encuentra en estado normal el sistema de gestión se encuentra en estado de gestión normal;
- Cuando el sistema afectable se encuentra en estado normal y existe una transición imprevista que lo dirige hacia un estado insuficiente, o bien, existe un aviso sobre la posibilidad de ocurrencia de una calamidad, que lo lleve al estado de desastre, el sistema de gestión pasa a un estado de alarma;
- Cuando se desea regresar al sistema afectable del estado insuficiente al normal, el sistema de gestión realiza actividades de mantenimiento correctivo;
- Cuando el sistema afectable pasa a un estado de desastre, el sistema de gestión pasa a un estado de emergencia;
- Cuando el sistema afectable se encuentra en el estado de desastre y se declaró el estado de emergencia, se realizan las actividades de rescate que lo lleven a un estado de retorno;
- Para llevar del estado de retorno al estado normal al sistema afectable, el sistema de gestión realiza actividades de recuperación, lo que disminuye el estado de emergencia;
- Para llevar del estado de desastre al normal se realizan actividades de rescate y de recuperación.

En la tabla 2, se resumen estos estados y actividades del sistema de gestión, en relación con los estados del sistema afectable:

Estados del sistema afectable		Transición	Estado del sistema de gestión	Actividades del sistema de gestión
Estado Inicial	Estado Final			
Normal			Normal	
Normal	Normal c/aviso de calamidad	Imprevista	Alerta	
Normal	Insuficiente	Imprevista	Alerta	
Insuficiente	Normal	Controlada		Mantenimiento correctivo
Normal, Insuficiente, Retorno	Desastre	Imprevista	Emergencia	
Desastre	Retorno	Controlada		Rescate, se comienzan con los servicios de auxilio
Retorno	Normal	Controlada		Recuperación, disminuyendo el estado de emergencia
Desastre	Normal	Controlada		Restablecimiento, recuperación+rescate

Tabla 2. Estados y actividades del sistema de gestión
Fuente: Elaboración propia.

De esta manera el estado de emergencia es un estado importante del sistema de gestión para el control de desastres; se puede conceptualizar en cinco etapas, explicada en la figura 11.

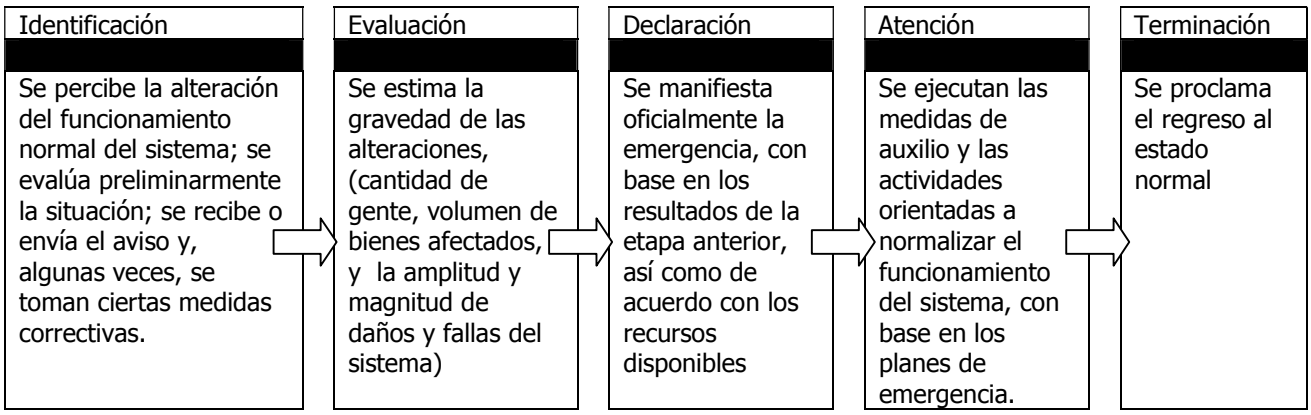

Figura 11. Etapas del estado de emergencia
Fuente: Elaboración propia.

Para lograr los objetivos de reducción de riesgos y de restablecimiento, se debe definir la estructura organizativa del sistema de gestión, con las atribuciones y responsabilidades de sus componentes, así como el conjunto de actividades, integradas en planes y programas, que deben ser realizadas antes, durante y después de un desastre. Esta estructura se conforma por un conjunto de diversos organismos, que tienen injerencia en los asuntos relevantes.

Idealmente se concibe como un sistema jerárquico piramidal en el que se considera por lo menos, tres niveles:

1) *Consultivo*. Asesora al tomador de decisiones en lo relacionado con; la identificación de la problemática; determinación de prioridades y definición de alternativas de solución; definición y recomendación de políticas, estrategias y acciones prioritarias; aprobación de los programas generales de reducción de riesgo y restablecimiento, y; sobre estimaciones de presupuestos;

2) *Ejecutivo*. Constituye la parte medular de la estructura, al ser responsable por coordinar y dirigir la organización, planeación y operación de las actividades de prevención y de atención de desastres, así como de su realización;

3) *Participativo*. Busca aprovechar, organizar, coordinar y asegurar la amplia participación de los involucrados, antes, durante y después del desastre.

Por otro lado dicha estructura organizativa se complementa con la gestión de actividades planeadas, a través de programas de reducción de riesgo y restablecimiento ante desastres; cada programa debe integrar: objetivos (finalidad perseguida); políticas (principios y lineamientos que apoyen el logro de los objetivos); estrategias (cursos de acción); alcances (especificación de resultados esperados en tiempo y espacio); acciones (actividades para

asegurar los alcances); actividades (acciones) y; responsabilidades (roles dentro del programa). Se identifican tres tipos de programas:

1. *Por objetivo.* Pueden ser: de *prevención*, en donde antes de la ocurrencia de un desastre se busca eliminar o minimizar la presencia de fenómenos destructivos y sus posibles daños; de *auxilio*, en donde al presentarse un desastre, se busca rescatar a los elementos afectados (personas, bienes, etc.) así como proteger y rehabilitar los servicios básicos y equipamiento estratégico, y; de *apoyo*, que busca coadyuvar a la elaboración, implantación, ejecución y actualización de los subprogramas de prevención y auxilio en forma eficaz y eficiente.

2. *Por el nivel y compromisos de participación.* Pueden ser: *nacionales*, elaborados por dependencias u organismos federales que constituyen fuentes potenciales de peligro; de *entidades federativas o regionales*, elaborados por los estados; *municipales o delegacionales*, cuyo ámbito de competencia se suscribe a un municipio o delegación.

3. *Por su ámbito.* Pueden ser: *generales o externos*, cuyos objetivos son proteger a los elementos que se encuentran en peligro así como asegurar el funcionamiento de los sistemas de subsistencia y de los que dan el servicio estratégico indispensable, y; *particulares o internos*, con el objetivo de proteger a los elementos que se encuentran bajo peligro en las instalaciones o en zonas de influencia adversa de la institución.

2.3.5 Estudios de riesgo

Una vez establecidos los conceptos relevantes sobre el sistema perturbador, el afectable y el de gestión, involucrados en el fenómeno del desastre, se pueden abordar las bases metodológicas para alcanzar los objetivos de *evaluación y reducción del riesgo*, el cual se debe tanto a la propensión del sistema expuesto a las diversas calamidades como a la vulnerabilidad y complejidad de sus componentes integrantes, ante los impactos de dichas calamidades y los daños que pueden ser ocasionados.

Un aspecto importante, entonces, en el estudio de riesgos es la identificación y evaluación de los daños que pueden ser causados en el sistema afectable por una calamidad, fenómeno destructivo o amenaza, y que son una manifestación del desastre. Los daños se pueden clasificar en relación con:

- El *objetivo dañado.* Pueden ser: *humanos* (los que sufren los individuos en su integridad física y mental); *materiales* (causados a los bienes); *productivos* (se ocasionan en la producción de bienes o generación de servicios); *ecológicos* (causados a la conservación de sistemas ecológicos y a su equilibrio dinámico); *sociales* (sufridos por la sociedad), y; *políticos* (sufridos por partidos políticos y personas públicas).

- El *tiempo.* Pueden ser: *directos*, generados inmediatamente al ocurrir un desastre y se manifiestan a corto plazo, e; *indirectos*, generados en un tiempo posterior al desastre y se revelan a largo plazo.

- El *costo económico.* Pueden ser: *primarios*, que corresponden al costo causado propiamente por el daño, y; *secundarios*, en donde el costo corresponde al rescate y recuperación.

Otro aspecto relevante para el estudio de riesgos es la *vulnerabilidad*, que se entiende como la susceptibilidad al daño, en este caso, es la facilidad con que el sistema afectable puede cambiar de un estado normal a uno de desastre ante los impactos de una calamidad.

De esta manera la vulnerabilidad constituye una característica de la relación entre el nivel de daños y la intensidad del impacto, la figura 12 muestra una curva en la que la primera parte se refiere a los niveles de intensidad del impacto que pueden ser absorbidos por el propio sistema, sin sufrir daños sensibles, mientras que la última, al caso de destrucción o inutilización completa del mismo. Esto puede ser idealizado por una recta, donde la vulnerabilidad es la pendiente de la recta y el daño es representado por la multiplicación de la vulnerabilidad por el término independiente (I - Io), como se muestra en la figura 13.

En términos generales la vulnerabilidad depende de:

- La vejez o deterioro del sistema, que generalmente sólo puede ser estimada con una inspección periódica de campo;
- El mantenimiento y reforzamiento para contrastar el deterioro;
- Cambio de entorno o uso, que puede influir sobre las características de operación de los elementos del sistema.

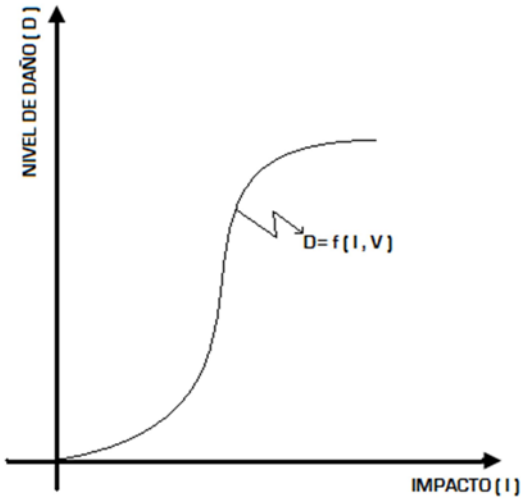

Figura 12. Gráfica de vulnerabilidad
Fuente: Gelman O. (1996)

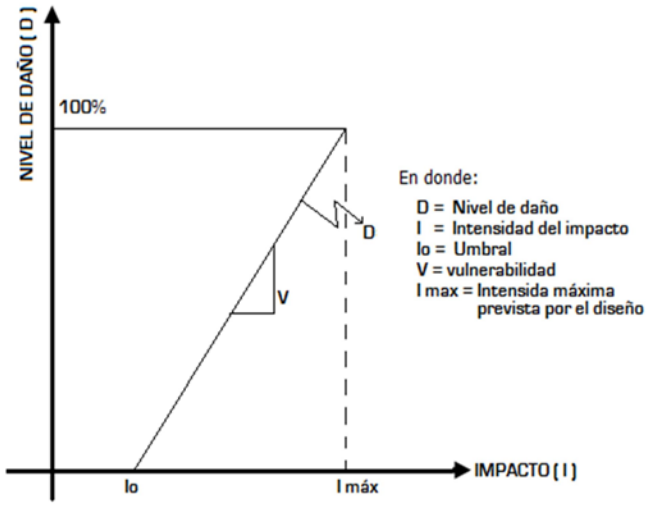

Figura 13. Gráfica idealizada de vulnerabilidad
Fuente: Gelman O. (1996)

La *estimación de riesgos*, no es más que la evaluación anticipada de las alteraciones probables en el sistema afectado, resultantes de los impactos de los fenómenos destructivos a los cuales están expuestos. De acuerdo con el paradigma fundamental de desastre cualquier método de estimación de riesgos tiene que contemplar:

1. *Determinar las calamidades*, que pueden provocar los daños, y evaluar su peligrosidad. Es posible considerarlas como un todo agregado y evaluar los daños en el sistema expuesto ante este todo, o desglosar una calamidad hasta un nivel grande de detalle, analizando cada uno de sus impactos por separado. El desglose depende del pronóstico requerido, de la información disponible y del estado de desarrollo de la disciplina correspondiente.

2. *Describir al sistema expuesto*, en donde pueden manifestarse los daños como efectos de los impactos de las calamidades. De la misma manera, puede llevarse a un nivel global o en cada uno de sus elementos, dependiendo también, de la precisión y confiabilidad del pronóstico requerido, mientras menor sea el elemento básico considerado mayor será la precisión del pronóstico resultante.

3. *Estimar los daños probables*, a través de procedimientos de evaluación de la interrelación de la calamidad, del probable resultado de la eventual interacción entre el impacto del fenómeno destructivo y el sistema expuesto. Los métodos de pronóstico de daños existentes se basan en:

   - *Uso de expertos*, cuando una persona, o grupo, con un amplio conocimiento y experiencia en el área, basándose en la expresión de su juicio, realiza la evaluación de los efectos de los impactos de una calamidad sobre un sistema expuesto. Dependiendo de la experiencia de los expertos, la confiabilidad y precisión de este tipo de métodos aumenta considerablemente

- *Uso de modelos*, cuando el proceso de evaluación se basa en la investigación de un objeto artificial, llamado modelo, el cual sustituye al sistema real, de tal forma que su estudio permite hacer conclusiones sobre el comportamiento sobre los posibles daños del sistema real y la evaluación de la vulnerabilidad. Pueden ser:

  - ✓ *Fenomenológicos o de caja negra*, que presentan al sistema en su totalidad, a través de una función matemática, un programa de cómputo o un objeto físico, por mencionar algunas realizaciones, en este caso, la estimación de riesgos son frecuentemente estadísticos, se estima como un promedio de los diversos daños que han ocurrido por el mismo fenómeno destructivo en el transcurso de muchos años, lo que implica la necesidad de contar con datos históricos confiables o por medio de datos empíricos que resultan de ensayos y pruebas en laboratorios; se debe asegurar que se trata del mismo sistema afectable y que, en el transcurso de los años, se han empleado los mismos procedimientos y técnicas de observación y evaluación del peligro.

  - ✓ Estructurales o de caja transparente, que permitan explicar, o por lo menos, pronosticar el funcionamiento del sistema en su totalidad; el riesgo se calcula a través de la evaluación de la magnitud del impacto, así como por medio de un análisis estructural del sistema expuesto, esto es, se identifican los subsistemas, partes, componentes y elementos con sus interrelaciones y sus comportamientos, y se evalúan los pesos de sus contribuciones a la vulnerabilidad total del sistema con base en:

    - ❖ El tipo de daño considerado (un mismo elemento puede tener distintos pesos para los diferentes tipos de daño);

    - ❖ Sus relaciones de peligrosidad (elementos que por sí mismos pueden no tener un peso significativo, sin embargo, su falla o daño fácilmente pueden provocar nuevos daños en los elementos que lo rodean o que están conectados a éste).

  De esta manera, la identificación del *integrante crítico*, que es un componente y/o elemento muy importante y, a la vez, muy vulnerable, permite tomar las medidas anticipadas que permiten disminuir daños probables.

  Ante situaciones en las que el concepto de vulnerabilidad para un sistema en su totalidad se pierde, en lugar de considerar la susceptibilidad al daño se puede recurrir a la capacidad del sistema para mantener su funcionamiento ante fenómenos destructivos, en este sentido, se pretende conocer la probabilidad de alteración o falla sustancial en el funcionamiento o rendimiento de un sistema en su totalidad ante diversas perturbaciones, empleando entonces el concepto de confiabilidad funcional, la cual se calcula como una función de la

organización estructural del sistema y de la vulnerabilidad de los elementos que lo integran, así como de la intensidad de los fenómenos destructivos; proporciona una medida de la capacidad del sistema por mantener los parámetros substanciales de su operación en ciertos márgenes. Para su determinación es necesario conocer el estado y funcionamiento actual de los elementos, componentes, partes y subsistemas que conforman al sistema, principalmente de sus condiciones de seguridad, mantenimiento y operación.

La precisión y confiabilidad de las estimaciones arrojadas por cualquier método dependerán de la profundidad y detalle empleados en el estudio, un buen pronóstico no es el más preciso y confiable, sino aquél que proporciona la información adecuada para el correspondiente nivel de toma de decisiones de acuerdo con los recursos disponibles, de acuerdo con los horizontes de tiempo y las necesidades de planeación se distinguen tres tipos básicos de pronósticos:

- *A corto plazo*, se refiere a la información sobre la ocurrencia en horas o días de una calamidad, sirve para establecer el estado de alerta en el que se presenta la movilización de cuerpos especializados o voluntarios en la atención de emergencias, el aviso a la población y suspensión de servicios peligrosos, con el fin de poner en marcha los planes de emergencia.

- *A mediano plazo*, se refiere a la ocurrencia de un desastre en semanas o meses, se utiliza para estimar los daños probables de los sistemas de subsistencia, con el fin de reforzarlos, mejorar la ubicación y operación de los sistemas de monitoreo, y realizar la intervención oportuna en los mecanismos productores de calamidades.

- *A largo plazo*, se refiere a la probable ocurrencia de un desastre en los siguientes años, se aprovecha para priorizar los estudios de desastres, así como para mejorar los códigos, reglamentos, manuales y procedimientos de construcción de sistemas, dando un énfasis especial a la elaboración de políticas de uso del suelo y al desarrollo de planes de protección y restablecimiento.

ESTUDIO COMPARATIVO DE LAS METODOLOGÍAS DE EVALUACIÓN DE RIESGOS Y PROPUESTAS DE ADECUACIÓN PARA LA METODOLOGÍA CIDETES

CAPÍTULO 3

El presente capítulo se divide en tres secciones: en la primera se caracterizan funcional y estructuralmente cuatro metodologías utilizadas para la evaluación de riesgos, incluida la metodología CIDETES; en la segunda sección, se realiza un análisis comparativo de las cuatro metodologías a través de cuatro criterios, seleccionados con base en lo tratado en el capítulo anterior, y; finalmente en la tercera se presentan las propuestas de mejora como resultado del análisis comparativo y de la teoría expuesta, también en el capítulo anterior.

3.1 Caracterización de las metodologías

Las metodologías seleccionadas para ser caracterizadas estructural y funcionalmente, son las siguientes:

- Security Vulnerability Assessment (SVA);
- MOSLER;
- Risk Assessment Methodology (RAM);
- CIDETES.

La metodología SVA fue elegida por el sector al cual está dirigida (petrolero y petroquímico), que resulta relevante por uno de los proyectos que se estaba desarrollando al momento de la realización de este trabajo de investigación. La metodología MOSLER es de las más utilizadas en la evaluación de riesgos, incluso aplicada por el mismo CIDETES. Por su parte la metodología RAM, que ha sido desarrollado por una de las instituciones más reconocidas en el ámbito de la seguridad física, es aplicada a una gran variedad de áreas, que van desde cárceles, industria química, industria eléctrica, en comunidades, entre otras.

3.1.1 Metodología SVA (Security Vulnerability Assessment)

Esta metodología fue desarrollada por el "American Petroleum Institute" "API" y la "National Petrochemical and Refiners Association" "NPRA", para la industria petrolera y petroquímica en Estados Unidos.

Caracterización funcional

La metodología se define como un proceso sistemático realizado por un equipo interdisciplinario, que busca:

- ✓ Identificar y analizar los peligros de seguridad, así como las amenazas y vulnerabilidades que enfrenta una instalación;
- ✓ Determinar la probabilidad de que un adversario explote con éxito las vulnerabilidades de la instalación;
- ✓ Evaluar el grado resultante del daño o impacto que se manifiesta en consecuencias, así como las medidas y estrategias referentes a la protección de las instalaciones;

- ✓ Establecer juicios sobre lo que se puede hacer en relación con el grado de riesgo y las medidas necesarias para su reducción o mitigación.

Esta metodología no necesariamente realiza una evaluación cuantitativa del riesgo, generalmente se realiza cualitativamente a través del criterio de expertos y entrega un resultado cualitativo, por otro lado, no establece las medidas de seguridad, sugiere medios para identificar, analizar y reducir las vulnerabilidades.

Caracterización Estructural

El proceso de SVA es una metodología basada en el riesgo y en el rendimiento, que se realiza en 5 pasos generales, y un paso de preparación, mostradas en la figura 14, las cuales son:

0. Preparación de la SVA;
1. Caracterización de Activos;
2. Evaluación de amenazas;
3. Análisis de Vulnerabilidad;
4. Evaluación de Riesgos;
5. Análisis de las medidas de protección existentes y propuestas de mejora.

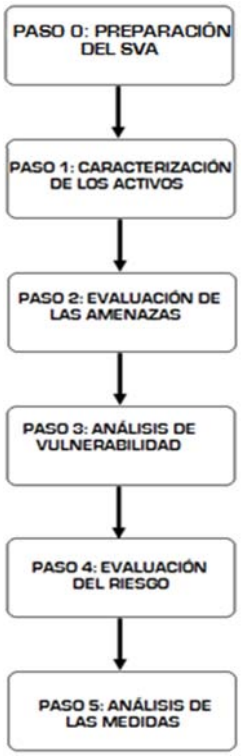

Figura 14. Etapas de la metodología SVA
Fuente: Elaboración propia

Paso 0: Preparación del SVA

Antes de realizar el estudio se lleva a cabo una serie de actividades que buscan garantizar un análisis eficiente y preciso, considerando factores y requisitos importantes para su éxito, a través de una planeación, en donde se establecen objetivos y alcances. Las etapas de preparación son:

0.1) **Definición del equipo de trabajo** (selección y conformación de grupo de expertos en materia de seguridad);

0.2) **Establecimiento de objetivos, ámbito y alcance del estudio**;

0.3) **Recolección de datos, revisión e integración** (obtención de los datos necesarios relacionados con la seguridad de la instalación sobre posibles actos no deseados previstos o que ya hayan ocurrido). Se identifican 4 sub-pasos:

- ✓ **Identificación del origen de los datos** o fuentes de información (la propia instalación, un sistema de información, registros de operación, fuentes externas);
- ✓ **Identificación de los datos necesarios** (tipo y cantidad de datos requeridos que dan soporte al estudio);
- ✓ **Localización de los datos requeridos** (identificar y ubicar dónde se pueden encontrar las formas y formatos en que se presenta la información necesaria)
- ✓ **Recolección y revisión de los datos** (obtención de los datos confiables, marcando aquellos a revisar e indicando cuales no pudieron ser obtenidos)

0.4) **Análisis de datos sobre incidentes de seguridad anteriores en el sitio** a través de documentos históricos o estadísticas, en medida de su disponibilidad, con la finalidad de generar perspectivas sobre vulnerabilidades potenciales y tendencias.

0.5) **Inspección del sitio** para obtener información (sobre iluminación, condiciones de la zona de vecinos, etc.) que permita comprender y determinar vulnerabilidades.

0.6) **Recopilación y análisis de información sobre amenazas** (provistas por el gobierno, la compañía, o autoridades locales).

Paso 1: Caracterización de Activos

En este paso se caracterizan las instalaciones con la finalidad de identificar y analizar tanto los activos de la empresa como los peligros a los que están expuestos, su grado de atracción, las posibles consecuencias y su gravedad, así como la infraestructura con la que se cuenta y las capas de protección existentes, con la finalidad de seleccionar rigurosamente los activos que

sólo requieren medidas generales de seguridad y aquellos que requieren medidas más específicas. Se generará entonces una lista de posibles activos críticos. Los sub-pasos que se llevan a cabo aquí son:

1.1) **Identificación de los activos críticos**, enlistando y analizando los posibles activos que representan un valor relevante para las instalaciones (pueden ser procesos, personal o bienes materiales) que hacen posible su operación y funcionamiento;

1.2) **Identificación de funciones Críticas o esenciales de la instalación**, determinando los bienes o activos que realizan y/o apoyan dichas funciones críticas;

1.3) **Identificación de la infraestructura crítica** (interna y externa) **y las interdependencias que dan soporte a las operaciones críticas** de cada activo (pueden ser el suministro eléctrico, telecomunicaciones, transporte, servicios de emergencia, etc.) [13];

1.4) **Evaluación de las medidas existentes** que tienen por función apoyar y proteger a los activos y a las funciones críticas, incluyendo las capas relevantes de los sistemas de seguridad física, informática, operativa, administrativa, etc., y los procesos de protección existentes. El objetivo de esta etapa es reunir información sobre las estrategias utilizadas y su efectividad, con relación a la seguridad de las instalaciones, que permitirán formar una perspectiva para los pasos 3 y 5 de la metodología.

1.5) **Evaluación de Impactos**, consiste en determinar las posibles fuentes de riesgo y sus consecuencias (desde la interrupción, daño o incluso su pérdida) a través de los activos y funciones que son esenciales para la instalación. Se desarrolla una lista de activos, que representan un blanco u objetivo, y se clasifica el grado de severidad de las posibles consecuencias, generalmente expresadas o categorizadas en términos de efectos para la salud (mortalidad, heridas, etc.), efectos económicos debido a daños materiales, efectos ambientales, interrupción en la operación del negocio, entre otros.

1.6) **Selección de activos que sean objetivos o blancos**. Para cada activo identificado se analiza su *criticidad*, se construyen escenarios, auxiliándose en un formato como el mostrado en la figura 15, en el cual, en la primera columna se listan los activos que tengan una mayor probabilidad de ser atractivos y atacados (esta lista se utilizará en el paso 3); en la segunda columna se describe su criticidad, con base en la importancia o valor del activo y las posibles consecuencias, en caso de ser atacado; en la última columna se clasifica la severidad del activo, utilizando una escala del 1 al 5, donde 1 es el valor más bajo y 5 es el valor más alto.

[13] Para la determinación de esta información se siguen ciertos formatos, que pueden ser consultados en la guía sobre esta metodología "http://www.npra.org/docs/publications/newsletters/SVA_2nd_edition.pdf", consultada el 13 febrero de 2011

Paso 1 : Formato para activos Criticos y su criticidad		
Activos Críticos	Criticidad	Clasificación de la Severidad

Figura 15. Formato de Criticidad
Fuente: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

Paso 2: Evaluación de amenazas

Con la finalidad de inferir y estimar la probabilidad de los tipos de ataque potenciales de adversarios, en contra de los activos de las instalaciones bajo estudio, con base en factores como la capacidad del adversario, su intención y el impacto de dicho ataque; así como, establecer las medidas de salvaguarda y determinar las prioridades sobre las necesidades de los programas de seguridad, planeación y asignación de recursos; en este paso se identifican las posibles amenazas (internas, externas, y posibles combinaciones), las cuales se evalúan en términos de los activos de la compañía y se determina el grado de atracción de dichos activos con respecto a cada adversario identificado. Esta evaluación de amenazas es acompañada por una evaluación de vulnerabilidades (realizada en el paso 3), como soporte para la evaluación de las medidas para la gestión de dichas amenazas (realizada en el paso 5). Tres sub-pasos integran este proceso:

2.1) **Identificación de adversarios**. Se evalúa la información sobre las amenazas externas, internas (con mayor énfasis por tener conocimiento y acceso sobre las instalaciones), o bien una combinación de ambas; se categorizan e identifican aquellas cuyos adversarios (conocidos y potenciales) con intensión y/o capacidad de comprometer la seguridad de las instalaciones y causar daños.

2.2) **Caracterización del adversario**. Aquí se desarrolla una matriz en la que se proporciona una clasificación y valoración global de las amenazas, al evaluar cada clase de adversario identificado, tomando en cuenta factores como su naturaleza, historia (operativa, en las instalaciones), capacidades (métodos, medios, acciones posibles, inteligencia), fortalezas, debilidades, motivación, etc.

Paso 2. Formato para la Evaluación de Amenazas								
Tipo de adversario	Origen	Historia general de la Amenaza	Historia de la amenaza en el sitio de estudio	Acciones Potenciales	Capacidad de los adversarios	Intensiones o motivaciones del adversaio	Evaluación Global	Clasificación

Figura 16. Formato para la evaluación de amenazas
Fuente: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

El formato mostrado en la figura 16, se utiliza para la realización de los sub-pasos anteriores; para cada tipo de adversario expresado en la columna 1, de izquierda a derecha, se analiza y documenta lo siguiente:

- Columna 2, "origen": La fuente de ataque (si es externa a la instalación, interna a la instalación, o una combinación);

- Columna 3, "historia general de la amenaza": Los antecedentes sobre la amenaza que el tipo de adversario pudiera manifestar hacia instalaciones similares en ámbitos locales o internacionales;

- Columna 4, "historia de la amenaza en el sitio de estudio": Los antecedentes de la amenaza hacia las instalaciones de interés;

- Columna 5, "acciones potenciales": Descripción de las posibles acciones potenciales que el adversario pudiera llevar a cabo;

- Columna 6, "capacidad de los adversarios": Descripción de la capacidad que el adversario pudiera tener, en referencia con posibles armas, tácticas, etc.;

- Columna 7, "Intensiones o motivaciones del adversario": Posibles motivaciones o intenciones que pudiera tener el adversario para perpetrar un ataque;

- Columna 8, "evaluación global": Descripción global de la amenaza;

- Columna 9, "Clasificación": Valoración de la amenaza con base al sistema establecido en la tabla 3, mostrada a continuación:

Clasificación de la Amenaza	Descripción
1: Muy Bajo	Indica que no hay evidencia creíble de la capacidad o intención de alguna amenaza, además sin antecedentes de amenazas reales o planeadas contra los activos.
2: Bajo	Indica que existe una baja amenaza contra los activos y que adversarios poco conocidos representan una amenaza para los activos.
3: Medio	Indica que existe una posible amenaza para el activo basado en el deseo del adversario para comprometer los activos.
4: Alto	Indica que existe una amenaza creíble contra el activo basado en el conocimiento de la capacidad del adversario y la intención de atacar los activos
5: Muy Alto	Indica que existe una amenaza creíble contra el activo y que el adversario demuestra la capacidad y la intención de lanzar un ataque, y que los activos son seleccionados (son el objetivo) repetidamente con una frecuencia.

Tabla 3. Escala para determinar el nivel de la amenaza.
Fuente: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

Este sistema de clasificación, sin embargo, implica subjetividad y un problema de ambigüedad al no definir con precisión los niveles de clasificación en la escala de amenazas, por ejemplo, el valor 2 "bajo", se describe como la existencia de una "amenaza baja"; o bien, en los valores 4 y 5, "alto" y "muy alto", se habla de una "amenaza creíble" sin definir a que se refiere dicho término.

2.3) **Análisis del grado de atracción del activo seleccionado como objetivo**. Como una parte importante para determinar la probabilidad de ataque, al igual que el análisis de vulnerabilidades y de consecuencias, se realiza una evaluación, desde la perspectiva del adversario, del grado de atracción sobre cada uno de los activos críticos (identificados en el paso 1), que permita determinar los factores que los hacen más o menos atractivos, como pueden ser su alto valor económico, emblemático, funcional u operativo, lo cual varia en relación con el tipo de amenaza y adversario, ya que pueden variar las motivaciones, intensiones y capacidades. Para este sub-paso el formato mostrado en la figura 17 es utilizado para expresar el grado de atracción encontrado con base en la escala mostrada en la tabla 4.

Nivel de Atracción	Descripción
1: Muy Bajo	El adversario no tendría un nivel de interés en el activo
2: Bajo	El adversario tendría algún grado de interés en el activo
3: Medio	El adversario tendría un grado moderado de interés en atacar a los activos
4: Alto	El adversario tendría un alto grado de interés en el activo
5: Muy Alto	El adversario tendría un muy alto grado de interés en el activo

Tabla 4. Escala para la clasificación del nivel de atracción que tiene el adversario por los activos.
Fuente: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

Sobre esta escala, al igual que la mostrada en la tabla 3 del sub-paso anterior, presenta el mismo problema de definición, en el que no sólo se manifiesta la subjetividad inherente a este tipo de estudios por el hecho de depender de las apreciaciones de quien los realice, sino también la ambigüedad, puesto que no resulta claro, por ejemplo, que tan alto es "muy alto grado de interés" del nivel 5, para diferenciarse de "alto grado de interés" del nivel 4.

Paso 2 : Formato para determinar el grado de atracción sobre los activos y su clasificación									
			Atractividad del activo (s)						
Activos Críticos	Funciones Criticidad	Clasificación de la Severidad del Activo	Adversario 1	Grado de Atracción del Adversario 1	Adversario 2	Grado de Atracción del Adversario 2	Adversario 3	Grado de Atracción del Adversario 3	Grado de Atracción Sobre el Activo Crítico

Figura 17. Formato para determinar el grado de atracción sobre los activos
Fuente: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

Las columnas 1 a 3, de izquierda a derecha, del formato mostrado en la figura 17, se repiten del formato utilizado en el paso 1; en la columna 4 "adversario X", se documentan las razones por las que el activo en particular es atractivo (o poco atractivo) para el adversario; mientras que en la columna 5 "grado de atracción del adversario X", se clasifica el grado de atracción, con base a la escala presentada en la tabla 4; la columna 4 y 5 se repiten conforme al número de adversarios identificados; finalmente en la última columna se establece la clasificación general sobre el grado de atracción, con base en la misma escala mostrada en la tabla 4, sólo que aquí normalmente se considera el valor más alto, de los valores asignados individualmente al grado de atracción de cada adversario, aunque en ocasiones también se considera que la suma de todos los valores asignados al grado de atracción puede hacer que el activo sea más atractivo;

Paso 3: Análisis de Vulnerabilidad

El análisis que se realiza en este paso incluye la vinculación "activo crítico – amenaza" para identificar posibles vulnerabilidades relacionadas con eventos de seguridad. Una vez que se identifica cómo un evento o ataque puede ser inducido, se debe determinar cómo el adversario podría ejecutar el acto; al conocer la consecuencia más grave que puede ser causada por la amenaza de un adversario y el grado de atracción que tiene el adversario por el activo, es posible aplicar un enfoque basado en escenarios para realizar el análisis de vulnerabilidad y de riesgos, debido al nivel de detalle con que permite entender cómo el evento no deseado puede llevarse a cabo.

En este paso se realizan tres sub-pasos:

3.1) **Definición de escenarios y evaluación de las consecuencias específicas**. Se comienza con una inspección del sitio en el que se hará el estudio para recoger información específica requerida; el equipo de expertos plantea hipótesis (desde su perspectiva) sobre las consecuencias que puedan derivarse de los eventos de seguridad no deseados, dada una amenaza, para un determinado activo. Se construye el escenario como una secuencia de eventos, que incluyen al acto malintencionado específico, su causa, las posibles situaciones relativas entre cada activo y amenaza asociada, la categoría de la amenaza (terrorismo, robo, etc.), el tipo de adversario (externo, interno, combinación, etc.) y sus posibles consecuencias; se considera también el reto que representan las medidas de seguridad existentes, de las cuales se evalúa su integridad, confiabilidad y capacidad para disuadir, detectar, y retardar. Los escenarios son valorados en términos de la gravedad de las consecuencias y la probabilidad de ocurrencia de eventos de seguridad, con base en un análisis cualitativo basado en el juicio y deliberación de los expertos.

3.2) **Evaluación de la efectividad de las medidas de seguridad existentes**. Se identifican las medidas existentes destinadas a proteger los activos críticos y se estiman los niveles de su efectividad en función de la reducción de las vulnerabilidades de cada activo respecto a cada amenaza o adversario.

3.3) **Identificación de vulnerabilidades y estimación de su grado**. Se identifican las posibles vulnerabilidades y el grado con el que cada activo crítico puede ser afectado por las amenazas que generan los adversarios.

En este paso se utiliza el formato mostrado en la figura 18, en el cual se recopila toda información que da forma al escenario; la tabla 5, muestra la escala utilizada para determinar el grado de vulnerabilidad para cada uno de los activos.

Nivel de Vulnerabilidad	Descripción
1: Muy Bajo	Indica que existen múltiples capas de medidas de protección y son efectivas para disuadir, detectar, retardar, y responder ante las amenazas, por lo que la posibilidad de que el adversario sea capaz de atacar al activo es muy baja.
2: Bajo	Indica que existen medidas de protección que son efectivas para disuadir, detectar, retardar, y responder, sin embargo, existe por lo menos una debilidad que un adversario sería capaz de atacar con un poco de esfuerzo para evadir las medidas.
3: Medio	Indica que aunque hay algunas medidas de protección que son efectivas para disuadir, detectar, retardar, y responder, no hay una aplicación completa y efectiva de estas estrategias de seguridad y así los activos o las medidas existentes probablemente podrían estar comprometidos.
4: Alto	Indica que hay algunas medidas de protección para disuadir, detectar, retardar, responder pero no hay una aplicación completa o efectiva de estas estrategias de seguridad por lo que es relativamente fácil para el adversario atacar con éxito al activo.
5: Muy Alto	Indica que no hay medidas de seguridad para disuadir, detectar, retardar, y responder a la amenaza, por lo que un adversario sería capaz de atacar un activo crítico fácilmente.

Tabla 5. Escala para determinar el grado de vulnerabilidad de los activos
Fuente: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

Sobre esta escala, el nivel 2 "bajo", proporciona una definición que sí específica una unidad de medición que permite clasificar dándole un valor a la vulnerabilidad, sin embargo, en el nivel 1 "muy bajo", nuevamente se cae en ambigüedades al incluir en su definición que la posibilidad de que el adversario explote las vulnerabilidades del activo es muy baja, además, entre el nivel 3 "medio" y 4 "alto" no se define claramente la diferencia entre ellos.

Paso 3 al 5 : Formato para el Análisis de Vulnerabilidad, Clasificación del Riesgo y Medidas de Seguridad											
Activo Crítico:											
Grado de Atracción:											
Tipo de Evento de Seguridad	Categoría de la amenaza	Tipo de adversario	Evento no Deseado	Consecuencias	Clasificación de la severidad	Medidas de seg. existententes	Vulnerabilidad	Clasificación de la Vulnerabilidad	Probabilidad	Riesgo	Propuesta de medidas de seg.

Figura 18. Formato para el análisis de vulnerabilidad, clasificación y medidas de seguridad
Fuente: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

En relación con la construcción del escenario y el formato mostrado en la figura 18, la información manejada es la siguiente:

- En el campo "activo crítico" se coloca el nombre del activo para el cual se construirá el escenario, esto se realizará para cada uno de los activos identificados como críticos;

- En la columna "tipo de evento de seguridad" se describe el tipo acto malicioso del que se trate (puede ser robo, explosión, etc.);

- En la columna "Categoría de la amenaza", se categoriza al adversario (pueden ser terroristas, empleados activistas o descontentos, etc.);

- En la columna "Tipo de adversario", el cual puede ser: (I) Interno, (E) Externo, o (C) una combinación de los dos anteriores;

- En la columna "Evento no deseado", se realiza una descripción de la secuencia de eventos que tienen que ocurrir para violar las medidas de seguridad;

- En la columna "consecuencias", se realiza una descripción de las consecuencias del evento no deseado, considerando el éxito o fallo del ataque.

- En la columna "clasificación de la severidad", derivada del paso anterior el valor de la gravedad de las consecuencias identificadas.

- En la columna "medidas de seguridad existentes", se enlistan las medidas de seguridad identificadas con relación a la disuasión, prevención, retardo y respuesta, que evitan que los adversarios exploten las debilidades del activo y éste sea alcanzado;

- En la columna "vulnerabilidad", se enlistan las características que hacen vulnerable al activo (como las medidas de seguridad que pueden ser eludidas o no cumplen con su objetivo de seguridad);

- En la columna "clasificación de la vulnerabilidad", se obtiene el grado de vulnerabilidad encontrada en el escenario, con base en la escala mostrada en la tabla 5.

- Las tres columna restantes: "probabilidad", "riesgo" y "propuestas de medidas de seguridad", son llenados en los paso 4 y 5.

Paso 4: Evaluación de Riesgos

El siguiente paso es determinar el nivel de riesgo de que el adversario explote las debilidades del activo, dadas las medidas de seguridad existentes. Este paso se realiza en dos sub-pasos:

4.1) **Estimación del riesgo de un ataque con éxito**. Se estima el relativo grado de riesgo en función de dos factores:

1. El efecto esperado en cada activo identificado, que está a su vez en función de las consecuencias o impactos en las funciones esenciales de la instalación, ya sea con la interrupción o pérdida del activo crítico (evaluado en el paso 1);

2. La probabilidad de éxito del ataque, que es determinada a juicio por el grupo de expertos en función del grado de atracción del activo (evaluado en el paso 1), del nivel de la amenaza o adversario (evaluado en el paso 2), y el grado de vulnerabilidad de los activos (evaluado en el paso 3).

Una vez obtenida la severidad de las consecuencias y la probabilidad de éxito del ataque, se vinculan ambos valores a través de la matriz mostrada en tabla 6, con la intención de clasificar a los activos en niveles discretos de riesgo, como alto, medio o bajo, y completar el escenario iniciado en el paso 3.

Matriz de riesgos		**Severidad de las consecuencias**				
		5	4	3	2	1
Probabilidad de éxito del ataque	5	Alto	Alto	Alto	Medio	Medio
	4	Alto	Alto	Medio	Medio	Bajo
	3	Alto	Medio	Medio	Bajo	Bajo
	2	Medio	Medio	Bajo	Bajo	Bajo
	1	Medio	Bajo	Bajo	Bajo	Bajo

Tabla 6. Matriz de riesgos
Fuente: Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, Second Edition

4.2) **Establecimiento de prioridades a los riesgos**, con base en los grados relativos encontrados y la probabilidad de éxito de los ataques.

Un aspecto que resalta por su importancia es que no se define como se obtiene la probabilidad, solo se menciona que los expertos la determinan a juicio, además los valores que manejan, del 1 al 5, no representan como tal una probabilidad de ocurrencia.

Paso 5: Análisis de las medidas de protección existentes y propuestas de mejora

Con base en las vulnerabilidades y riesgos identificados en las instalaciones, que incluye las deficiencias entre la seguridad existente y la seguridad deseable, se recomiendan mejoras sobre las medidas de seguridad con la finalidad de reducir dicha vulnerabilidad y la probabilidad de éxito de un ataque; se consideran factores como el grado de reducción del riesgo, capacidades, eficiencia y costos de mitigación, su viabilidad, fiabilidad y facilidad de mantenimiento. Además se evalúan los méritos de las posibles medidas adicionales, mediante la inclusión y estimación de su efecto neto sobre la reducción de la probabilidad o la gravedad de los ataques. Esto se realiza en dos sub-pasos:

5.1) **Identificación y propuesta de medidas** para reducir las vulnerabilidades y por lo tanto los riesgos, considerando factores como:

- ✓ La reducción de la probabilidad de éxito de un ataque;
- ✓ El grado de reducción del riesgo previsto por las propuestas;
- ✓ La fiabilidad y facilidad de mantenimiento de las propuestas;
- ✓ Las capacidades y efectividad de estas propuestas;
- ✓ Los costos que implican las propuestas;
- ✓ La viabilidad de las propuestas.

5.2) **Establecimiento de la prioridad de las posibles mejoras**. Se Da prioridad a las alternativas para la implantación de las diversas opciones y se preparan recomendaciones a incluir en el informe final para que el decisor actúe.

Resultados y Seguimiento de la SVA

Los resultados de la SVA son los siguientes:

- Identificación de las vulnerabilidades de seguridad;
- Un conjunto de recomendaciones (si son necesarias) para reducir el riesgo.
- Los activos críticos identificados, sus riesgos y consecuencias;

Una vez que el SVA se ha completado, se da seguimiento a las mejoras recomendadas y a las medidas de seguridad, con la finalidad de que estén debidamente revisadas, y gestionadas hasta que sean resueltas. La resolución puede ser la adopción de las recomendaciones, la sustitución de otras mejoras que permitan alcanzar el mismo nivel de reducción de riesgo, o ser rechazadas.

3.1.2 Metodología MOSLER

Esta metodología es comúnmente usada en proyectos sobre seguridad física; se tiene una percepción de ser sencilla y fácil de seguir al momento de determinar el riesgo, ya que como característica, las escalas que utiliza, aunque subjetivas y ambigüas, resultan un tanto amigables para quien aplica la metodología. A pesar del uso frecuente en muchas instituciones y empresas, la literatura no ofrece información acerca de cómo surgió o quién la desarrolló, sin embargo, representa una herramienta ilustrativa en el rubro de la seguridad física.

Descripción funcional

Esta metodología permite llevar a cabo la identificación y evaluación de algunos factores que pueden influir en la manifestación del riesgo. Su análisis parte de una hipótesis en la que se da por hecho que una amenaza genera un evento no deseado de seguridad, sin embargo, no especifica cómo o por qué se ha elegido dicha amenaza, o por qué actuaría en contra del activo (o conjunto de activos), de esta manera, no profundiza en el estudio de los elementos involucrados en la obtención del riesgo, y se deja de lado, incluso, aspectos importantes para una metodología de evaluación de riesgos, como lo son la caracterización del sistema en el que se puede presentar el evento no deseado (sistema afectable), el análisis de amenazas, el análisis de vulnerabilidades, o bien, sobre el sistema de seguridad física

Así, los resultados de esta metodología, entonces, se limitan al cálculo del riesgo, de forma cuantitativa y se proporciona una clasificación del mismo, sin realizar propuestas que permitan su reducción.

Descripción estructural

Se trata de una metodología secuencial compuesta por 4 etapas, en la figura 19, se muestra que cada etapa se apoya de los datos obtenidos en las fases que le preceden.

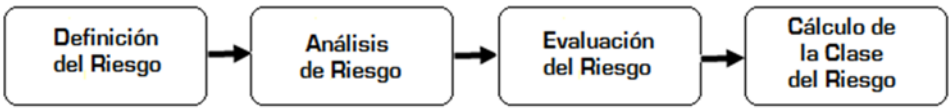

Figura 19. Etapas de la metodología Mosler.
Fuente: Elaboración propia.

Etapa 1. Definición del riesgo.

En esta etapa se identifican y definen los riesgos a los que se encuentra expuesta la entidad de interés, se establece su alcance, se identifican los bienes y los posibles daños que se pueden presentar; los bienes se refieren a aquello considerado como valioso y los daños a la variación que sufre el bien al tener una desviación de su valor.

Más que el riesgo en sí mismo, puesto que no es posible identificar y definirlo como tal, en esta etapa lo que se establece es una hipótesis sobre una amenaza y los activos

que puede llegar a afectar, y en la cual que se define un evento de seguridad, mismo que es analizado en la siguiente etapa.

Etapa 2 – Análisis del riesgo

En esta fase se definen seis criterios bajo los cuales se analizan factores relacionados con las amenazas, y con base en una penta-escala se cuantifica el grado en que estos factores influyen en dichos criterios. Los criterios son los siguientes:

Criterio de función. Se denota con una "F", y se valora el grado con que las consecuencias negativas o daños que puedan alterar o afectar la actividad o actividades de la entidad en estudio; la escala y valores utilizados son:

Muy gravemente	→	5
Gravemente	→	4
Medianamente	→	3
Levemente	→	2
Muy levemente	→	1

Criterio de sustitución. Se denota con una "S" y se valora si los bienes pueden ser sustituidos en caso de que las amenazas se manifiesten; la escala y sus valores son los siguientes:

Muy difícilmente	→	5
Difícilmente	→	4
Sin muchas dificultades	→	3
Fácilmente	→	2
Muy fácilmente	→	1

Criterio de Profundidad. Se denota con una "P" y se valora la perturbación y los efectos psicológicos que se pueden presentar y afectar a la imagen de la entidad en estudio; su escala y valores son:

Perturbaciones muy graves	→	5
Perturbaciones graves	→	4
Perturbaciones limitadas	→	3
Perturbaciones leves	→	2
Perturbaciones muy leves	→	1

Criterio de extensión. Se denota con "E" y se valora el alcance que llegarían a tener los daños o pérdidas, de manifestarse las amenazas, según su amplitud o extensión puede ser:

De alcance internacional	→	5
De carácter nacional	→	4
De carácter regional	→	3
De carácter local	→	2
De carácter individual	→	1

Criterio de agresión. Se denota con una "A" y se valora la probabilidad de que el riesgo se manifieste o materialice; su escala y valores son:

Muy alta	→	5
Alta	→	4
Normal	→	3
Baja	→	2
Muy baja	→	1

Criterio de vulnerabilidad. Se denota con una "V" y se valora la probabilidad de que se produzca un daño si se manifiesta la amenaza; su escala y valores son:

Muy alta	→	5
Alta	→	4
Normal	→	3
Baja	→	2
Muy baja	→	1

Al analizar hasta el momento esta metodología no solo presenta manejos equivocados sobre conceptos, las escalas que se utilizan en la clasificación de los criterios no definen las unidades de medición que permitan ubicar su valor. Para realizar una evaluación es necesario:

1) Establecer los criterios de comparación;
2) Definir la escala de medición, y;
3) Definir las unidades de medición.

Ahora bien, "criterio" dentro éste marco de evaluación, se refiere a la definición de los elementos, categorías o parámetros que nos permitirán realizar una comparación con lo que se pretende evaluar. En este sentido lo primero que hay que entender es qué se va a evaluar, resulta confuso en esta etapa saberlo, primeramente, partiremos del hecho que se evaluará el riesgo, entonces los criterios que define la metodología son:

1) Función
2) Sustitución
3) Profundidad
4) Extensión
5) Agresión
6) Vulnerabilidad

La escala de medición es nominal, y se define en un rango entre 1 y 5. El problema se presenta entonces en la definición de las unidades de medición:

- Para el criterio de función, se tendrían que definir las características que hacen que la función del sistema se vea afectada, no se puede decir simplemente "la función del sistema se ve afectada muy gravemente debido a las consecuencias negativas o

daños", se tiene que establecer cómo, cuándo o en qué momento, dichas consecuencias afectan dicha función "muy gravemente", "gravemente", "medianamente", "levemente" o "muy levemente", permitiendo discernir entre una u otra forma. Esto aplica para el criterio de sustitución y de profundidad.

- Para el criterio de extensión, en lo referente a las unidades de medición, solo restaría delimitar exactamente a que se refiere regional, local e individual, aunque eso dependerá del sistema que sea estudiado.

- Por otro lado, para el criterio de agresión, se pretende valorar la probabilidad de que se produzca un daño, estrictamente los valores que toma la probabilidad se encuentran en un rango entre 0 y 1; luego, si pretende "mapear" de una escala cualitativa a una cuantitativa, por ejemplo, si se dice que la probabilidad es "alta", se tiene que definir qué tan "alta" es, como para diferenciarla de "Normal", o bien, que "tan baja" es para diferenciarla de "Muy Alta".

- Para el criterio de vulnerabilidad, se pretende valorar la probabilidad de que se produzca un daño si se manifiesta el riesgo (ver definición de riesgo capítulo 2), lo cual no corresponde al concepto de vulnerabilidad, debido a que la vulnerabilidad no se determina por la probabilidad de que se produzca un daño, sino por un análisis sobre la mayor o menor facilidad que presenta el activo ante un ataque realizado por una amenaza, es decir, la susceptibilidad que un activo presenta al daño.

Ahora bien, como ya se analizó, lo que se pretende obtener con estos criterios es:

- ✓ El grado de afectación en la función del sistema estudiado;
- ✓ El grado de sustitución del activo ;
- ✓ El grado de perturbación causado en el sistema estudiado;
- ✓ El alcance de los daños;
- ✓ La ocurrencia de que se manifieste el riesgo (en realidad se trata de un evento no deseado);
- ✓ La ocurrencia de que se produzca un daño (se considera como vulnerabilidad, aunque está mal empleado el concepto).

Para lo cual no solo no se definen las unidades de medición, sino que tampoco se definen los criterios de comparación para determinarlas. Existe la posibilidad de que la metodologías se presenta en un sentido muy general, para que pueda aplicarse a una gran variedad de casos, y quede en quien lleva a cabo el estudio definir específicamente estas unidades y la adecuación en el manejo de los criterios, sin embargo, en la literatura consultada sobre su aplicación se encontró que se aplica literalmente como fue presentada en esta sección.

Etapa 3 – Evaluación del riesgo

En esta se etapa se cuantifica el riesgo en una serie de sub-pasos descritos a continuación:

1. **Cálculo del carácter del riesgo**. Se denota con una "C", y se obtiene al sumar la "importancia del suceso" (I), más "los daños ocasionados" (D), que son calculados con base en las valoraciones realizadas en la etapa anterior; la "importancia del suceso" (I) queda definida por el producto del valor asignado al "criterio de función" (F), por el valor asignado al "criterio de sustitución" (S); mientras que "los daños ocasionados" (D), quedan definidos por el producto del valor asignado al "criterio de profundidad" (P), por el valor asignado al "criterio de extensión" (E). Siendo:

$$C = I + D$$

En donde:

I = Importancia del suceso = $F \times S$
D = Daños ocasionados = $P \times E$

2. **Cálculo de la probabilidad**. Se denota con una "P", y se obtiene del producto del valor asignado al "criterio de agresión" (A,) por el valor asignado al "criterio de vulnerabilidad" (V). Siendo:

$$P = A \times V$$

   En la literatura consultada, no se establece que probabilidad se obtiene, se puede entender que se trata de la probabilidad de que un evento no deseado se realice con éxito; el valor obtenido (entre 1 y 25) no corresponde a una probabilidad.

3. **Cuantificación del riesgo considerado**. Se denota por "ER" y se obtienen de multiplicar los valores obtenidos en los dos sub-pasos anteriores, siendo:

$$ER = C \times P$$

Etapa 4 – Cálculo de la clase de riesgo

En esta etapa se clasifica el riesgo en función del valor obtenido en la etapa anterior, con base en la siguiente escala:

De 2 a 250	→	"Muy Bajo"
De 251 a 500	→	"Pequeño"
De 501 a 750	→	"Normal"
De 751 a 1000	→	"Grande"
De 1000 a 1250	→	"Elevado"

3.1.3 Metodología de Evaluación de Riesgos, Risk Assessment Methodology (RAM).

A principios de la década de 1970, los Laboratorios Nacionales Sandia estuvieron a cargo de desarrollar conceptos, tecnologías y soluciones para hacer frente a la preocupación de robo de materiales nucleares durante su transporte, para el Departamento de Energía "DOE", de Estados Unidos. Al mismo tiempo, la Fuerza Aérea de Estados Unidos inició junto con Sandia, un programa para llevar a cabo la investigación y desarrollo de sistemas de seguridad física, así como su implantación para la protección de sus activos críticos alrededor de mundo. A mediados de esa misma década el DOE designó a Sandia como laboratorio principal para el desarrollo de tecnología sobre seguridad física y lo financió para desarrollar capacidad técnica en el modelado de seguridad y análisis de sistemas, así como equipos y componentes de seguridad. De esta manera Sandia ha desarrollado métodos basados en el desempeño para diseñar y evaluar sistemas de protección física, mismos que se han aplicado en diversas entidades como lo son instalaciones gubernamentales, servicios de agua (presas federales, empresas de servicios públicos, etc.), prisiones, comunidades, sistemas de transmisión eléctrica, instalaciones químicas, entre otras.

Caracterización funcional

Esta metodología evalúa la vulnerabilidad de sistemas de protección o seguridad en instalaciones, con base en su rendimiento o eficacia; su objetivo es estimar el valor del riesgo asociado al sistema y determinar si se requieren mejoras, que implican una actualización cíclica del sistema, con la finalidad de reducir ese valor del riesgo. La metodología también es empleada para el diseño de sistemas de seguridad.

Descripción estructural

El proceso comienza con una caracterización de la instalación, incluyendo la identificación de los eventos no deseados y los activos críticos, después se definen y describen las amenazas para estimar la probabilidad de algún ataque hacia una instalación específica. Se estiman valores sobre las consecuencias que se pueden presentar. Se estima la efectividad del sistema de seguridad contra los ataques de los adversarios. Y por último se calcula el riesgo. En el caso de que el valor del riesgo se considere no aceptable (muy alto), la metodología agrega un proceso para identificar y evaluar mejoras de las actualizaciones del sistema de seguridad con el fin de reducir el riesgo. Esta metodología está constituida por 7 etapas o pasos, la figura 20 describe el orden y la secuencia de estos. Los pasos son:

1) Caracterización de las instalaciones;
2) Identificación de eventos no deseados y activos críticos;
3) Determinación de consecuencias;
4) Definición de amenazas;
5) Análisis de la efectividad del sistema de protección;
6) Estimación de riesgos;
7) Actualización del sistema y análisis del impacto de dicha actualización.

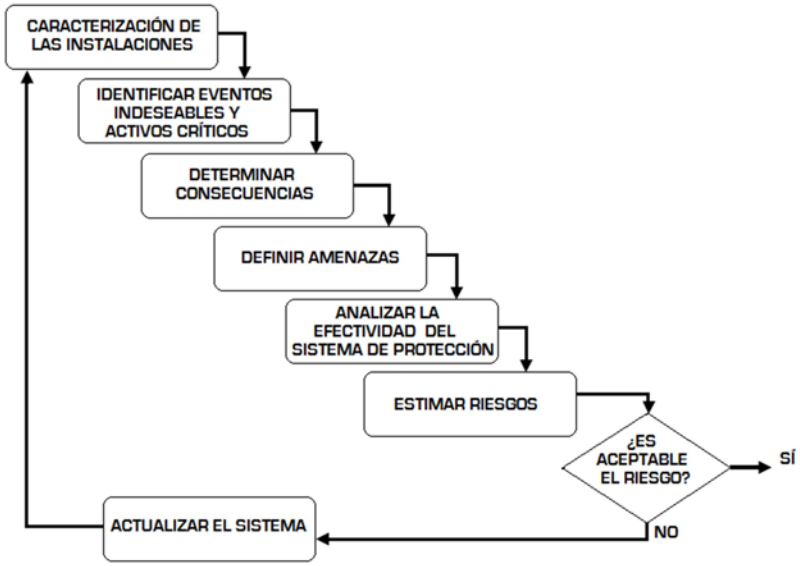

Figura 20. Etapas de la metodología RAM
Fuente: RAM White Paper, Sandia National Laboratories

Paso 1. Caracterización de las instalaciones

En este primer paso se caracterizan las condiciones y los estados de funcionamiento u operación de las instalaciones sobre las que se va aplicar la metodología, se realiza una descripción detallada de la instalación (ubicación de los límites del sitio, localización de sus edificios, planos de planta, puntos de acceso, etc.), una descripción de los procesos dentro de la instalación, así como la identificación de cualquiera de las funciones de protección física existentes.

Paso 2. Identificación de los eventos no deseados y los activos críticos

Con la finalidad de prever eventos no deseados o incidentes en materia de seguridad (efectos adversos en la salud, el medio ambiente, en los activos, en los objetivos de las instalaciones, en las personas, etc.) y proteger a los activos se utilizan herramientas estructuradas, como árboles de fallas, que permitan identificar o prevenir fallas antes de que ocurran. Un análisis de árbol de fallas permite representar gráficamente las posibles combinaciones de eventos y los componentes asociados o involucrados, que pueden dar lugar a un estado no deseado, utilizando símbolos que siguen las leyes del álgebra de Boole.

La figura 21 muestra un árbol de fallas con sus principales símbolos utilizados.

- Puerta "Y": Representa una condición en la que todos los eventos por debajo de ella tienen que cumplirse para que ocurra el evento definido por encima de ella.
- Puerta "O": Representa una situación en que el evento definido por encima de ella ocurrirá si alguno de los eventos definidos por debajo de ella se lleva a cabo.
- Rectángulo: Representa el evento negativo.
- Círculo: un evento base en el árbol.

- Diamante: identifica un evento terminal sin desarrollar.
- Óvalo: Representa una situación especial que puede ocurrir solamente si ocurren ciertas circunstancias.

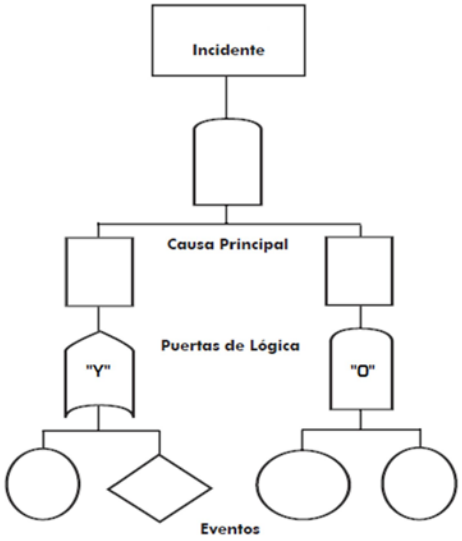

Figura 21. Diagrama de Árbol para el análisis de Fallas
Fuente: Centro de Recursos del Departamento de Seguros de Texas.

Paso 3. Determinación de las consecuencias

El siguiente paso es estimar el valor relativo de la consecuencia o consecuencias, con respecto de cada evento no deseado identificados en el paso en anterior, con base en la escala mostrada en la tabla 7.

Categoría de la consecuencia	Valor relativo
Resultados catastróficos, provocando muertes, pérdida totales, o daño ambientales graves.	Muy alta
Resultados críticos, provocando lesiones graves o enfermedades, pérdidas mayores, o daños ambientales mayores.	Alta
Resultados marginales, provocando lesiones o enfermedades menores, pérdidas menores, o daños ambientales menores.	Media
Resultados despreciables, provocando lesiones o enfermedades insignificantes, pérdidas inferiores, daños ambientales insignificantes.	Baja

Tabla 7. Consecuencias de las categorías y sus valores asociados
Fuente: RAM White Paper, Sandia National Laboratories

Al igual que en las metodologías analizadas en la sección 3.1 y 3.2 de este capítulo se puede observar que en lo referente a las escalas empleadas se presenta el mismo problema de ambigüedad, en el que no se define de forma clara y precisa con qué unidades de medición se puede realizar la clasificación, en este caso, de las consecuencias, ya que se utilizan términos como "daños graves", "daños mayores", "daños menores" y "daños insignificantes", pero no se establecen las características que permitan establecer la diferencia sobre cómo o cuándo un daño es grave, mayor, menor o insignificante.

Paso 4. Definición de Amenazas

Se realiza una descripción de las amenazas, que incluye el tipo y número de adversarios, sus tácticas, capacidades, modus operandi, tipo de herramientas o armas que podría utilizar, así como el tipo de hechos o actos que podrían ejecutar. Esta información se obtiene de organizaciones federales, estatales y locales, así como de agencias de inteligencia, y de la literatura basada en informes sobre incidentes relacionados con el sitio.

Después de describir el espectro de la amenaza y con información estadística de acontecimientos pasados, así como la percepción de los sitios específicos, se clasifican las amenazas en términos de su probabilidad. La probabilidad de un ataque por parte de un adversario puede ser estimado como un parámetro cualitativo relativo a la amenaza potencial. Algunos de los factores que pueden ser utilizados para esta estimación son:

- Sobre la capacidad del adversario:
  - El acceso a la región;
  - Recursos materiales;
  - Conocimientos y habilidades técnicas;
  - Habilidades de planeación y de organización;
  - Recursos financieros.
- Sobre la intención e historia del adversario:
  - Intereses históricos;
  - Ataques históricos;
  - Actuales intereses en el sitio;
  - Actuales parámetros de vigilancia;
  - Amenazas documentadas.
- Sobre el relativo grado de atracción sobre los activos:
  - Nivel deseado de consecuencia;
  - Ideología;
  - Facilidad de ataque.

El proceso para estimar el potencial de una amenaza sigue un completo análisis de amenazas que se calcula con base al evento no deseado y al grupo de adversarios. Para esta estimación se incluyen:

- Las características del grupo adversario en relación con los activos que deben protegerse;
- El relativo grado de atracción de los activos por el grupo adversario.

Paso 5. Análisis de la efectividad del sistema de protección

Se describen a detalle las características de la protección física y después se evaluar la eficacia del sistema de seguridad. La eficacia del sistema de seguridad está en función de su capacidad de detectar a tiempo al adversario y retardarlo el tiempo suficiente para que las fuerzas de respuesta de seguridad puedan llegar y neutralizar al adversario antes de que se lleve a cabo el acto malintencionado. Esta metodología no considera la función de disuasión.

El análisis y evaluación del sistema de seguridad comienza con una revisión y comprensión a fondo de los objetivos de protección y las condiciones de seguridad. Se puede realizar simplemente mediante la comprobación sobre el diseño de las características necesarias de un sistema de seguridad, como lo son la detección de intrusos, el control de entrada, retrasar el acceso, las comunicaciones de respuesta, y la fuerza de respuesta. Sin embargo, se puede utilizar un análisis más sofisticado de evaluación para estimar el nivel mínimo de rendimiento alcanzado por un sistema de seguridad, a través de un "diagrama de secuencia sobre el adversario", como el mostrado en la figura 22, el cual se desarrolla para un solo activo crítico asociado con un evento no deseado, por medio de una representación gráfica de los elementos del sistema de protección física que se encuentran a lo largo del posible camino que los adversarios pueden seguir para lograr su objetivo, de esta manera, se puede determinar, para una amenaza, el camino más vulnerable; éste camino, menos efectivo del sistema de protección física establece la efectividad del sistema de protección física total.

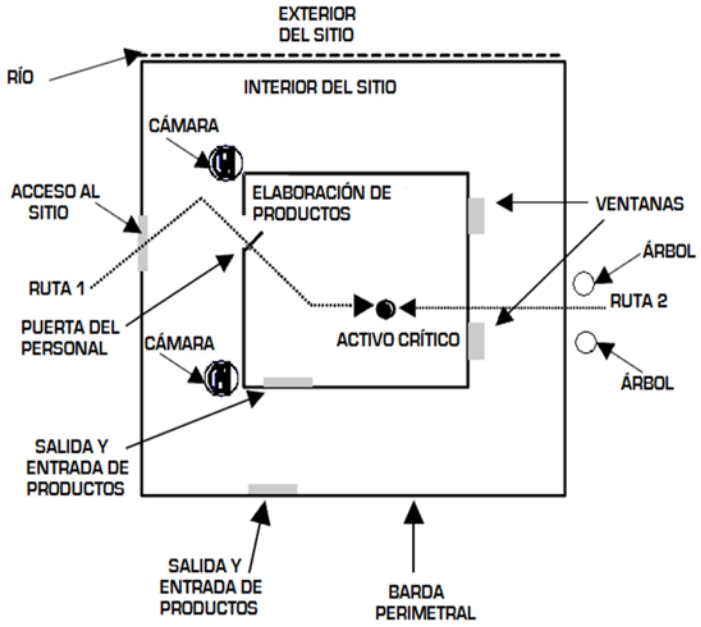

Figura 22. Diagrama de secuencia sobre el adversario
Fuente: RAM White Paper, Sandia National Laboratories

Paso 6. Estimación de Riesgo

El riesgo se cuantifica mediante la siguiente ecuación:

$$R = P_A * (1-P_E) * C$$

En la cual:

R = riesgo asociado con el ataque del adversario
P_A = probabilidad del ataque
P_E = probabilidad de que el sistema de seguridad es eficaz contra el ataque
$(1 - P_E)$ = probabilidad de que el ataque del adversario tenga éxito, o bien, la probabilidad de que el sistema de seguridad no es eficaz contra el ataque
C = consecuencia de la pérdida del ataque.

Paso 7. Actualizaciones e Impactos

Si el riesgo estimado para el espectro de la amenaza se considera inaceptable, se deben considerar mejoras, así como una actualización del sistema. El primer paso es revisar y reevaluar con cuidado los resultados que se hicieron sobre los factores que influyen en el riesgo del sistema, es decir; los posibles eventos no deseados; la atracción sobre activos (objetivos o blancos); las consecuencias de los eventos no deseados; la caracterización de las amenazas; la estimación de la probabilidad de ataque; y las funciones de salvaguarda.

Las mejoras en el sistema pueden incluir modernizaciones, características adicionales en las funciones de salvaguarda o funciones adicionales de mitigación en la seguridad. La actualización del sistema se analiza, entonces, para calcular la variación en el riesgo debido al cambio en la probabilidad de ataque, la efectividad del sistema, o los valores de las consecuencias. Si el riesgo estimado para la actualización del sistema se considera aceptable, la actualización del sistema se ha completado. Si el riesgo sigue siendo inaceptable, el proceso de actualización de la revisión y mejora del sistema se repite hasta que el riesgo se considere aceptable.

Una vez que la actualización del sistema ha sido determinada, es importante evaluar el impacto de la actualización del sistema en la misión de las instalaciones y su costo. Si las actualizaciones del sistema representan una carga pesada para el funcionamiento normal, se tiene que considerar una compensación entre el riesgo y las operaciones. El presupuesto puede ser el conductor en la implantación de las actualizaciones del sistema de seguridad, ya que se debe buscar un equilibrio entre el riesgo y el costo total, de resultar suficiente el sistema está listo para su aplicación.

3.1.4 Metodología CIDETES

Como se trató en el capítulo 1, en la sección 1.4, esta metodología tomó como base la metodología de evaluación para la protección de puertos (EPP), en el que se construye una matriz de análisis de amenazas y riesgos con la finalidad de identificar amenazas y de esta manera adoptar y recomendar medidas de neutralización que impidan, detectan y atenúan las consecuencias de cualquier posible incidente, asignando recursos, formulando previsiones, planeando emergencias y elaborando presupuestos.

Fue aplicada, por primera vez, en el proyecto "Alternativas Tecnológicas para la protección del puerto de Veracruz" en 2006, con una buena aceptación por parte del cliente. De esa fecha a la actual ha sido utilizada en otros proyectos con algunas modificaciones, aunque su esencia se ha mantenido, en las siguientes secciones se realiza una descripción de ésta.

3.4.1 Caracterización Funcional

La metodología CIDETES busca realizar una evaluación diagnóstica del riesgo de los elementos que componen a una organización o empresa, así como establecer los medios (equipos tecnológicos, procedimientos, políticas y personal) en forma de propuesta, que permitan reducir los riesgos que pongan en peligro la integridad de dicha empresa u organización.

3.4.2 Caracterización Estructural

Para alcanzar su objetivo la metodología CIDETES se realiza en 9 etapas, ver figura 23, las cuales son:

1) Definición del Universo o sistema objeto del estudio de riesgo.
2) Identificación y definición de amenazas
3) Determinación del grado con el que los elementos representan un objetivo para las amenazas
4) Determinación del grado de vulnerabilidad de los elementos con respecto de las amenazas
5) Determinación del impacto en caso de pérdida de los elementos
6) Cálculo del riesgo
7) Obtención del mapa de riesgo
8) Equipamiento
9) Diseño del programa de presupuesto

Como apoyo a la etapa 4, se realiza un análisis del sistema de seguridad que se basa en una serie de formatos en los que, con base en una serie de criterios definidos por los investigadores del CIDETES se evalúan los elementos físicos y normativos de los rubros de control de accesos, centro de mando y control, perimetrales y procedimientos.

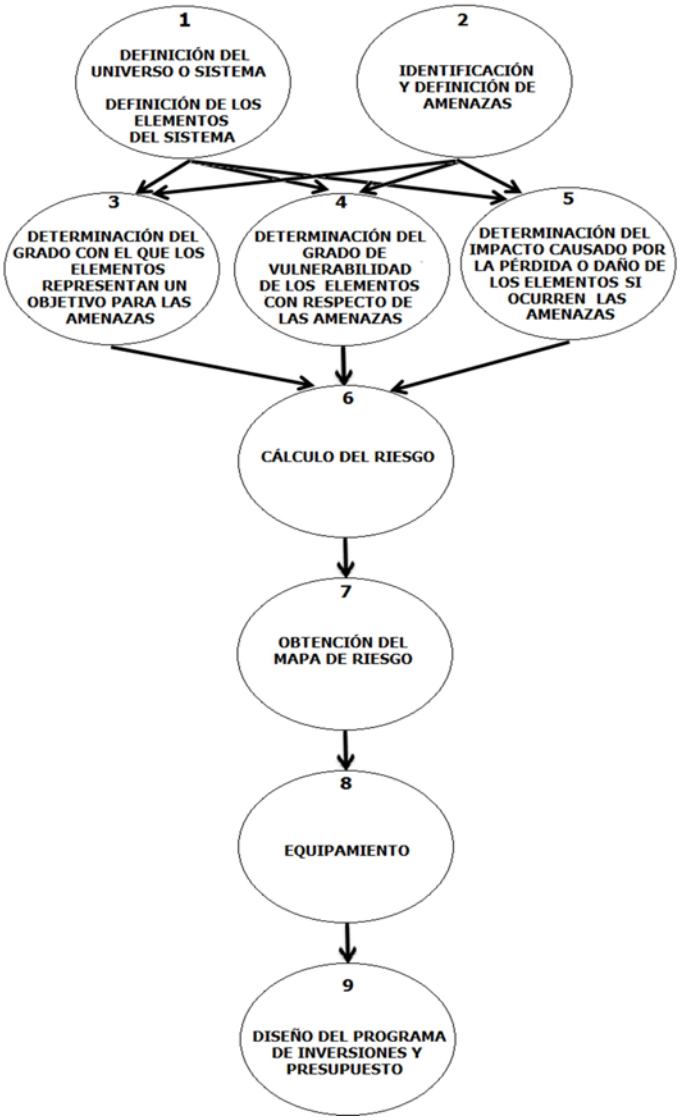

Figura 23. Etapas de la metodología empleada por el CIDETES
Fuente: Elaboración propia.

Paso 1) Definición del Universo o sistema objeto del estudio de riesgo.

Descripción. Se identifica al universo o sistema objeto del estudio de riesgo (entidad, empresa u organización) enlistando al conjunto de elementos que lo conforman. Esta lista se forma con base en un criterio de agregación que esté relacionado con los eventos nocivos en materia de seguridad. Los elementos humanos, bienes materiales, información, etc.

$$\text{Elementos (E)} = \left\{ \begin{array}{l} \text{Elemento } E_1 \\ \text{Elemento } E_2 \\ \text{Elemento } E_3 \\ \ldots\ldots\ldots\ldots\ldots \\ \text{Elemento } E_n \end{array} \right\}$$

Forma de Operación. Se reúne el equipo de expertos y se realiza una lluvia de ideas sobre los elementos del sistema, previamente se solicita información concerniente a este aspecto, y con las visitas en campo se comienza a discriminar aquellos elementos de interés para el estudio.

Paso 2) Definición de amenazas

Descripción. En esta etapa se listan las amenazas que podrían afectar al sistema, y se estima su probabilidad de ocurrencia, se toma como referencia la estadística e información disponible sobre hechos que han ocurrido y se toman en cuenta aquellos que aún no han sucedido pero que tienen una probabilidad alta de hacerlo. Se considera suficiente trabajar con un mínimo de tres amenazas y un máximo de cinco.

$$\text{Amenazas (A)} = \left\{ \begin{array}{l} \text{Amenaza } A_1\text{, probabilidad } pA_1 \\ \text{Amenaza } A_2\text{, probabilidad } pA_2 \\ \text{Amenaza } A_3\text{, probabilidad } pA_3 \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \text{Amenaza } A_n\text{, probabilidad } pA_n \end{array} \right\}$$

Forma de Operación. Se reúne el grupo de expertos para analizar la información recabada, con base en los acontecimientos ocurridos (registros y estadísticas sobre eventos ocurridos en el lugar) y lo observado en el trabajo de campo, se realiza una lluvia de ideas sobre las amenazas que pudieran presentarse, posteriormente se analizan las causas y medios por los cuales puede manifestarse y finalmente con base en la opinión de los expertos se estima la probabilidad de ocurrencia de cada amenaza.

Los resultados de estos dos primeros pasos, alimentan los tres pasos siguientes, en los que se genera una matriz "elemento-amenaza", que relaciona a cada uno de los elementos con cada una de las amenazas, y en la que se asigna un valor a cada relación formada, dependiendo del objetivo del paso. A continuación se muestra la forma general de una matriz "amenaza-elemento":

	amenaza1	amenaza2	amenaza3	...	amenaza N
elemento1	Ve1,a1	Ve1,a2	Ve1,a3		Ve1,aN
elemento2	Ve2,a1	Ve2,a2	Ve2,a3		Ve2,aN
elemento3	Ve3,a1	Ve3,a2	Ve3,a3		Ve3,aN
.....					
elementoM	VeM,a1	VeM,a2	VeM,a3		VeM,aN

Paso 3) Determinación del grado de atracción con el que los elementos representan un objetivo para las amenazas

Descripción. En una matriz "amenaza-elemento", se estima el grado atracción con que cada elemento definido, representa un objetivo o blanco para cada amenaza identificada, con base a una escala que va del 0 (cero) al 100 (cien), en donde 100 (cien) se asigna al elemento que resulta más relevante o atractivo para la amenaza y 0 (cero) a aquel que no es atractivo y por tanto no representa un objetivo para la amenaza; los valores intermedios son asignados en función al peso relativo de dicha atracción elemento-amenaza. En la asignación del valor se

toma en cuenta que existen objetivos o blancos directos e indirectos, es decir, para alcanzar su objetivo principal, una amenaza, puede primero alcanzar otros objetivos.

El producto en este paso es la matriz "O", en donde el elemento "$O_{m,n}$" representa el grado con que el elemento "m" es atractivo para la amenaza "n".

Objetivo (O) = f (A,E) =

	A_1	A_2	A_3	::::::::::::::::	A_n
E_1	O_{11}	O_{12}	O_{13}	::::::::::::::::	O_{1n}
E_2	O_{21}	O_{22}	O_{23}	::::::::::::::::	O_{2n}
E_3	O_{31}	O_{32}	O_{33}	::::::::::::::::	O_{3n}
::::	::::::::::::::::	::::::::::::::::	::::::::::::::::	::::::::::::::::	::::::::::::::::
E_m	O_{m1}	O_{m2}	O_{m3}	::::::::::::::::	O_{mn}

Forma de operación. El grupo de expertos se reúne y le asignan un valor a cada relación elemento-amenaza que corresponde a la percepción y experiencia de cada uno de ellos.

Paso 4) Determinación del grado de vulnerabilidad de los elementos

Descripción. El grado de vulnerabilidad se obtiene en función del grado de protección de los elementos. En una matriz "elemento-amenaza", para cada elemento definido se estima el grado de vulnerabilidad con respecto de cada amenaza identificada, con base en una escala que va del 0 (cero) al 100 (cien), en donde 100 (cien) se asigna al elemento más vulnerable con respecto de la amenaza y 0 (cero) a aquel que se encuentra totalmente protegido de la amenaza. Esto último sustentado en un análisis del sistema de seguridad física, descrito más adelante.

El producto en este paso es la matriz "V", en donde el elemento "$V_{m,n}$" representa el grado de vulnerabilidad del elemento "m" con respecto a la amenaza "n".

Vulnerabilidad (V) = f (A,E) =

	A_1	A_2	A_3	::::::::::::::::	A_n
E_1	V_{11}	V_{12}	V_{13}	::::::::::::::::	V_{1n}
E_2	V_{21}	V_{22}	V_{23}	::::::::::::::::	V_{2n}
E_3	V_{31}	V_{32}	V_{33}	::::::::::::::::	V_{3n}
::::	::::::::::::::::	::::::::::::::::	::::::::::::::::	::::::::::::::::	::::::::::::::::
E_m	V_{m1}	V_{m2}	V_{m3}	::::::::::::::::	V_{mn}

Forma de operación. El grupo de expertos se reúne y le asignan un valor a cada relación elemento-amenaza que corresponde a la percepción, resultado del trabajo de campo y experiencia de cada uno de ellos.

Este paso se apoya importantemente, de la información recabada sobre el sistema de seguridad física, ya que permite a los expertos, identificar que activos se encuentran desprotegidos o con un alto grado de ser alcanzados debido a las fallas de este sistema.

Esta información la obtienen cuatro brigadas, en las que se divide el equipo de trabajo, las cuales abarcan los siguientes rubros:

1) *Control de Accesos*. Que se encarga del análisis de: puertas (peatonales y vehiculares); caminos (peatonales y vehiculares); elementos de seguridad (barreras disuasivas, detectores, alarmas, sensores, etc.); sistemas CCTV (cámaras); áreas críticas; personal de vigilancia; casetas de vigilancia (visibilidad , ubicación, sistema de iluminación, sistema contra-incendios y sistema de comunicación);

2) *Centro de Mando y Control*. Que recaba información sobre: (ubicación; sistema de iluminación; sistema contra-incendios; sistema de comunicación; personal que labora en el centro; sistema CCTV (cámaras -análisis de lo recolectado en control de accesos y perimetrales- , servidores, video-grabadoras y software);

3) *Perimetrales*. En donde se analizan: bardas perimetrales; caminos perimetrales; sistema de iluminación perimetral, y; sistema CCTV (cámaras);

4) Procedimientos. En donde se analiza: Políticas Programas Planes Fuerzas de reacción Evaluación del personal Estructura orgánica

Estas brigadas se auxilian de cuestionarios o formatos para la recopilación de información en campo, los cuales están enfocados en la evaluación del estado y características de los elementos físicos o materiales del sistema de seguridad, así como en la operación de los procedimientos del mismo. A continuación, tomado íntegramente de los documentos del CIDETES, se presentan los criterios de evaluación utilizados y la forma en la que se realiza dicha evaluación.

Elementos físicos:

1. *Falla en la operación***.** El personal no sabe cómo usarlo por falta de capacitación. El equipo o sistema no trabaja por un error en la forma de operarlo, o no lo pusieron a funcionar por alguna razón, olvido, falta de operador, falta de cuidado o atención, pero el equipo está en condiciones de trabajar corrigiendo la falla humana.

2. *Equipo Incompleto***.** El sistema no está en condiciones de operar adecuadamente porque no está completo, le falta algún componte, funciona parcialmente y ha sido reportado para su arreglo.

3. *Falta de mantenimiento***.** El equipo no trabaja por algún defecto que no se ha corregido y este ha sido reportado para su mantenimiento

4. *Equipo dañado***.** Por mal funcionamiento del mismo, o tiene daños provocados por efectos meteorológicos, picos de voltaje o descargas eléctricas, o por algún accidente o algún hecho de vandalismo y ha sido reportado para su reparación.

5. *Falta de supervisión.* El equipo está dañado y no ha sido reportado, ni corregido por lo que falta supervisión del funcionamiento

6. *Obsolescencia.* El equipo está en funcionamiento pero ya no cumple con los requerimientos del sistema.

7. *Innecesario.* Su funcionamiento y operación no contribuye en nada; puede dejar de utilizarse

8. *No permiten su operación***.** Por algún motivo hay una indicación que impide su uso, ya sea patronal o sindical

9. *Su operación causa otro daño***.** El sistema o equipo causa daño o mal funcionamiento en otros equipos o sistemas y requiere de algún arreglo específico para que pueda entrar en operación

10. *No sirve, daño total o no existe***.** El equipo o sistema no tiene reparación o no existe por lo que se requiere reposición total o adquisición.

Por su parte para los procedimientos operativos de seguridad física se tienen:

1. *Falla en el uso de la información***.** El personal no sabe cómo usarla por falta de capacitación. La interpretación de la información no se hace de manera correcta por vicios adquiridos al paso del tiempo, o no aplican los procedimientos por a alguna razón, costumbre, olvido, falta de interés, falta de cuidado o atención, pero la información está completa y puede funcionar, corrigiendo la falla humana.

2. *Documentación Incompleta***.** La información no está completa y es confusa por lo que no está en condiciones de aplicarse adecuadamente, le falta algún componte o condiciones adecuadas para poderse aplicar, por lo que funciona parcialmente y la falla en el procedimiento ha sido reportada para poderla cumplir

3. *Falta de actualización*. La información con que se cuenta no está actualizada debido a que las condiciones para su aplicación han cambiado y su aplicación no se hace ahora posible y esa situación ha sido reportada.

4. *Información equivocada***.** La información o procedimientos han sido establecidos de manera equivocada y no van de acuerdo totalmente a lo dispuesto por algún plan rector, y se mantiene así por tradición o costumbre.

5. *Falta de supervisión*. La información de los sistemas y procedimientos operativos es correcta, pero los encargados no los siguen a cabalidad por falta de supervisión lo que ha creado situaciones de vicios y costumbres

6. *Obsolescencia*. La información es obsoleta y los procedimientos se han vuelto inaplicables o se aplican sin sentido.

7. *Innecesario*. Sistemas y sistemas operativos que por el cambio de las condiciones a través del tiempo se han vuelto innecesarias pero por rutina se siguen aplicando.

8. *No permiten su operación*. Por algún motivo hay una indicación que impide su uso y aplicación, ya sea patronal o sindical

9. *Su aplicación causa problemas a otras áreas*. La aplicación de un sistema o procedimiento operativo que incluso ser bueno en sí mismo, no puede aplicarse ya que su utilización, puede hacer que afecte a otras áreas si se aplica

10. *No existe*. La información no existe y se requiere elaborarla o implantarla completamente

La forma en la que se le evalúan asignando una calificación a los elementos del sistema de seguridad es la siguiente: se parte de un valor de 10 y se comienza a restar una unidad si por cada criterio se han encontrado características que cumplen su definición, excepto en el criterio de "No sirve o daño total", en el cual, se restan diez unidades, dejando de lado lo encontrado anteriormente y obteniendo así un valor de 0 para el elemento analizado.

Criterio	Unidades a restar
1. Falla en la operación	
2. Equipo incompleto	1
3. Falta de mantenimiento	1
4. Equipo dañado	
5. Falta de supervisión	1
6. Obsolescencia	
7. Innecesario	
8. No permiso de operación	
9. Su operación ocasiona otro daño	
10. No sirve/daño total	
Total de las unidades a restar	3
Calificación del elemento	10-3=7

Tabla 8. Ejemplo sobre la evaluación de un elemento material.
Fuente: Guía para la evaluación de elementos materias y de procedimientos, CIDETES, 2010.

Criterio	Unidades a restar
1. Falla en la operación	
2. Equipo incompleto	1
3. Falta de mantenimiento	1
4. Equipo dañado	
5. Falta de supervisión	1
6. Obsolescencia	
7. Innecesario	
8. No permiso de operación	
9. Su operación ocasiona otro daño	
10. No sirve/daño total	10
Total de las unidades a restar	10
Calificación del elemento	10-10=0

Tabla 9. Ejemplo sobre la evaluación de un elemento material que no sirve.
Fuente: Guía para la evaluación de elementos materias y de procedimientos, CIDETES, 2010

En la tabla 8 se presenta un ejemplo, en el que se supone que durante el trabajo en campo se encuentra un elemento incompleto, presenta falta de mantenimiento y falta de supervisión, de acuerdo con la definición de los criterios, entonces se restarían 3 unidades a la calificación inicial de 10, resultando un 7. Si además se encontrara que el elemento no sirve, como se muestra en la tabla 9, se tendrían que restar 10 unidades en lugar de las 3 unidades de los criterios anteriores, por lo que el resultado sería un 0.

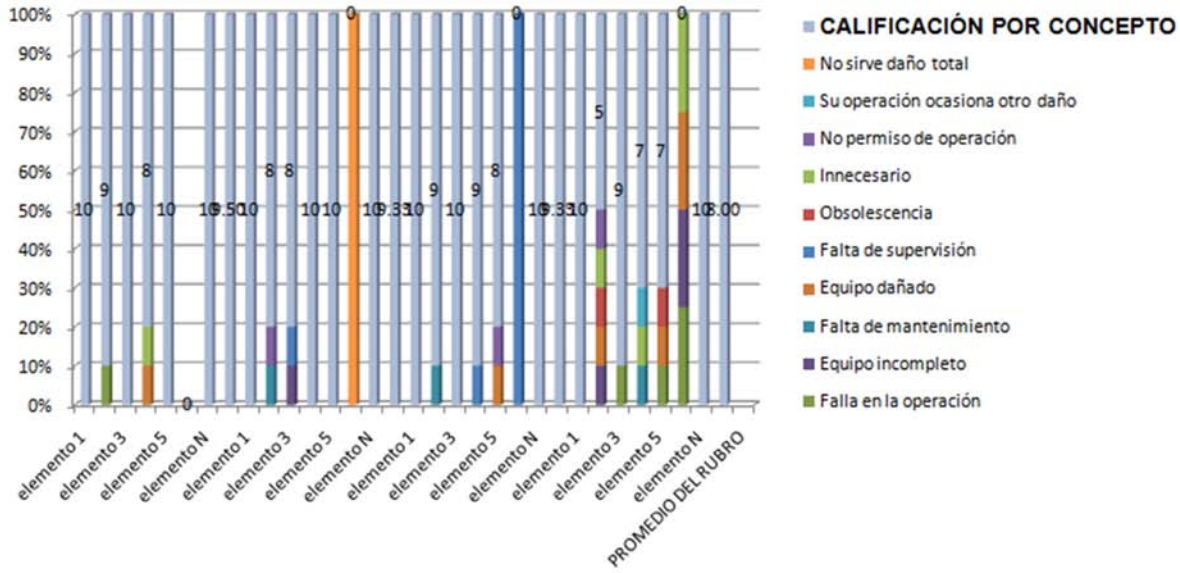

Figura 24. Gráfica que muestra la calificación de los elementos de una zona o área de estudio
Fuente: Guía para la evaluación de elementos materiales y procedimientos, CIDETES, 2010.

CLAVES	CONCEPTO	Acceso 1 e1	e2	e3	e4	e5	eN	(Z1)	Acceso 1 e1	e2	e3	e4	e5	eN	(Z2)	ZONA 3 e1	e2	e3	e4	e5	eN	(Z3)	ZONA 4 e1	e2	e3	e4	e5	eN	(Z4)	PROMEDIO DEL RUBRO	Incidencia de falla
	CPQ																														
	RUBRO:	Acceso 1						(Z1)	Acceso 1						(Z2)	ZONA 3						(Z3)	ZONA 4						(Z4)		
FO	Falla en la operación		1																						1		1	1			4
EI	Equipo incompleto										1												1					1			3
FM	Falta de mantenimiento									1							1									1					3
ED	Equipo dañado				1															1			1				1	1			5
FS	Falta de supervisión										1								1		1										3
OB	Obsolescencia																						1				1				2
IN	Innecesario				1																		1		1			1			4
NP	No permiso de operación									1										1			1								3
DA	Su operación ocasiona otro daño																								1						1
NE	No sirve daño total													10																	1
	CALIFICACIÓN POR CONCEPTO	10	9	10	8	10		10	9.50	10	8	8	10	10		10	9.33	10	9	10	9	8		10	9.33	10	5	9	7	7		10	8.00		
	Calificación Total																													9.04	2.90
																															11.94

Figura 25. Tabulación que muestra la calificación de los elementos de una zona o área de estudio, los promedios de dichas zonas, y de la toda instalación.
Fuente: Guía para la evaluación de elementos materiales y procedimientos, CIDETES, 2010.

Una vez evaluados los elementos físicos y normativos, se tabulan y grafican los resultados, como se muestra en las figura 24 y 25, en las que dichos resultados se agrupan por zonas, según convenga al estudio o sistema del que se trate, y se presenta el valor promedio de los elementos por zona y globalmente.

En relación con los criterios de evaluación definidos en esta parte, resultan ambiguos, incluso se hace un uso equivocado de los conceptos. Se definieron diez criterios para los elementos físicos y se extrapolaron a los elementos normativos. A continuación se presentan algunas observaciones sobre los primeros ya que es a partir de éstos se "adaptaron" los segundos:

- ✓ Sobre el criterio "*falla en la operación*" no se definen las condiciones que provocan que la falla se presente en términos del elemento, dejando de lado su característica operativa, que es la que se pretende evaluar, sin embargo, sí se resalta la parte humana, por ejemplo, en su definición se menciona: "el personal no sabe cómo usarlo por falta de capacitación"; "el equipo o sistema no trabaja por un error en la forma de operarlo" ; "no lo pusieron a funcionar por alguna razón, olvido, falta de operador, falta de cuidado o atención"; "pero el equipo está en condiciones de trabajar corrigiendo la falla humana".

- ✓ En "*equipo incompleto*"**,** se define: "el sistema no está en condiciones de operar adecuadamente …", mezclando este criterio con el anterior; después: "… porque no está completo, le falta algún componte, funciona parcialmente …", lo que resulta nuevamente ambiguo, ya que no se puede definir un equipo incompleto porque no está completo, además no se define qué característica o componente es la que lo hace incompleto; finalmente se menciona: "…y ha sido reportado para su arreglo", idea que no gurda relación con el fin último del criterio, es decir, el saber si se ha reportado o no, para su arreglo, no refleja valor alguno en la evaluación sobre el criterio.

- ✓ En *"falta de mantenimiento"* se define: "el equipo no trabaja por algún defecto que no se ha corregido y este ha sido reportado para su mantenimiento", pareciera que lo que se define es una de las causas por las que no opera el equipo, en lugar de evaluar la existencia de un programa de mantenimiento, en el que entre otras cosas resulta importante, por ejemplo, su periodicidad.

- ✓ Para el criterio sobre "falta de supervisión", se define: "el equipo está dañado …", lo que hace referencia al criterio "equipo dañado"; después: "… y no ha sido reportado, ni corregido por lo que falta supervisión del funcionamiento", expresa que una supervisión se limita a reportar y corregir el funcionamiento del equipo, asumiendo que se trata de una actitud reactiva, cuando en realidad una función de supervisión implica actitudes activas y proactivas, además da la impresión de que la evaluación está enfocada únicamente a quienes operan el equipo.

- ✓ Para el criterio "*No permiten su operación*", se define que: "por algún motivo hay una indicación que impide su uso, ya sea patronal o sindical", lo que refleja más una posible causa sobre las fallas en la operación del equipo.

- ✓ En **"***equipo dañado***",** se establece que "está dañado por mal funcionamiento", y no se define a que se refiere "mal funcionamiento", se establecen las causas del daño: el mal funcionamiento, efectos meteorológicos, picos de voltaje, accidentes y vandalismo, sin embargo, no se explica cómo se manifestarían estas causas en el elemento, es decir, qué tipo de daño se tendría en el elemento; al final se establece que: "… ha sido reportado para su reparación", idea que no refleja algún tipo de valor sobre el criterio.

- ✓ Ahora bien, lo establecido en "*obsolescencia"* e "*innecesario*" no corresponden a una propiedad que pueda ser evaluada para un equipo, ya que en un momento dado, serían resultado de la evaluación, es decir, después de evaluar al equipo, se puede decir como conclusión, que el equipo es obsoleto o innecesario.

- ✓ En el criterio *"Su operación causa otro daño"***,** se define: "…requiere de algún arreglo específico para que pueda entrar en operación", mezclando de esta manera, dos aspectos distintos: 1) que el equipo cause un daño a otro equipo y, 2) el "arreglo" necesario para que entre en operación, aspecto que no debiera aportar valor a la evaluación del criterio.

- ✓ Finalmente, en el criterio "*No sirve, daño total o no existe"***,** no puede considerarse la "no existencia" como una propiedad a evaluar del equipo, mientras que en lo referente al término "daño total" hace más referencia a una medida del criterio "equipo dañado".

Por otro lado la forma de evaluar resulta confusa y los resultados no arrojan elementos importantes en el estudio del sistema, ya que se deja de lado aspectos como el impacto que los equipos tienen en la seguridad, es decir, si cumplen realmente con su funcionalidad dentro del sistema de seguridad física, aspecto que refleja en gran parte la efectividad del mismo.

Otro aspecto importante, es que se les da el mismo peso a todos los elementos del sistema de seguridad, lo que indica que una "lámpara dentro de una caseta", por ejemplo, tiene la misma importancia que un "detector de metales", sin importar qué es más importante en términos del riesgo.

Paso 5) Determinación del impacto en caso de pérdida de los elementos

Descripción. En una matriz "elemento-amenaza" para cada elemento definido se estiman los impactos, que pueden presentarse si cada una de las amenazas alcanzaran al elemento, esto como una cuantificación del daño en función de su valor económico y como un valor absoluto (en pesos o dólares), el cual puede presentarse como el valor por reparación o sustitución del elemento, y los efectos colaterales originados por la pérdida total o temporal del mismo, en el caso de bienes materiales, sin dejar de lado la parte humana. Además de considerar los impactos generados como consecuencia de otros impactos. El producto en este paso es la matriz "I", en donde el elemento "$I_{m,n}$" representa el impacto por pérdida, reparación, o sustitución del elemento "m" con respecto de la amenaza "n".

Impacto(I) = f (A,E) =

$$
\begin{array}{c} \\ E_1 \\ E_2 \\ E_3 \\ :::: \\ E_m \end{array}
\begin{array}{c}
\begin{array}{ccccc} A_1 & A_2 & A_3 & ::::::::::::::::: & A_m \end{array} \\
\begin{pmatrix}
\$_{11}=I_{11} & \$_{12}=I_{12} & \$_{13}=I_{13} & ::::::::::::::::: & \$_{1n}=I_{1n} \\
\$_{21}=I_{21} & \$_{22}=I_{22} & \$_{23}=I_{23} & ::::::::::::::::: & \$_{2n}=I_{2n} \\
\$_{31}=I_{31} & \$_{32}=I_{32} & \$_{33}=I_{33} & ::::::::::::::::: & \$_{3n}=I_{3n} \\
::::::::::::::::: & ::::::::::::::::: & ::::::::::::::::: & ::::::::::::::::: & ::::::::::::::::: \\
\$_{m1}=I_{m1} & \$_{m2}=I_{m2} & \$_{m3}=I_{m3} & ::::::::::::::::: & \$_{mn}=I_{mn}
\end{pmatrix}
\end{array}
$$

Forma de operación. El grupo de expertos analiza la información proporcionada por el cliente sobre el valor de sus activos, procesos y producción; se realiza una investigación sobre los valores de mercado de los mismos, y se comienza asigna un valor (económico) de los posibles impactos, considerando los impactos encadenados, es decir, impactos causados por otros impactos para cada relación elemento-amenaza.

Paso 6) Cálculo del riesgo

Descripción. En esta etapa se obtiene el valor del riesgo, en dos pasos:

1) El riesgo para cada elemento con respecto de cada amenaza multiplicando cada valor encontrado al momento de vincular a los elementos con las amenazas expresados en las matrices O, V, I, y con la probabilidad de ocurrencia de la amenaza,"Pa" como se muestra a continuación:

$$
\begin{array}{c} \\ E_1 \\ E_2 \\ E_3 \\ ::: \\ E_m \end{array}
\begin{array}{c}
\begin{array}{ccccc} A_1 & A_2 & A_3 & \begin{matrix}:::\\:\end{matrix} & A_n \end{array} \\
\begin{pmatrix}
O_{11}*V_{11}*I_{11}*Pa_1 & O_{12}*V_{12}*I_{12}*Pa_2 & O_{13}*V_{13}*I_{13}*Pa_3 & ::: & O_{1n}*V_{1n}*I_{1n}*Pa_n \\
O_{21}*V_{21}*I_{21}*Pa_1 & O_{22}*V_{22}*I_{22}*Pa_2 & O_{23}*V_{23}*I_{23}*Pa_3 & ::: & O_{2n}*V_{2n}*I_{2n}*Pa_n \\
O_{31}*V_{31}*I_{31}*Pa_1 & O_{32}*V_{32}*I_{32}*Pa_2 & O_{33}*V_{33}*I_{33}*Pa_3 & ::: & O_{3n}*V_{3n}*I_{3n}*Pa_n \\
::::::::::::::::: & ::::::::::::::::: & ::::::::::::::::: & ::: & ::::::::::::::::: \\
O_{m1}*V_{m1}*I_{m1}*Pa_1 & O_{m2}*V_{m2}*I_{m2}*Pa_2 & O_{m3}*V_{m3}*I_{m3}*Pa_3 & ::: & O_{mn}*V_{mn}*I_{mn}
\end{pmatrix}
\end{array}
=
\begin{array}{c}
A_1\ ,\ A_2\ ,\ A_3\ ::\ A_m \\
\begin{pmatrix}
R_{11},R_{12},R_{13}:::R_{1m} \\
R_{21},R_{22},R_{23}:::R_{2m} \\
R_{31},R_{32},R_{33}:::R_{3m} \\
::::::::::::::::: \\
R_{m1},R_{m2},R_{m3}:::R_{mn}
\end{pmatrix}
\end{array}
$$

El riesgo asociado a cada elemento con respecto de cada amenaza, se calcula multiplicando la probabilidad de ocurrencia de las amenazas por cada valor asignado en la relación elemento-amenaza de los pasos anteriores, es decir, la probabilidad de ocurrencia "Pa_n", de la amenaza "n", por el elemento "$O_{m,n}$", obtenido en el paso 3 (grado con el que los elementos representan un objetivo para las amenazas), por el elemento "$V_{m,n}$", obtenido en el paso 4 (grado de vulnerabilidad de los elementos con respecto de las amenazas), por el elemento "$I_{m,n}$", obtenido en el paso 5 (impacto económico que se tendría si las amenazas alcanzaran sus objetivos), cuyo resultado genera al elemento "$R_{m,n}$", que conforma, entonces, la matriz "R" y en donde dicho elemento representa el riesgo asociado al elemento "m" con respecto a la amenaza "n".

Esta forma de calcular el riesgo pretende proporcionar una idea de la magnitud del riesgo, como se muestra en la figura 26.

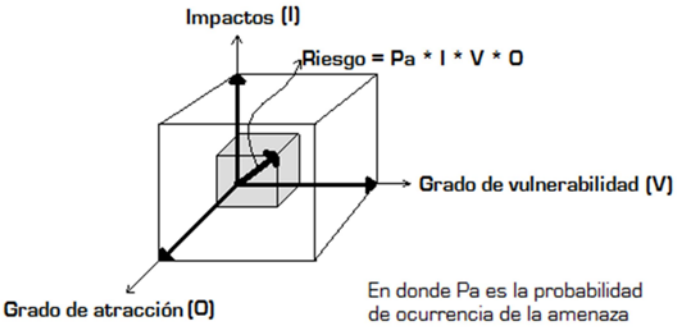

Figura 26. Magitud del riesgo
Fuente: Zúñiga, 2010

2) El riesgo acumulado de cada elemento, que resultaría de presentarse simultáneamente todas las amenazas, es decir, para el elemento "m" el riesgo se obtiene al sumarse todos los valores del riesgo para ese elemento: "$R_m = R_{m,1} + R_{m,2} + R_{m,3} + \ldots + R_{m,n}$".

$$\begin{matrix} R_1= \\ R_2= \\ R_3= \\ \\ R_m= \end{matrix} \begin{pmatrix} R_{11} + R_{12} + R_{13} + \cdots\cdots\cdots\cdots + R_{1n} \\ R_{21} + R_{22} + R_{23} + \cdots\cdots\cdots\cdots + R_{2n} \\ R_{31} + R_{32} + R_{33} + \cdots\cdots\cdots\cdots + R_{3n} \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ R_{m1} + R_{m2} + R_{m3} + \cdots\cdots\cdots\cdots + R_{mn} \end{pmatrix}$$

Una vez que se obtienen estos valores, se jerarquizan los elementos "Rm" con el propósito de expresar de mayor a menor el riesgo, y clasificarlos en tres conjuntos: riesgo alto, riesgo medio y riesgo bajo; la forma en la que se realiza varía, dependiendo de las diversas situaciones y factores que se hayan observado al momento de aplicar la metodología, se puede tomar como parámetro el valor de riesgo máximo encontrado, y realizar la clasificación por arriba o abajo del 50% de dicho valor; otra forma es con base en valores en donde se puede apreciar una diferencia muy marcada.

Forma de Operación. El cálculo se realiza a través de software; para la clasificación del riesgo, el grupo de expertos, en conjunto, analiza los resultados obtenidos y establecen los parámetros de clasificación, así como la correspondiente jerarquización del riesgo.

Paso 7) Obtención del mapa de riesgo

Descripción. A partir de uno o varios planos arquitectónicos se ubican los elementos analizados, en relación con su valor de riesgo asociado y se identifican con un código de color: rojo para los elementos de mayor riesgo; naranja para elementos de riesgo medio; y verde claro para los elementos de riesgo bajo. Esto con la finalidad de delimitar las zonas de riesgo y establecer prioridades al momento de realizar las propuestas tecnológicas (inversión) en pro de reducir los riesgos encontrados.

Forma de trabajo. En esta etapa se ubican en planos los elementos de acuerdo con el riesgo obtenido en la etapa anterior, y se comienzan las discusiones sobre las posibles tecnologías que pueden utilizarse, y su prioridad de implantación.

Paso 8) Equipamiento

Descripción. Con la obtención del mapa de riesgos y bajo la naturaleza y probabilidad de las amenazas, se propone el equipo tecnológico necesario, así como la infraestructura requerida, buscando reducir, al mínimo posible, el riesgo encontrado. Los equipos que son propuestos cubres tres rubros:

- Equipos disuasivos, que son aquellos que desalientan o dificultan el que se cometan ilícitos (barreras físicas, controles de acceso, vigilancia, letreros, entre otros).

- Equipamiento para vigilancia, que son aquellos elementos que permiten observar en tiempo real las zonas críticas, los elementos de mayor valor y las zonas en donde se es susceptible al daño (CCTV, alarmas, detectores, entre otros).

- Equipamiento de reacción inmediata, que son los medios utilizados a partir del momento en que se comete el ilícito o se presenta un evento que requiere atención (equipos de radiocomunicación, vehículos, barreras que se activen en caso de alarma, entre otros)

Forma de trabajo. El equipo de expertos se reúne y discute, en función del riesgo asociado a los elementos, el equipo necesario (cantidad y ubicación), y la infraestructura requerida, justificando la selección con el apoyo de software para la toma de decisiones; básicamente se buscan tres proveedores, proporcionando cuadros comparativos en los que se muestran las características técnicas de los equipos.

Paso 9) Diseño del programa de inversiones y presupuesto

Descripción. En esta etapa se establecen los costos sobre los equipos propuestos, y en función de la jerarquización del riesgo encontrado, se atiende en primer instancia a aquellos elementos en los que el riesgo es alto, después a los de riesgo medio, y finalmente a los de riesgo bajo. Para la integración del programa de inversiones se obtiene la relación de los requerimientos de equipo e implantaciones para cada una de las zonas de riesgo, estableciendo prioridades y un periodo, generalmente, a tres años

Forma de trabajo. El grupo de expertos realiza una investigación sobre el costo actual de cada equipo y establece la prioridad de la inversión.

3.2 Análisis comparativo de las metodologías

Una vez caracterizadas las metodologías, el siguiente paso es realizar una comparación entre ellas, su objetivo no radica en determinar si una es mejor o peor que otra, sino en establecer sus diferencias y similitudes, y de esta manera sustentar las propuestas, que en aquellas partes del proceso de la metodología CIDETES, aporten un fortalecimiento en su práctica.

Los criterios que permiten esta comparación, definidos en la tabla 10, resultan de la investigación teórica que involucra el fenómeno del desastre, en el que se pueden presentar eventos no deseados de seguridad física.

Criterio	Descripción
Estructura	Se refiere a las etapas y en general al proceso que siguen las metodologías, persigue establecer si cumplen con las instancias necesarias implicadas en evaluación de riesgos. De acuerdo con la IID cualquier metodología de estimación de riesgos debe contemplar: ➢ Determinación de las amenazas ➢ Descripción del sistema bajo estudio ➢ Identificación de los daños Además de estas tres instancias, se utilizará una más: *instancias adicionales,* en la que se analizarán aquellos elementos considerados aparte de los enunciados anteriormente.
Funcionalidad	Tiene por objetivo comparar el propósito o propósitos de las metodologías, enmarcado(s) por el enfoque de la planeación como un proceso básico en la conducción, en el que se consideran cuatro etapas: ➢ Diagnóstico ➢ Prescripción ➢ Instrumentación ➢ Control
Evaluación del riesgo	Bajo este criterio se hace énfasis en la comparación de los elementos utilizados por las metodologías para cumplir con su principal propósito, que es la estimación del riesgo asociado a un sistema afectable, los cuales son: ➢ Variables ➢ Criterios ➢ Escalas ➢ Unidades de medición
Alcances y Resultados	A través de este criterio se comparan los productos finales de la aplicación de las metodologías, así como su alcance e impacto.

Tabla 10. Criterios para la comparación de metodologías.

Fuente: Elaboración propia.

Por cada criterio definido se presenta el correspondiente análisis comparativo realizado con las cuatro metodologías, a través de cuadros que expresan esta información. En estos cuadros, la primer columna, enuncia los elementos que componen, o actividades que realizan, las metodologías bajo el criterio definido; las cuatro columnas restantes están destinadas a cada metodología, en ellas mediante el símbolo ✓ se establece si cumplen o no, o si realiza o no, dicho elemento o actividad; para los cuadros construidos en el criterio *estructura,* la última fila presentan el paso o pasos en los que están presentes dichos elementos dentro de las metodologías.

3.2.1 Estructura

La primer instancia analizada es la descripción del sistema expuesto o afectable, que como se trató en el capítulo 2, se trata del sistema en el que se pueden manifestar los efectos de las calamidades o amenazas. El cuadro comparativo 1, mostrado a continuación, presenta esta información.

Descripción del sistema afectable	SVA	MOSLER	RAM	CIDETES
Caracterización de las instalaciones (de procesos, de identificación)	✓*		✓	✓*
Identificación de posibles activos críticos	✓	✓*	✓	✓
Determinación de funciones críticas	✓			✓*
Determinación de la infraestructura crítica y de las relaciones que dan soporte a funciones críticas	✓			
Determinación de la criticidad de los activos:				
Valuación de los activos (económico, emblemático, operacional, etc.)	✓		✓	✓
Identificación de posibles consecuencias si el activo fuera atacado	✓		✓	✓*
Sustitución del activo		✓		
Estimación de la severidad del activo	✓			
Determinación de los activos críticos	✓		✓	✓*
Etapas en las que se realizan o están presentes estos elementos o actividades	0, 1	1	1,2,3	1

Cuadro comparativo 1. Descripción del sistema afectable.
Fuente: Elaboración propia

* *Observaciones*: La metodología SVA aborda esta instancia en su paso 1; la "caracterización de las instalaciones" no se encuentra explícitamente definida, sin embargo, en la preparación de la metodología se abarcan aspectos que la incluyen. La metodología MOSLER en su paso 1 solo identifica los bienes, aquello valioso que puede ser dañado por una amenaza, sin explicar cómo lo realiza. Por su parte la metodología CIDETES caracteriza a las instalaciones al momento de comenzar con el proyecto de seguridad física; en su paso 1, solo se listan los posibles activos que pueden ser importantes para el sistema, los expertos que aplican la metodología discuten aspectos como las funciones críticas y las

consecuencias que se tendrían si el activo es alcanzado por una amenaza, y determinan así, qué activos son los que se consideran para el estudio, sin embargo, esto no se documenta.

La segunda instancia analizada es la determinación de las calamidades o amenazas que pueden provocar daños en un sistema afectable. El cuadro comparativo 2 construido, se muestra a continuación.

Determinación de calamidades (Análisis de amenazas)	**SVA**	**MOSLER**	**RAM**	**CIDETES**
Identificación de adversarios (número, tipo, etc.)	✓	✓*	✓	✓*
Caracterización del adversario (antecedentes, capacidades, fortalezas, tácticas, modo de operación, acciones potenciales y motivaciones)	✓		✓	✓*
Determinación de la peligrosidad de las amenazas (nivel/potencial)	✓		✓	
Estimación de la probabilidad de ocurrencia de las amenazas / de que se presente un ataque		✓*	✓	✓
Estimación particular del grado de atracción por los activos críticos (por cada elementos definido como crítico en relación con cada amenaza identificada)	✓		✓	✓
Estimación global del grado de atracción por los activos críticos (para cada elemento definidos como crítico)	✓			
Etapas en las que se realizan o están presentes estos elementos o actividades	2	1, 2	4	2,3

Cuadro comparativo 2. Determinación de las calamidades (amenazas)
Fuente: Elaboración propia

**Observaciones:* La metodología MOSLER en su paso 1 define los riesgos, que en realidad son las amenazas, que pueden causar daños, aunque no explica cómo hacerlo, careciendo, entonces, de este análisis; por otro lado en el paso 2 el criterio de "agresión" se define como la probabilidad de que el riesgo se manifieste, que en realidad se trata de la amenaza, además, los valores expresados para ese criterio estrictamente no representan una probabilidad. La metodología CIDETES, lleva a cabo la identificación y caracterización de los adversarios, sin embargo, no se documenta, solo es discutido al momento de realizar la evaluación de riesgos en su paso 2.

La tercer instancia considerada dentro del criterio de estructura, es la estimación de los daños probables que pueden provocar las amenazas en el sistema afectable. Los elementos o actividades que se consideran para esta instancia, como lo muestra el cuadro comparativo 3, básicamente abarcan los pasos de análisis de vulnerabilidad e impactos que se realizan en las metodologías.

Estimación de los daños probables		SVA	MOSLER	RAM	CIDETES
Planteamiento de hipótesis sobre:					
	Eventos no deseados de seguridad	✓	✓*	✓	✓*
	consecuencias	✓		✓	✓*
Evaluación de consecuencias/impactos					
	Económicos	✓		✓	✓
	En la función del sistema		✓		✓*
	Psicológicos en la imagen del sistema		✓		
	Para la salud	✓		✓	✓*
	Ambientales	✓		✓	
	En la operación del negocio	✓			✓*
Alcance de los daños			✓		✓*
Identificación de las medidas de seguridad/funciones de seguridad		✓		✓	✓*
Evaluación física y operativa de los elementos del sistema de seguridad		✓*		✓*	✓
Evaluación de la efectividad del sistema de seguridad/ de las medidas de seguridad		✓		✓	
Determinación de Vulnerabilidades		✓		✓	✓*
Estimación del grado de las vulnerabilidades		✓	✓	✓	✓
Etapas en las que se realizan o están presentes estos elementos o actividades		1,3	1,2	2,3,5	4,5

Cuadro comparativo 3. Estimación de los daños probables
Fuente: Elaboración propia.

**Observaciones:* Aunque la evaluación física y operativa de los elementos del sistema de seguridad física no la realizan estrictamente, las metodologías SVA y RAM, al evaluar la efectividad de las medidas de seguridad y del sistema de seguridad física, respectivamente, se entiende que en algún momento es tratado por ambas metodologías. La metodología MOSLER en su paso 1, en realidad plantea una hipótesis sobre un evento no deseado de seguridad, en el que una amenaza puede dañar determinados bienes. La metodología CIDETES, al estimar el grado de vulnerabilidad de los activos con respecto de las amenazas, así como los impactos económicos que se pueden presentar si las amenazas se materializan, toma en cuenta, con excepción de la efectividad del sistema de seguridad física y los impactos ambientales, sociales y psicológicos, a los demás elementos o actividades consideradas para la instancia, solo que no se documenta ni se realiza de una forma estructurada.

Finalmente, el último elemento considerado en el criterio estructura, se refiere a las instancias adicionales consideradas por las metodologías. El cuadro comparativo 4, a continuación muestra el análisis sobre este elemento.

Instancias adicionales en las metodologías	SVA	MOSLER	RAM	CIDETES
Preparación de la metodología	✓			✓*
Caracterización del sistema regulador				
Propuestas para la reducción de riesgos	✓		✓	✓
Obtención de mapas de riesgo				✓
Diseño de programas de inversiones y presupuestos				✓
Seguimiento de la metodología	✓			✓*
Actualizaciones del sistema de seguridad física			✓	
Etapas en las que se realizan o están presentes estos elementos o actividades	5		7	7,8,9

Cuadro comparativo 4. Instancias adicionales en las metodologías
Fuente: Elaboración propia.

**Observaciones:* La metodología CIDETES no considera como parte de sus estructura la preparación de la misma, sin embargo, sí se considera al momento de iniciar el proyecto de seguridad física en la que es aplicada; se definen entre otras cosas: el equipo de trabajo, objetivos y alcance del estudio, la información requerida; además, se llevan a cabo visitas por parte del equipo de trabajo a las instalaciones en las que se aplicará la metodología. Con relación al seguimiento de la metodología, al venderse como un servicio, se hace la propuesta de seguir con la planeación de la implantación y la implantación de las propuestas realizadas.

3.2.2 Función

El objetivo principal de estas metodologías es la identificación y evaluación de aquellos elementos involucrados en eventos no deseados de seguridad física (amenazas, vulnerabilidades e impactos) que enfrenta un sistema (afectable) con la finalidad de estimar el riesgo asociado. Además, con excepción de la metodología MOSLER, las demás establecen propuestas orientadas a la reducción o mitigación del riesgo. Sin embargo, resulta interesante analizar a estas metodologías con referencia al proceso de planeación y conocer que instancias de este proceso sigue. El cuadro comparativo 5, que se presenta a continuación, muestra este análisis.

Etapas de planeación abordadas por las metodologías	SVA	MOSLER	RAM	CIDETES
Diagnóstico	✓	✓	✓	✓
Prescripción	✓		✓	✓
Instrumentación				
Control				

Cuadro comparativo 5. Etapas de planeación abordadas por las metodologías
Fuente: Elaboración propia

3.2.3 Evaluación del riesgo

Al ser su principal objetivo, todas las metodologías realizan la evaluación del riesgo, para lo cual utilizan diversos parámetros y elementos, que pueden o no, coincidir entre sí, además la forma en la que es obtenido (el riesgo) varía entre cada una de ellas. De esta manera resulta importante distinguir a esos parámetros y elementos en cada metodología.

Para el primer elemento analizado en este criterio, el cuadro comparativo 6 se presenta las variables que utiliza cada una de las metodologías, de las cuales, el manejo que la metodología RAM da al riesgo (menciona que es "aceptable" o "no aceptable") y la forma en que determina la efectividad del sistema de seguridad física (el tiempo es su principal unidad de medida), así como los valores que la metodología CIDETES utiliza en los impactos (corresponden a montos económicos), corresponden a un tipo de variable nominal; el resto son variables ordinales, puesto que su intención es establecer la mayor o menor medida del valor que es asignado a la variable.

Variables	SVA	MOSLER	RAM	CIDETES
Severidad del activo	✓			
Grado de severidad de las consecuencias e impactos causados por el ataque hacia los activos críticos	✓	✓	✓	✓
Grado con que las consecuencias afectan las funciones del sistema bajo estudio.		✓		
Grado con que los activos pueden ser sustituidos si son alcanzados por las amenazas.		✓		
Grado de perturbación y efectos psicológicos causados al sistema bajo estudio que afectan su imagen.		✓		
Alcance de los daños según la extensión de la amenaza		✓		
Grado de atracción para el adversario sobre los activos.	✓		✓	✓
Grado o nivel de la amenaza	✓		✓	
Grado de vulnerabilidad	✓	✓*	✓	✓
Importancia del suceso		✓		
Daños ocasionados		✓		
Carácter del riesgo		✓		
Probabilidad de ocurrencia de la amenaza		✓*		✓
Probabilidad de que se realice un ataque			✓	
Probabilidad de éxito de un ataque	✓	✓	✓	
Probabilidad de que el sistema de seguridad física sea efectivo contra un ataque ($1-P_E$)			✓	
Riesgo	✓	✓	✓	✓

Cuadro comparativo 6. Variables
Fuente: Elaboración propia

*Observaciones: La metodología MOSLER en su paso 2, define un criterio de vulnerabilidad, en el que se valora la probabilidad de que se produzca un daño si se manifiesta la amenaza, esto en realidad puede ser interpretado como la susceptibilidad

al daño, que corresponde a la definición formal del término *vulnerabilidad*, así, tomando como referencia los valores que son asignados a este criterio (de 1 al 5, de muy alta a muy baja) se considera que se trata del grado de vulnerabilidad. En ese mismo paso, se define el criterio de agresión, en el que se valora la probabilidad de que el riesgo se manifieste, y que en realidad hace referencia a la manifestación de la amenaza, ahora bien, aunque no se trate de una valor de probabilidad en un sentido estricto, se consideró así, para la realización del cuadro comparativo.

El segundo elemento bajo el cual se analiza la *evaluación del riesgo*, es con referencia a los criterios de evaluación que utilizan las metodologías. El cuadro comparativo 7, mostrado a continuación, presenta el análisis de este elemento. Este cuadro es construido a partir de los elementos a evaluar, se identifican los criterios bajo los cuales son evaluados, y de estos a su vez, los sub-criterios bajo los cuales pueden ser evaluados también.

Elemento a evaluar	**Criterios y sub-criterios utilizados por las metodologías**			
	SVA	**MOSLER**	**RAM**	**CIDETES**
Riesgo	✓ Probabilidad de éxito de un ataque ✓ Severidad de las consecuencias	✓ Carácter del riesgo ✓ Probabilidad de éxito de un ataque	✓ Probabilidad de ataque ✓ Probabilidad de que el sistema de seguridad sea efectivo contra un ataque / probabilidad de éxito de un ataque ✓ Consecuencias (severidad)	✓ Probabilidad de ocurrencia de la amenaza ✓ Grado de atracción de los activos ✓ Grado de vulnerabilidad ✓ Impactos
Probabilidad de éxito de un ataque	✓ Grado de atracción de los activos ✓ Grado de vulnerabilidad ✓ Nivel de la amenaza	✓ Agresión (probabilidad de ocurrencia de la amenaza) ✓ Vulnerabilidad	✓ Efectividad del sistema de seguridad física	
Carácter del riesgo		✓ Importancia del suceso ✓ Daños ocasionados (severidad de consecuencias)		
Probabilidad de ataque			✓Potencial de la amenaza ✓Grado de atracción sobre los activos	
Probabilidad de ocurrencia de la amenaza		✓ Agresión		✓ Antecedentes ✓ Capacidad e Intensión del adversario ✓ Factores sociales

Cuadro comparativo 7. Criterios y sub-criterios utilizados por las metodologías...Continúa en la siguiente página
Fuente: Elaboración propia

Elemento a evaluar	Criterios y sub-criterios utilizados por las metodologías			
	SVA	**MOSLER**	**RAM**	**CIDETES**
Severidad de las consecuencias / Impactos	✓ Severidad del activo: ○ Criticidad del activo (valor económico, emblemático, operacional, peligros a los que está expuesto) ✓ Consecuencias: ○ Efectos para la salud ○ Efectos económicos ○ Efectos ambientales ○ Interrupción del negocio (tiempo) ○ Daños materiales	✓ Profundidad (gravedad de la perturbación o efectos psicológicos con que es afectada la imagen del sistema) ✓ Extensión (alcance geográfico de los daños)	✓ Consecuencias: ○ Efectos para la salud ○ Pérdidas económicas ○ Daños ambientales ○ Periodo de los impactos ○ Alcance de los daños	✓ Consecuencias traducidas a montos económicos: ○ Efectos para la salud ○ Daños materiales ○ Interrupción del negocio ○ Sustitución de bienes
Grado de atracción de los activos	✓ Interés del adversario en función del valor del activo (económico, emblemático, funcional, etc.)		✓ Nivel deseado de consecuencias ✓ Ideología ✓ Facilidad de ataque	✓ Interés del adversario en función del valor del activo (económico, emblemático, funcional, etc.)
Grado de vulnerabilidad	✓ Efectividad de las capas de protección		✓ Efectividad del sistema de seguridad física	✓ Condición de los elementos físicos/normativos del sistema de seguridad.
Nivel de la amenaza / Potencial de la amenaza	✓ Intensión del adversario ✓ Capacidad del adversario ✓ Antecedentes históricos		✓ Capacidad del adversario ✓ Intensión del adversario ✓ Historia del adversario	
Importancia del suceso		✓ Función (gravedad con que las consecuencias negativas afectan a la función del sistema) ✓ Sustitución (facilidad con que pueden ser sustituidos los activos)		
Efectividad de las capas de protección / del sistema de seguridad	✓ Capacidad de: ○ Disuasión ○ Detección ○ Retardo ○ Respuesta		✓ Capacidad y tiempo de: ○ Detección ○ Retardo ○ Respuesta	

Cuadro comparativo 7. Criterios y sub-criterios utilizados por las metodologías… Continúa en la siguiente página
Fuente: Elaboración propia

Elemento a evaluar	Criterios y sub-criterios utilizados por las metodologías			
	SVA	MOSLER	RAM	CIDETES
Condición de los elementos físicos del sistema de seguridad física				✓ Falla en la operación. ✓ Equipo Incompleto. ✓ Falta de mantenimiento. ✓ Equipo dañado. ✓ Falta de supervisión. ✓ Obsolescencia. ✓ Innecesario. ✓ No permiten su operación. ✓ Su operación causa otro daño. ✓ No sirve, daño total o no existe.
Condición de los elementos normativos del sistema de seguridad física				✓ Falla en el uso de la información. ✓ Documentación Incompleta. ✓ Falta de actualización. ✓ Información equivocada. ✓ Falta de supervisión. ✓ Obsolescencia. ✓ Innecesario. ✓ No permiten su operación. ✓ Su aplicación causa problemas a otras áreas ✓ No existe.

Cuadro comparativo 7. Criterios y sub-criterios utilizados por las metodologías… Continuación
Fuente: Elaboración propia

Los conjuntos de posibles valores que las variables pueden tomar quedan establecidas por las escalas de medición empleadas por cada una de las metodologías, y las cuales constituyen el tercer elemento bajo el cual se analiza la *evaluación del riesgo*. A continuación, el cuadro comparativo 8, muestra este análisis.

Elemento	Escala	SVA	MOSLER	RAM	CIDETES
Clasificación del riesgo	Nominal			Aceptable No aceptable	
	ordinal	Alto Medio Bajo	Rango:2-1250 Muy Bajo Pequeño Normal Grande Elevado		Alto Medio Bajo
Severidad de las consecuencias / Impactos	Nominal				Valor absoluto del valor económico
	ordinal	Rango:1-5		Rango: 0 - 1	
Severidad del activo	Nominal				
	ordinal	Rango:1-5			
Grado de atracción del activo	Nominal				
	ordinal	Rango:1-5 Muy Bajo Bajo Medio Alto Muy Alto			Rango:0-100

Cuadro comparativo 8. Escalas empleadas por las metodologías **…** Continúa en la siguiente página
Fuente: Elaboración propia.

Elemento	Escala	SVA	MOSLER	RAM	CIDETES
Grado de vulnerabilidad	Nominal				
	ordinal	Rango:1-5 Muy Bajo Bajo Medio Alto Muy Alto	Rango 1-5 Muy Baja Baja Normal Alta Muy Alta		Rango:0-100
Profundidad	Nominal				
	ordinal		Rango 1-5 Muy leves Leves Limitadas Graves Muy graves		
Alcance	Nominal				
	ordinal		Rango 1-5 individual local regional nacional internacional		
Nivel de la amenaza / Potencial de la amenaza	Nominal				
	ordinal	Rango:1-5 Muy Bajo Bajo Medio Alto Muy Alto			
Agresión	Nominal				
	ordinal		Rango: 1-5 Muy Baja Baja Normal Alta Muy Alta		
Efectividad de las capas de protección / del sistema de seguridad	Nominal			Retraso: Valor del tiempo Respuesta: Tiempo, equipamiento, tácticas, capacidades	
	ordinal			Detección: probabilidad (0-1)	
Condición de los elementos físicos y normativos del sistema de seguridad física	Nominal				
	ordinal				Rango: 1-10

Cuadro comparativo 8. Escalas empleadas por las metodologías … Continúa en la siguiente página
Fuente: Elaboración propia

Elemento	Escala	SVA	MOSLER	RAM	CIDETES
Función	Nominal				
	ordinal		Rango 1-5 Muy levemente Levemente Medianamente Gravemente Muy gravemente		
Sustitución	Nominal				
	ordinal		Rango 1-5 Muy fácilmente fácilmente Sin muchas dificultades Difícilmente Muy difícilmente		

Cuadro comparativo 8. Escalas empleadas por las metodologías … Continuación
Fuente: Elaboración propia

El siguiente elemento en el proceso para la evaluación de riesgos es la definición de las unidades de medición, las cuales permiten asignar de forma clara un valor a los elementos que son evaluados. El cuadro comparativo 9, presentado a continuación, muestra el análisis para este elemento.

	Unidades de medición			
Elemento	**SVA***	**MOSLER**	**RAM***	**CIDETES***
Clasificación del riesgo	Sin definir	Sin definir	Sin definir	Sin definir
Severidad de las consecuencias / Impactos	✓ # Muertes ✓ # Heridos ✓ Valor económico de los activos ✓ Tiempo de interrupción del negocio	No se toma en cuenta	✓ Lesiones y muertes dentro o fuera de las instalaciones ✓ Contaminación provocada ✓ Pérdidas económicas ✓ Daños en servicios de abastecimiento ✓ # de años	Valor absoluto [$]
Severidad del activo	Sin definir	No se toma en cuenta	No se toma en cuenta	No se toma en cuenta
Grado de atracción del activo	✓ Valor económico de los activos ✓ Valor emblemático de los activos ✓ Valor funcional u operativo de los activos	No se toma en cuenta	Sin definir	Sin definir
Grado de vulnerabilidad	✓ # capas de medidas de seguridad ✓ # de debilidades de las medidas de seguridad	Sin definir	✓ Rendimiento del sistema de seguridad	Sin definir

Cuadro comparativo 9. Unidades de medición … Continúa en la siguiente página
Fuente: Elaboración propia

	SVA*	MOSLER	RAM*	CIDETES*
Profundidad	No se toma en cuenta	Sin definir	No se toma en cuenta	No se toma en cuenta
Alcance	No se toma en cuenta	1. Individual 2. Local 3. Regional 4. Nacional 5. Internacional	No se toma en cuenta	No se toma en cuenta
Nivel de la amenaza / Potencial de la amenaza	✓ Métodos ✓ Medios ✓ Acciones posibles ✓ Conocimiento de los adversarios ✓ Selección de los activos	No se toma en cuenta	Sin definir	No se toma en cuenta
Agresión/probabilidad de ocurrencia de la amenaza	No se toma en cuenta	Sin definir	No se toma en cuenta	Sin definir
Efectividad de las capas de protección / del sistema de seguridad	✓ # de debilidades de las medidas de seguridad	No se toma en cuenta	✓ Rendimiento del sistema de seguridad	No se toma en cuenta
Condición de los elementos físicos y normativos del sistema de seguridad física	No se toma en cuenta	No se toma en cuenta	No se toma en cuenta	✓ # de fallas (operativas, físicas, de información) de los elementos
Función	No se toma en cuenta	Sin definir	No se toma en cuenta	No se toma en cuenta
Sustitución	No se toma en cuenta	Sin definir	No se toma en cuenta	No se toma en cuenta

Cuadro comparativo 9. Unidades de medición … Continuación
Fuente: Elaboración propia

**Observaciones:* Para la metodología SVA no se definen de forma clara las unidades consideradas para el nivel de la amenaza, se habla de "evidencia creíble de la capacidad o intensión de alguna amenaza" o de "bajas amenazas", pero no se especifica como determinar esa capacidad o intensión; para el nivel de atracción del activo, se habla de "interés moderado", "interés alto" e "interés muy alto", lo cual no es propiamente una unidad de medición; en relación con la vulnerabilidad, se habla de la efectividad de las capas de las medidas de protección, pero no define con que unidades se determina dicha efectividad. Lo mismo ocurre en la metodología RAM, para la determinación de consecuencias se habla de "lesiones", "lesiones graves", "perdidas mayores", "perdidas menores", "perdidas inferiores", "daños ambientales graves", "daños ambientales mayores", "daños ambientales menores", "daños ambientales insignificantes"; en la parte de vulnerabilidad se habla de la efectividad de sistema de seguridad, en donde se mide el rendimiento de dicho sistema a través de diagramas, pero no se específica exactamente como se hace. Por su parte, la metodología CIDETES, para el valor de los impactos utiliza el valor absoluto de los montos económicos correspondientes a los daños estimados, y para determinar las condiciones de los elementos físicos y

normativos del sistema de seguridad, se centra en las posibles fallas que se pueden presentar, sin embargo, tampoco se definen claramente la unidades de medición.

3.2.4 Alcances y resultados

El análisis para el último criterio de comparación entre las metodologías es presentado a continuación en el cuadro comparativo 10.

Alcances y resultados	SVA	MOSLER	RAM	CIDETES
Valor cuantitativo del riesgo		✓	✓	✓
Valor cualitativo del riesgo	✓			
Clasificación del riesgo	✓	✓		✓
Efectividad del sistema de seguridad	✓		✓	
Análisis de vulnerabilidades	✓		✓	✓*
Análisis de amenazas	✓		✓	✓*
Mapa de riesgos				✓
Recomendaciones y/o propuestas para la reducción de riesgos	✓		✓	✓
Programa de inversión				✓

Cuadro comparativo 10. Alcances y resultados
Fuente: Elaboración propia

* Observaciones: En la metodología CIDETES el análisis de vulnerabilidades y el análisis de amenazas no se documenta y no existe una forma estructurada de realizarlo.

3.2.5 Resultados de la comparación

A continuación se presentan los aspectos relevantes de la comparación realizada entre las metodologías; para el criterio *estructura* se puede concluir, en el rubro sobre la caracterización del sistema expuesto, lo siguiente:

- La metodología SVA es la que profundiza más en su estudio, es la única que obtiene la severidad del activo crítico, además de identificar y definir la infraestructura crítica y las interdependencias que dan soporte a las funciones críticas, cubriendo en parte, el estudio sobre los subsistemas de subsistencia, un punto de suma importancia para los estudios de riesgos; después lo hacen (profundizan) las metodologías RAM, CIDETES y MOSLER, en ese orden, esta última incluso, sólo considera la identificación de posibles activos críticos para esta instancia, por lo que es la que menos profundiza en dicha instancia;

- La metodología CIDETES pretende aplicar un enfoque sistémico, sin embargo, sólo lista los elementos del sistema que son de interés para el estudio y deja de lado la caracterización de elementos relevantes como lo son el supra-sistema, los subsistemas, sus relaciones, sus funciones, etc., utilizando en realidad un enfoque reduccionista, en el que se aíslan dichos elementos. Estrictamente, ninguna de las metodologías lo hace.

Con referencia a la determinación de calamidades (análisis de amenazas):

- De alguna u otra manera las cuatro metodologías identifican a los adversarios. La metodología SVA es la única que realiza una estimación global del grado de atracción por los activos críticos; sin embargo, no estima la probabilidad de que ocurra la amenaza. De esta manera, junto con la metodología RAM, son las metodologías que profundizan de manera importante en este rubro; realizan un análisis muy parecido, en el que describen a los adversarios y enfatizan en la importancia sobre conocer si son internos, externos o una colusión de ambos; en contra parte, la metodología MOSLER es la que menos profundiza en ella, este análisis se limita a la identificación del posible activo crítico y la estimación de la probabilidad de ocurrencia de la amenaza;

- Por su parte la metodologías CIDETES, determina las posibles amenazas, sus expertos realizan un análisis sobre los medios y manifestaciones de estas, y para determinar la probabilidad de ocurrencia se hace una inspección sobre las condiciones internas y externas del sistema bajo estudio y las posibles motivaciones de quien ejecutará las acciones potenciales, sin embargo, esto no se documenta.

Al respecto de la estimación de los daños probables:

- Las cuatro metodologías lo hacen, aunque MOSLER es la que lo hace con menor grado de profundidad; además en su forma de analizar las consecuencias solo se consideran las funciones del sistema y perturbaciones psicológicas, sin considerar impactos ambientales, para la salud o económicos; por otro lado no determina las vulnerabilidades del sistema bajo estudio, ni considera, como parte de su estructura, un análisis sobre la efectividad de las medidas de seguridad, o bien, el sistema de seguridad física;

- La metodología SVA al apoyarse en la construcción de escenarios, y la RAM por su parte, en modelos lógicos, como los árboles de fallas, garantizan que se realice un análisis detallado de los eventos no deseados sobre seguridad, y de esta manera determinar la vulnerabilidad e impactos asociados para la obtención del riesgo;

- El análisis que se realiza en la metodología CIDETES va totalmente enfocado al plano económico, al ubicarse dentro de un proyecto como parte de un servicio, el cliente siempre está interesado en saber cuánto puede perder. Por otro lado se limita a una evaluación física y operativa de los elementos del sistema de seguridad física dejando de lado la efectividad propia de dicho sistema.

Finalmente, sobre las instancias adicionales consideradas por las metodologías:

- Ninguna de las metodologías utiliza el enfoque cibernético; no conceptualizan al sistema de gestión;

- La metodología MOSLER, es la única que no propone algún tipo de solución para la reducción de riesgos;

- La metodología RAM, al estar más enfocada en el diseño y evaluación del sistema de seguridad física, es la única que considera una actualización en dicho sistema, en la que después de obtener un valor inicial del riesgo y realizar propuestas orientadas a la reducción de riesgos y vulnerabilidades, vuelve a calcularlo para determinar si el nuevo valor encontrado es aceptable o no, y de esta manera terminar con el estudio o realizar nuevas propuestas; un aspecto a considerar es que no establece como determinar los niveles de riesgos aceptables o no aceptables;

- CIDETES es la única metodología que obtiene un mapa de riesgos, y considera, como parte de su estructura, la programación de inversiones y presupuestos.

Como resultado del análisis del criterio *función*, que toma como referencia al proceso de planeación presentado en el capítulo 2, se observa que, con excepción de la metodología MOSLER que sólo abarca la etapa de diagnóstico, el resto (SVA RAM y CIDETES) cubre también la etapa de prescripción, al establecer propuestas que tienen por objetivo la reducción de riesgos y vulnerabilidades (encontradas en el diagnóstico). La metodología CIDETES ofrece como servicio, la planeación de la implantación e incluso la implantación, con lo que se estaría considerando parte de la etapa de control, sin embargo, no forma parte de la estructura de la metodología.

Bajo el criterio *evaluación del riesgo* resulta claro observar que la forma en que obtienen el valor del riesgo es distinta en las cuatro metodologías, sin embargo, después de la comparación entre ellas, se pueden mencionar las diferencias y similitudes entre los elementos que utilizan para realizar esta parte.

En relación con las variables:

- Las cuatro metodologías manejan: el riesgo; las consecuencias (severidad de las consecuencias / impactos); y la vulnerabilidad (grado de vulnerabilidad), aunque la metodología MOSLER la define erróneamente, y la metodología RAM no le asigna formalmente un valor, ya que se centra en la efectividad del sistema de seguridad para estimar la probabilidad de que el sistema sea efectivo en contra de un ataque;

- El grado de atracción que sienten los adversarios por los activos es considerado por las metodologías SVA, RAM y CIDETES;

- CIDETES, deja de lado la probabilidad de éxito de un ataque, qué sí consideran las metodologías SVA, MOSLER y RAM.

Con referencia a los criterios, un elemento importante pero que no todas las metodologías abordan es la efectividad del sistema de seguridad; considerada en la probabilidad de éxito, por parte de la metodología RAM, es la que la realiza de una forma más completa, ya que se utilizan herramientas como el diagrama de secuencia de adversarios, y de esta

forma se establece una forma para medir dicha efectividad; sin embargo, aunque se basa en las funciones de detección, retardo y respuesta, deja de lado la función de disuasión, que sí considera la metodología SVA, pero la cual no establece como determinar esa efectividad. Bajo este mismo criterio, la metodología CIDETES es aplicada de manera similar a lo que realiza la metodología SVA, obtiene información sobre los elementos del sistema a través de formato en forma de cuestionarios, con la diferencia que se enfoca en una evaluación sobre el estado físico y operacional de los elementos, y deja de lado su efectividad. La metodología MOSLER, no toma en consideración este aspecto. Un aspecto que ninguna de las metodologías considera es el impacto que tienen los elementos del sistema de seguridad, en la propia seguridad del sistema afectable, y de esta manera conocer qué tanto estos elementos, en relación con su funcionalidad dentro del sistema de seguridad, contribuyen o incluso afectan la seguridad del sistema afectable.

Como conclusión sobre las escalas empleadas, aunque la literatura no muestra una justificación sobre sus valores, se puede inferir que se utiliza un "criterio de oportunidad", es decir, se buscan proporcionar rangos que sean fáciles de manejar por aquellos quienes apliquen la metodología.

Sobre las unidades de medición, se encontró que no se definen claramente, o bien, no se definen; se puede partir del supuesto, que la literatura presenta una descripción de carácter general y que para cada estudio se tendrán elementos distintos y condiciones distintas dependiendo del sistema en el que se aplique la metodología, sin embargo, se tendría que enfatizar en el hecho que es necesario definirlos al momento de realizar la evaluación, ya que el problema debido a la ambigüedad originada debido a esta definición poco clara, e incluso, su ausencia, puede causar pérdidas de tiempo en la aplicación de las metodologías, e incluso generar errores de percepción por parte de los equipos de trabajo, que se verían reflejados en un cálculo, también erróneo, del riesgo.

El último criterio alcances y resultados permite observar no solo que las cuatro metodologías calculan el riesgo, puesto que es su principal objetivo:

- La metodología SVA proporciona un valor cualitativo, MOSLER proporciona un valor cuantitativo y una clasificación cualitativa, al igual que la metodología CIDETES, por su parte la metodología RAM lo hace cuantitativamente;

- La metodología CIDETES es la única que construye un mapa de riesgos; y es la única que realiza un programa de inversión, en el que presenta los montos económicos necesarios para adquirir e implantar las propuestas tecnológicas.

Finalmente en esta sección se mencionan algunos elementos que la metodología CIDETES pretende agregar en su estructura y que ninguna de las metodologías abordan:

- Un análisis sobre el retorno de inversión en términos de la reducción del riesgo;
- Construir un indicador que refleje la reducción del riesgo;
- Construir indicadores que permitan la comparación entre diferentes sistemas en términos del valor del riesgo asociado a dichos sistemas.

3.3 Propuestas de adecuación para la metodología CIDETES

En esta sección se presentan las propuestas que han sido consideradas como aportes que enriquecen a la metodología CIDETES; una vez encontradas las diferencias y similitudes entre las metodologías en la sección anterior, así como las fortalezas y debilidades de la metodología CIDETES, las posibles adecuaciones a dicha metodología toman forma al retomar la experiencia que se tuvo en campo y las aportaciones que el grupo de expertos hizo durante uno de los últimos proyectos.

Se contempla la reestructuración de la metodología, iniciando con una preparación y 7 etapas:

- Etapa 0. Preparación de la metodología;
- Etapa 1. Caracterización del sistema afectable;
- Etapa 2. Caracterización del sistema perturbador;
- Etapa 3. Caracterización del sistema de gestión;
- Etapa 4. Evaluación del riesgo;
- Etapa 5. Propuesta para el tratamiento del riesgo;
- Etapa 6. Construcción del plan para la reducción de riesgos;
- Etapa 7. Control;

A continuación se aborda cada etapa propuesta, describiendo aquellos elementos que han sido agregados, o bien, modificados, mientras que aquellos que no han sido modificados solo son mencionados. En la figura 27 se muestra la representación gráfica de esta reestructuración, en la que se puede observar las etapas y pasos que la conforman. Por otro lado la figura 28 presenta una visualización de la metodología desde el punto de vista de las etapas del proceso de planeación discutido en el capítulo 2.

La realización de las etapas y pasos de la metodología dependen en gran medida de la participación de los expertos en seguridad y de las personas (profesionales formados en campos principalmente en ingeniería y técnicos especialistas en diversas áreas) que realizan el levantamiento en campo, por lo que existen diferentes perspectivas, que se debaten al momento de trabajar como equipo. Se recomienda, entonces, preparar sesiones de trabajo planeadas bajo alguna técnica participativa, con la finalidad de buscar una convergencia.

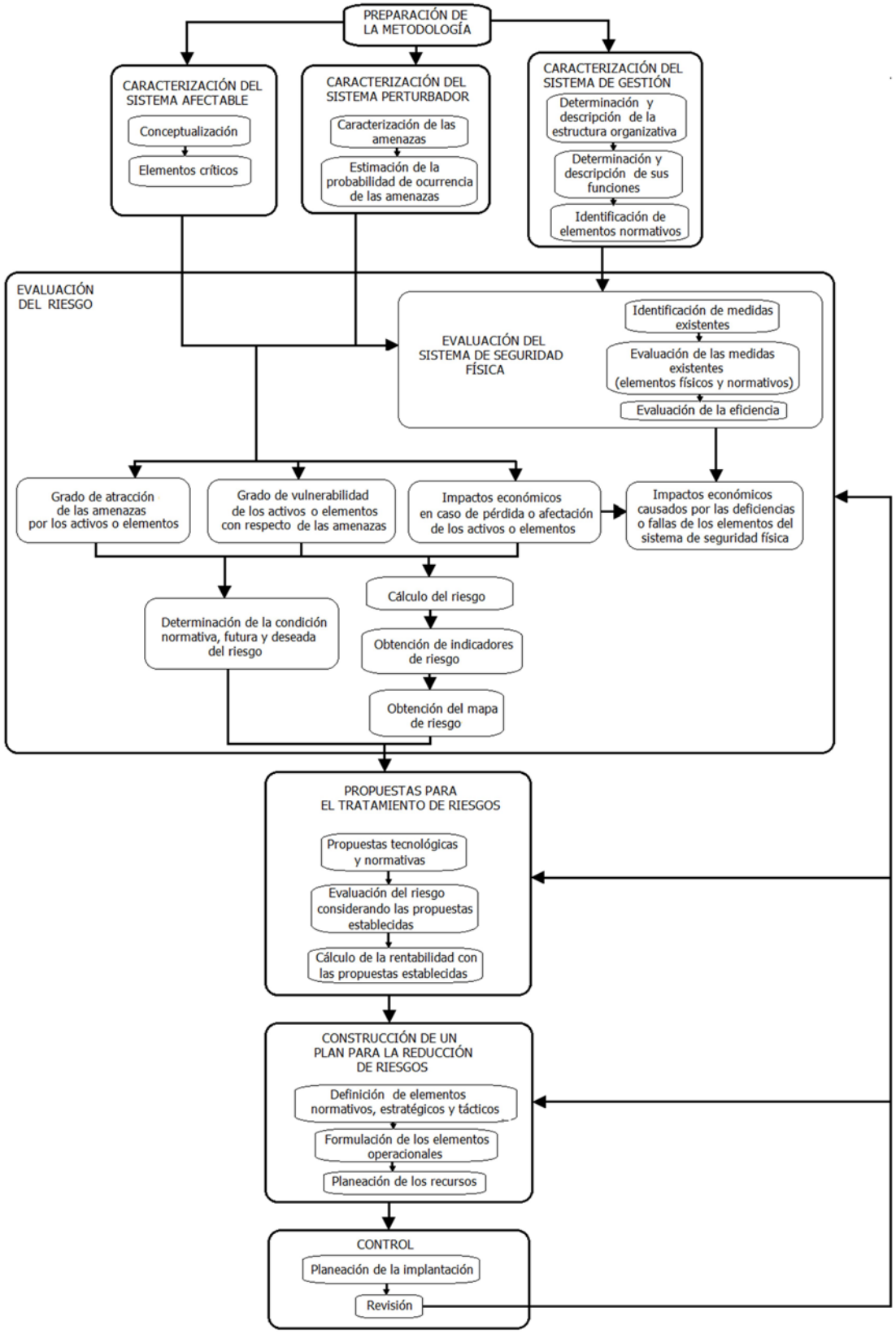

Figura 27. Representación gráfica de la reestructuración de la metodología CIDETES

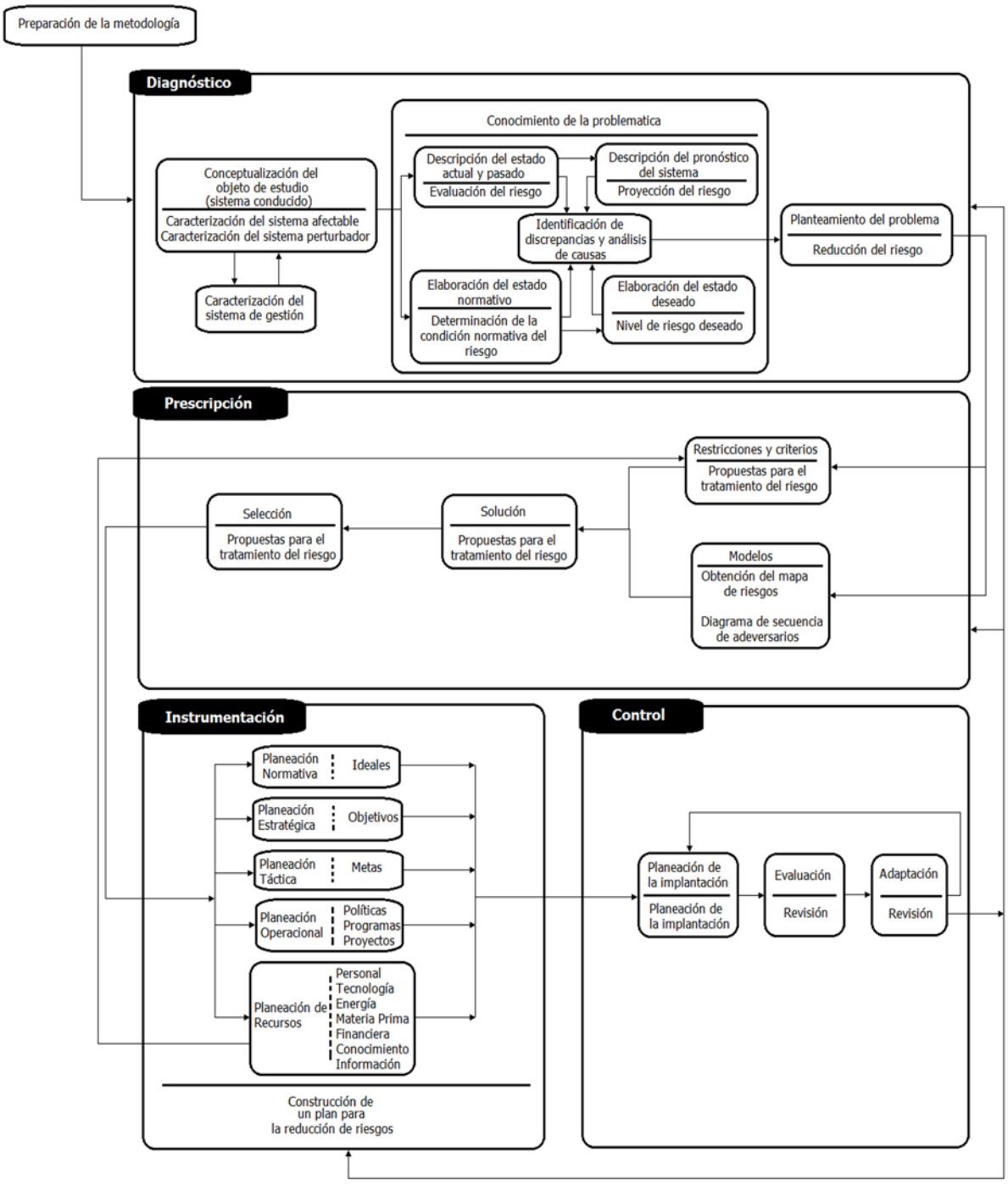

Figura 28. Visualización de la metodología CIDETES desde el punto de vista de las etapas del proceso de planeación

Etapa 0.- Preparación de la metodología

Antes de iniciar un proyecto, el CIDETES realiza una propuesta en la que, entre otras cosas, establece las características del personal que realizará el estudio de riesgos, y al iniciar el proyecto se selecciona dicho personal. Así mismo, en función del sistema, se establecen los objetivos y alcances del proyecto, se identifica la información requerida para las diferentes etapas, entre las que se encuentra el estudio de riesgos. Finalmente antes de iniciar con el proyecto se realiza una visita al sitio en el que se desarrollará el estudio, con la finalidad de conocerlo y tomar perspectiva de la magnitud e importancia del sistema.

Con la finalidad de ampliar el conocimiento sobre el sistema en el que se realizará el estudio, además de lo que ya se considera, se recomienda:

- Analizar los datos sobre incidentes anteriores en el sistema que será estudiado o en sistemas de la misma naturaleza en otras regiones (si existen).

- Realizar una investigación sobre aspectos sociales, políticos y económicos, de la localidad en la que se encuentra el sistema que será estudiado.

Etapa 1.- Caracterización del sistema afectable

En esta etapa se pretende construir una percepción holística del sistema afectable, conceptualizar al daño y sus consecuencias, como un estado de este sistema; así como determinar a los elementos relevantes del sistema a través de su criticidad.

Para ello se ha modificado la actual etapa 1 de la metodología, "definición del universo o sistema objeto del estudio de riesgo", reestructurándola en dos pasos: 1) conceptualización del sistema afectable; y 2) determinación de los activos críticos. A continuación se presentan las instancias o sub-pasos que se proponen para cubrirlos.

1.1 Conceptualización del sistema afectable:

a. Determinar su entorno (estructura externa).

   - Identificar y describir al supra-sistema
   - Definir el papel que desempeña el sistema afectable dentro de su supra-sistema, identificando sus objetivos y funciones
   - Identificar y describir los sistemas que se encuentran al mismo nivel que el sistema afectable dentro del supra-sistema

b. Determinar su estructura interna.
   - Identificar y describir los sub-sistemas, sus relaciones, funciones y elementos, hasta el nivel de desagregación que se considere pertinente para el estudio;

- Identificar y describir los sub-sistemas de subsistencia, sus relaciones, funciones y elementos, hasta el nivel de desagregación que se considere pertinente para el estudio.

c. Determinar los posibles estados del sistema, en colaboración con las autoridades de la entidad en la que se realiza el estudio, los cuales son (ver sección 2.1.5 del capítulo 2):

- Estados normales
- Estados insuficientes
- Estados de desastre
- Estados de retorno

1.2 Determinación de elementos críticos: Como resultado de este paso se generará una lista de elementos relevantes o críticos, se recomienda elegir entre 5 y 7 elementos, aquellos cuyo valor de criticidad sean los más altos. Se sugiere utilizar el formato mostrado en la figura 29.

ELEMENTO	VALOR			SOPORTE A FUNCIONES CRÍTICAS	INFRAESTRUCTURA CRÍTICA RELACIONADA CON EL ELEMENTO	POSIBLES CONSECUENCIAS POR DAÑO O PERDIDA	CRITICIDAD
	ECONÓMICO	EMBLEMÁTICO	OPERACIONAL				

Figura 29. Formato para identificar activos críticos

Los sub-pasos a seguir son:

a. Listar los posibles elementos, materiales y no materiales, que representan un valor económico, emblemático u operacional para el sistema afectable.

b. Identificar las funciones críticas, es decir, aquellas funciones que proporcionan sustento operacional al sistema (líneas de producción, suministro de combustibles, procesos de transformación de productos, etc.) y determinar que activos dan soporte a dichas funciones.

c. Identificar y describir la infraestructura crítica y las interdependencias que dan soporte a las operaciones críticas, como lo puede ser el suministro eléctrico, transporte, telecomunicaciones, etc. Se recomienda consultar los formatos seguidos por la metodología SVA, con la observación que dichos formatos van dirigidos a la industria petrolera y petroquímica.

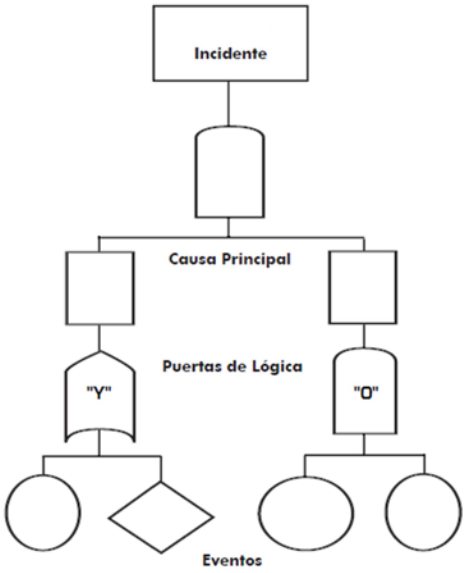

Figura 30. Diagrama de Árbol para el análisis de Fallas
Fuente: El Análisis de Fallas con Diagramas de Árbol. El Centro de Recursos del Departamento de Seguros de Texas.

d. Identificar las posibles consecuencias e impactos, que se presentarían si el elemento fuera atacado, y debido a su pérdida o afectación, manifiesta un efecto(s) en el sistema (social, ambiental, referentes a la salud, etc.), así como la facilidad o dificultad con que dicho elemento puede ser sustituido. Se sugiere utilizar modelos lógicos, como el "Análisis de Árbol de Fallas", (ver sección 3.3 de este capítulo, sobre la metodología RAM), ya que proporciona una representación gráfica sobre los elementos y las posibles consecuencias que pueden presentarse, ver figura 30.

e. Determinar el grado de criticidad, con base en el cual se elijan los elementos que serán analizados a lo largo del estudio de riesgos (elementos críticos). Será responsabilidad del grupo de trabajo definir los criterios, escalas y unidades de medición, en función del sistema que será estudiado.

   Se sugiere tomar como criterios al valor del activo (económico, emblemático y/u operacional) y las consecuencias que se tendrían si el elemento fuera dañado, total o parcialmente; con una escala ordinal discreta y con un rango entre 0 y 100, con la finalidad de guardar homogeneidad con las escalas empleadas por el CIDETES, en donde el 0 se utiliza para elementos que no son relevantes para el sistema y el 100 en el caso opuesto.

   La tabla 11, muestra un ejemplo de cómo podría ser estructurada esta forma de evaluar la criticidad de un elemento, cabe aclarar que no se trata de una escala formalmente propuesta, el fin es únicamente demostrativo, en el que se presentan las posibles unidades de medición que permitirían asignarle un valor a la criticidad del elemento.

Valor	Consecuencias		Criticidad
<$500,000.00	Sin heridos, ni muertes	Sin interrupción en la producción	0-4
		Con interrupción en la producción	5-8
	Heridos	Sin interrupción en la producción	9-12
		Con interrupción en la producción	13-16
	Muertes	Sin interrupción en la producción	17-20
		Con interrupción en la producción	21-24
>$500,000.00 <$750,000.00	Sin heridos, ni muertes	Sin interrupción en la producción	25-28
		Con interrupción en la producción	29-32
	Heridos	Sin interrupción en la producción	33-36
		Con interrupción en la producción	37-40
	Muertes	Sin interrupción en la producción	41-44
		Con interrupción en la producción	45-48
>$750,000.00 <$1,000,000.00	Sin heridos, ni muertes	Sin interrupción en la producción	49-52
		Con interrupción en la producción	53-56
	Heridos	Sin interrupción en la producción	57-60
		Con interrupción en la producción	61-64
	Muertes	Sin interrupción en la producción	65-68
		Con interrupción en la producción	69-72
>$1,000,000.00	Sin heridos, ni muertes	Sin interrupción en la producción	73-76
		Con interrupción en la producción	77-80
	Heridos	Sin interrupción en la producción	81-85
		Con interrupción en la producción	86-90
	Muertes	Sin interrupción en la producción	91-95
		Con interrupción en la producción	96-100

Tabla 11. Ejemplo de una posible escala de evaluación para determinar la criticidad

Etapa 2. Caracterización del sistema perturbador

Una vez conceptualizado el fenómeno del desastre, bajo la IID, se recomienda analizar al sistema perturbador, con la finalidad de entender cómo se pueden presentar o manifestar las amenazas, como se pueden generar los eventos "no deseados" de seguridad, y de esta manera, evaluar los impactos causados y analizar la factibilidad de intervención para controlarlos. Para ello se ha modificado la actual etapa 2 de la metodología, "definición de amenazas", reestructurándola en dos pasos: 1) caracterización de las amenazas; y 2) estimación de la probabilidad de ocurrencia de la amenaza. A continuación se describen los sub-pasos a seguir:

2.1 Caracterización de las amenazas (conocidas y potenciales):

a. Identificar a las amenazas (reconocimiento espacial y temporal), considerando:
   i. Nombre
   ii. Naturaleza
   iii. Historial de ocurrencias

b. Identificar y describir al adversario(s), considerando:
   i. Tipo (interno, externo, colusión de ambos)
   ii. Número
   iii. Posibles recursos que utilizan

c. Evaluar a las amenazas (reconocimiento de particularidades), considerando:

i. Parámetros directos:
   1. Capacidades:
      a. Acciones potenciales
      b. Medios (armas, formas de producir un daño)
      c. Métodos (forma de operación)
      d. Inteligencia
   2. Motivaciones
   3. Fortalezas
   4. Debilidades

ii. Parámetros indirectos:
   1. Primarios: posibles impactos causados por la amenaza, poniendo atención en aquellos que son manifestaciones propias de la amenaza;
   2. Agregados: aquellos que son resultado de integrar o transformar los anteriores.

iii. Parámetros específicos de la amenaza

d. Identificar los mecanismos de producción de eventos no deseados (ver sección 2.1.4):

i. Internos:

1) Preparación;
2) Iniciación;
3) Desarrollo;
4) Traslado;
5) Producción de impactos.

ii. Externos:

1) Encadenamiento corto
2) Encadenamiento largo
3) Encadenamiento integrado

2.2 Estimar la probabilidad de ocurrencia de la amenaza

En este punto un análisis estadístico sobre las incidencias de la amenaza es muy útil, sin embargo, la disponibilidad de la información es un aspecto que escapa en muchas ocasiones, además se debe poner énfasis que existen amenazas que no se han manifestado pero que en cualquier momento pueden presentarse. Para esto se propone utilizar 2 criterios: la motivación y la capacidad del adversario.

Motivación	Capacidad	Probabilidad
Alta Existen múltiples factores (condición social, económica, política, laboral) que hacen pensar que el adversario tendría un deseo muy fuerte de ejecutar algún acto en contra del sistema en estudio.	Alta El adversario presenta: • Más de una acción potencial • Puede atacar en más de una forma • Múltiples recursos (económicos, armas, etc.)	0.9 – 1.0
	Moderada El adversario presenta: • Por lo menos una acción potencial • Por lo menos una forma de atacar • Recursos limitados (económicos, armas, etc.)	0.8
	Baja El adversario presenta: • Una sola acción potencial • Por lo menos una forma de atacar • Recursos limitados (económicos, armas, etc.)	0.7
Moderada Existe por lo menos un factor o razón que hace pensar que el adversario tendría un deseo muy fuerte de ejecutar algún acto en contra del sistema en estudio.	Alta El adversario presenta: • Más de una acción potencial • Puede atacar en más de una forma • Múltiples recursos (económicos, armas, etc.)	0.6
	Moderada El adversario presenta: • Por lo menos una acción potencial • Por lo menos una forma de atacar • Recursos limitados (económicos, armas, etc.)	0.5
	Baja El adversario presenta: • Una sola acción potencial • Por lo menos una forma de atacar • Recursos limitados (económicos, armas, etc.)	0.4
Baja No existe una razón que permita considerar que el adversario desea ejecutar algún acto en contra del sistema en estudio.	Alta El adversario presenta: • Más de una acción potencial • Puede atacar en más de una forma • Múltiples recursos (económicos, armas, etc.)	0.3
	Moderada El adversario presenta: • Por lo menos una acción potencial • Por lo menos una forma de atacar • Recursos limitados (económicos, armas, etc.)	0.2
	Baja El adversario presenta: • Una sola acción potencial • Por lo menos una forma de atacar • Recursos limitados (económicos, armas, etc.)	0.0 – 0.1

Tabla 12. Definición de una posible escala para determinar la probabilidad de ocurrencia de la amenaza

A través del criterio *motivación* se trata de determinar si los adversarios tienen algún estímulo para querer afectar al sistema en estudio. Un análisis profundo de este rubro proporcionará una percepción sobre la postura del adversario, tomando en cuenta factores políticos, sociales y económicos que rodean al sistema, y especificando qué o cuáles son las razones que hacen que la motivación del adversario sea alta, moderada o baja, es decir, las unidades de medición empleadas.

La *capacidad* del adversario se refiere a las acciones potenciales (¿qué puede hacer), métodos (¿cómo lo puede hacer?), y medios (¿con qué lo puede hacer?); de lo obtenido en el sub-paso 2.1, se determinará si el adversario presenta una capacidad "alta", "moderada" o "baja", indicando en qué casos se considera cada categoría.

Como ejemplo se muestra la tabla 12, en la que se establecen unidades de medición que permiten estimar la probabilidad de ocurrencia de la amenaza, cabe aclarar que no se trata de una escala formalmente propuesta, el fin es únicamente demostrativo.

Etapa 3. Caracterización del sistema de gestión

Esta etapa actualmente no se realiza como parte de la metodología, sin embargo, la conceptualización de este sistema es importante como ya ha sido tratado por la IID. Aquí se pretende identificar y describir la estructura del sistema de gestión estableciendo sus atribuciones y responsabilidades, se proponen tres pasos a seguir:

3.1 Determinar y describir la estructura organizativa;

3.2 Determinar y describir sus funciones en términos del control de transiciones de los estados del sistema afectable (definidos en la etapa 1), identificando los estados del sistema de gestión (normal, alerta, emergencia –ver sección 2.1.6) y sus actividades;

3.3 Identificar los elementos normativos que existen, orientados a la reducción de riesgos y restablecimiento ante desastres (planes y programas).

Etapa 4. Evaluación del riesgo

Para esta etapa se propone reestructurar algunas de las etapas actuales de la metodología, además de agregar otras. A continuación se muestra la relación de modificaciones y adiciones hechas en esta etapa:

Etapas Modificadas	*Etapas Agregadas*	*Etapas sin cambios*
➢ *Grado de atracción con el que los activos representan un objetivo para las amenazas*	➢ *Evaluación del sistema de seguridad física*	➢ *Cálculo del riesgo;*
➢ *Grado de vulnerabilidad de los elementos con respecto de las amenazas*	➢ *Impactos causados por las deficiencias o fallas en los elementos del sistema de seguridad física*	➢ *Obtención del mapa de riesgos*
➢ *Impactos económicos en caso de pérdida o afectación de los activos*	➢ *Determinación de la condición normativa, futura y deseada del riesgo*	
	➢ *Obtención de indicadores de riesgo*	

De esta manera, la etapa quedaría estructurada bajo los siguientes pasos:

4.1 Evaluación del sistema de seguridad física;
4.2 Determinación del Grado de atracción con el que los activos representan un objetivo para las amenazas;
4.3 Grado de vulnerabilidad de los elementos con respecto de las amenazas;
4.4 Impactos económicos en caso de pérdida o afectación de los activos;
4.5 Impactos causados por las deficiencias o fallas en los elementos del sistema de seguridad física;
4.6 Cálculo del riesgo;
4.7 Determinación de la condición normativa, futura y deseada del riesgo;
4.8 Obtención de indicadores de riesgo;
4.9 Obtención del mapa de riesgo.

En los siguientes párrafos se describen las etapas que han sido modificadas y agregadas, siguiendo con el orden establecido.

4.1 Evaluación del sistema de seguridad física

El estudio sobre el sistema de seguridad física es una parte fundamental dentro de los proyectos que realiza el CIDETES, de él se desprenden conclusiones importantes para la evaluación de riesgos. Para este paso se propone seguir las siguientes instancias:

4.1.1 Identificar las medidas existentes en materia de seguridad, para lo cual se puede realizar una lista de verificación sobre los elementos físicos y normativos que deben existir.

4.1.2 Evaluar las medidas existentes en materia de seguridad (elementos físicos y normativos). Para lo cual se recomienda redefinir los criterios de evaluación manejados, así como las escalas y las unidades de medición; se entiende que dependerá en gran medida del sistema estudiado, y resulta complicado definir una forma general de evaluar a los elementos, ya que estos poseen diferentes propiedades. Como parte de esta propuesta, se definen, en la tabla 13, los criterios elegidos para realizar la evaluación de los elementos físicos y normativos del sistema de seguridad física:

Criterio	Definición	Escala	
Condición de los elementos físicos del sistema de seguridad			
Características	Cada elemento debe cumplir con determinadas particularidades que lo caracterizan como un elemento seguro, como puede ser el tipo de material del que está hecho, sus dimensiones, su forma, etc.	0	No cumple con las características necesarias
		1	Cumple al mínimo o parcialmente con las características necesarias
		2	Cumple con las características necesarias
Estado Físico	Se refiere a las condiciones bajo las que se encuentra el elemento, en este caso, físicas.	0	El elemento se encuentra en malas condiciones (por ejemplo rupturas o fracturas, etc.)
		1	El elemento presenta algunas imperfecciones
		2	El elemento se encuentra en óptimas condiciones
Mantenimiento	Hace referencia a las acciones destinadas al mejoramiento y conservación de los elementos físicos, a través de las cuales se hace posible recuperar, restaurar o renovarlos, y que se encuentren en condiciones óptimas y operen adecuadamente.	0	No se le da mantenimiento al elemento
		1	Se le da mantenimiento pero no regularmente
		2	Se le da mantenimiento regularmente
Operación / Funcionamiento	Tiene por objetivo conocer la forma en que el elemento realiza las funciones para las cuales fue destinado.	0	El elemento no opera o funciona
		1	El elemento presenta fallas de operación o funcionamiento
		2	El elemento opera o funciona adecuadamente
Condición de los elementos normativos			
Contenido	Cada elemento debe cubrir aspectos y puntos que lo definen como plan, programa o procedimiento.	0	Deja de lado aspectos de suma importancia
		1	Incluye solo algunos aspectos necesarios
		2	Incluye los aspectos necesarios
Estructura	Se refiere a la forma en la que se encuentra planteada la información o contenidos, de tal manera que es entendible, y resultan claros los conceptos e ideas del elemento normativo.	0	La información se encuentra mal estructurada.
		1	La información se encuentra estructurada deficientemente.
		2	La información se encuentra estructurada adecuadamente.
Revisión/ Actualización	Los planes, programas y procedimientos de seguridad física deben ser revisados y actualizados, de tal manera que sean corregidos, mejorados o que se abarquen otros aspectos de interés.	0	No se revisan o actualizan
		1	Se revisan o actualizan pero no regularmente
		2	Se revisan o actualizan regularmente
Aplicación / Ejecución	Se trata de medir el grado de cumplimiento del plan, programa o procedimiento, es decir, que sea ejecutado en tiempo y forma cuando es requerido.	0	No es ejecutado
		1	Se ejecuta pero no en su totalidad
		2	Se ejecuta en su totalidad
Impacto de los elementos físicos y normativos del sistema de seguridad en la seguridad del sistema afectable			
Impacto en la seguridad	A través de este criterio se estimará el grado en que los elementos dan soporte o incluso afectan la seguridad del sistema afectable, por medio de un análisis sobre el objetivo o fin último con el que forman parte del sistema de seguridad física.	-1	Se ha generado algún daño en el sistema
		0	Se compromete la integridad del sistema
		1	Da soporte a la seguridad del sistema

Tabla 13. Definición de los criterios para la evaluación de los elementos físicos y normativos del sistema de seguridad física.

El grupo de expertos definirá, de acuerdo con normas y estándares nacionales y/o internacionales, para cada elemento evaluado:

- Las características que son indispensables para que los elementos físicos cumplan con sus objetivos dentro del sistema de seguridad física;
- Las condiciones que hacen que el elemento físico se encuentre en "malas condiciones", "con algunas imperfecciones", o bien en "optimas imperfecciones";
- Los periodos pertinentes que garanticen que el programa de mantenimiento, en caso de existir, proporcione un estado óptimo a los elementos físicos;
- Las condiciones físicas o funcionales que hacen que el elemento físico "no opere" u "opere adecuadamente", y en su caso, qué fallas pueden presentarse;
- Los aspectos que deben considerar los elementos normativos para ser considerados como planes, programas o procedimientos;
- Las características que permiten diferenciar cuando la forma en la que se encuentra planteada la información, de los elementos normativos, se encuentra "mal estructurada", "deficientemente estructurada" y "estructurada adecuadamente";
- Los periodos pertinentes de revisión o actualización de los elementos normativos;
- Las condiciones que permiten distinguir cuando dicho los elementos normativos no son ejecutados, o ejecutados pero no en su totalidad o bien en su totalidad;

En las tablas 15 y 17 se muestra un ejemplo, con finalidad de mostrar una posible forma de definir estas unidades de medición, nuevamente se hace la aclaración de que no se trata de un propuesta formal, simplemente es un ejemplo sobre elementos ficticios, los cuales se han descrito en las tablas 14 y 16.

Elemento Físico	Descripción
Barda perimetral para una instalación cuyos procesos y productos son de gran importancia a nivel nacional	Debe tener al menos 2.10 metros de altura; debe ser de mampostería; idealmente se le debe dar mantenimiento por lo menos cada año

Tabla 14. Ejemplo de un elemento físico ficticio.

Criterio	Valor de la escala	Unidades de medición
Características	0	Su altura es menor a 2.0 m. y es de un material diferente a mampostería
	1	Su altura es mínimo de 2.10 m. aunque sea de un material distinto a la mampostería
	2	Su altura es de 2.10 m. o mayor, y el material de mampostería
Estado Físico	0	La barda presenta algunas de las siguientes características: ➢ discontinuidad en ciertos tramos; ➢ agujeros ➢ grietas
	1	La barda presenta deterioro del material que se encuentra hecha causado por humedad, erosión u otro factor.
	2	La barda se encuentra completa y sin ningún deterioro
Mantenimiento	0	No se le da mantenimiento.
	1	Se le da mantenimiento cada 5 años.
	2	Se le da mantenimiento cada año.
Operación / Funcionamiento	0	La barda no opera o funciona: ➢ Se tiene registro sobre intrusiones a través de ella. ➢ Existen características propias del elemento que favorecen la intrusión (agujeros, grietas, etc.)
	1	La barda presenta fallas de operación o funcionamiento: ➢ Se sabe, de manera no oficial, que ha habido intrusiones a través de ella. ➢ No existen características propias de la barda favorecen la intrusión, aunque existen factores naturales como árboles, montes a un lado de la barda, etc., que sí la favorecen.
	2	La barda opera o funciona adecuadamente: ➢ No existe registro ni rumor de que ha habido intrusiones a través de ella. ➢ No existen características que favorecen la intrusión.

Tabla 15. Ejemplo de una posible definición de las unidades de medición para un elemento físico ficticio.

Elemento Normativo	Descripción
Procedimiento sobre la revisión de vehículos que salen de las instalaciones en un punto de acceso y salida.	Debe contener 4 aspectos: ➢ Objetivo; ➢ Alcance; ➢ Descripción de las acciones a ejecutar; ➢ Descripción de las obligaciones que tiene los involucrados. Las acciones a ejecutar pueden ser: 1.- Detener el vehículo; 2.- Solicitar al conductor que salga del vehículo; 3.- Solicitar permiso de circulación dentro de las instalaciones; 4.- Verificar datos del permiso de circulación; 5.- Si no se cuenta con el permiso, comunicarse con las autoridades correspondientes; 6.- Revisar el interior del vehículo; 7.- Revisar la cajuela o parte trasera del vehículo; 8.- Revisar la parte de abajo del vehículo; 9.- Si se encuentra algún objeto extraño comunicarlo a las fuerzas de reacción; 10.- Si no se encuentra algún objeto extraño solicitar al conductor que ingrese al vehículo; 11.- Autorizar la salida del vehículo.

Tabla 16. Ejemplo de un elemento normativo ficticio.

Criterio	Valor de la escala	Unidades de medición
Contenido	0	El procedimiento no define el objetivo
	1	El procedimiento define los objetivos y las acciones a ejecutar, sin embargo no establece el alcance ni describe las obligaciones que tienen los involucrados.
	2	El procedimiento define su objetivo, alcance, descripción de las acciones a ejecutar y la descripción de las obligaciones que tienen los involucrados.
Estructura	0	Resulta imposible entenderla.
	1	Existen ambigüedades o incoherencias, que dificultan su entendimiento.
	2	Resulta clara y entendible.
Revisión/ Actualización	0	No se revisa y actualiza, o bien, lleva más de 3 años sin ser revisado o actualizado
	1	Se revisa y actualiza cada 2 años
	2	Se revisa y actualiza cada año
Aplicación / Ejecución	0	No se ejecutó ninguna de las acciones definidas en el procedimiento ni a vehículos propiedad de la instalación ni a vehículos externos.
	1	Cuando se presenta alguna de las siguientes situaciones: ➢ A vehículos externos se ejecutaron las 11 acciones y a vehículos propiedad de la instalación no. ➢ Tanto a vehículos externos como a externos se omitió por lo menos una de las acciones definidas ➢ Se ejecutaron las11 acciones pero no como se indica en el procedimiento (deficientemente)
	2	Se ejecutaron todas las acciones definidas en el procedimiento tanto a vehículos propiedad de la instalación como a vehículos externos, tal como se indica en el procedimiento

Tabla 17. Ejemplo de una posible definición de las unidades de medición para un elemento normativo ficticio.

Una vez evaluados los elementos, se sugiere establecer un factor de ponderación a los criterios establecidos:

Evaluación del elemento: $\alpha C1 + \beta C2 + \gamma C3 + \delta C4$

En donde: $\alpha + \beta + \gamma + \delta = 1$

Así mismo, se recomienda hacer una análisis estadístico sobre los resultados obtenidos, en primer instancia el promedio nos daría una medida de la evaluación de los elementos así como de los impactos en la seguridad, pero queda a discusión la utilización de otros estadísticos que expliquen o justifiquen dicha evaluación.

4.1.3 Evaluar la eficiencia del sistema de seguridad física, a través de un análisis de las funciones de disuasión, detección, retardo y respuesta, determinando:

- ✓ Existencia de elementos disuasivos (número, tipo, ubicación, etc.);
- ✓ La capacidad de detección (número de sensores o alarmas);
- ✓ El tiempo empleado en la evaluación de la alarma, reconocimiento del adversario y reporte;

- ✓ El tiempo, después de la detección, que emplearía el adversario para eludir los elementos de retardo (obstáculos);

- ✓ Tiempo en el que las fuerzas de reacción neutralizan, interrumpen o detienen el progreso del adversario, después de ser comunicados.

Se recomienda realizar diagramas de secuencia de los adversarios (ver sección 3.3 de este capítulo), ya que permiten mostrar los caminos que los adversarios pudieran seguir para alcanzar sus objetivos, realizando de esta manera, un diagrama por cada amenaza y objetivo, como se muestra en la figura 31.

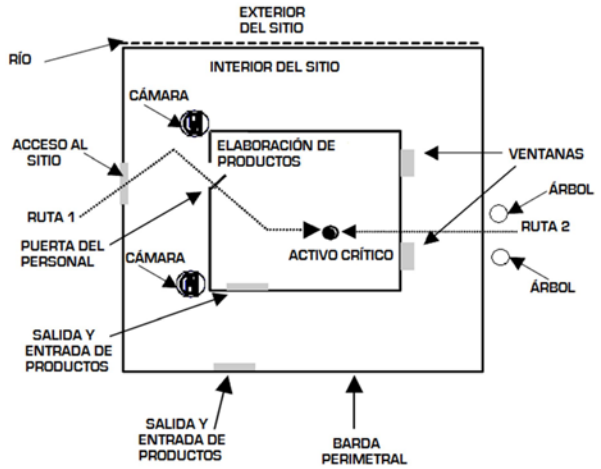

Figura 31. Diagrama de secuencia del adversario
Fuente: RAM White Paper, Sandia National Laboratories

	Activo Crítico	Funciones críticas	Infraestructura crítica
Amenaza			
Adversarios			
Probabilidad de Ocurrencia de la amenaza			
Interes del Adversario			
Grado de Atracción			
Evento no deseado			
Capas de seguridad			
Grado de Vulnerabilidad			
Consecuencias			
Impactos económicos			
Valor del riesgo			

Figura 32. Formato propuesto para la construcción de escenarios
Fuente: Elaboración propia

Una vez que se ha evaluado el sistema de seguridad física, para la obtención del riesgo se sugiere la construcción de escenarios con la finalidad de analizar la relación entre cada amenaza identificada y cada elemento crítico identificado. Se puede utilizar un formato parecido al mostrado en la figura 32, en el que se determina lo siguiente:

- El activo crítico, las funciones críticas que soporta y la infraestructura relacionada con dicho elemento serán retomados de la etapa1;

- La amenaza, los adversarios y la probabilidad de ocurrencia serán retomados de la etapa 2;

- El interés del adversario, se describirá en función del ánimo del adversario por el sistema en estudio y los daños que quisiera causarle;

- El grado de atracción de los activos para las amenazas, será establecido de acuerdo a lo establecido por el paso 4.2 de esta propuesta;

- El evento no deseado, descrito como una secuencia de hechos sobre cómo se presentarían o ejecutarían las posibles acciones de la amenaza contra el sistema, se apoyará en esta parte en los diagramas de secuencia de los adversarios realizados en el paso 4.1;

- Capas de seguridad, en este rubro se describirán las capas de seguridad que podrían ser superadas por el adversario, en relación con las funciones del sistema de seguridad (disuasión, detección, retardo y respuesta), y las líneas de defensa que superaría (de existir);

- Grado de vulnerabilidad, establecido por lo descrito en el paso 4.3 de esta propuesta;

- Consecuencias, en donde se describirán las posibles consecuencias partiendo del supuesto de que la amenaza se materializa y causa afectaciones al elemento crítico, incluyendo el caso de pérdida;

- Impactos económicos causados por la afectación del activo, determinado por lo obtenido en el paso 4.4 de esta propuesta;

- Valor del riesgo, se calculará conforme a lo establecido por la etapa 4.6 de esta propuesta.

4.2 Grado de atracción de las amenazas por los activos o elementos

Para determinar el grado de atracción que las amenazas "sienten" por los elementos o activos se sugiere seguir con lo establecido actualmente por la metodología, sin embargo, es necesario definir unidades de medición que permitan asignar un valor al grado de atracción. De esta manera, en la tabla 18 se muestra la propuesta para este fin; el rango de la escala no es modificado, solo es categorizado de acuerdo al interés por parte del adversario(s).

Grado de atracción de los activos para una amenaza	Valor
Sin interés. No existe interés alguno sobre el activo	0
Interés muy bajo. El interés del adversario no contempla causar daños en el sistema al alcanzar al elemento o activo, sus esfuerzos pueden concentrarse en: • Probar el sistema de seguridad; • Transmitir una advertencia.	1– 10
Interés bajo. El interés del adversario se encuentra enfocado en causar daños mínimos, reflejados en • Causar heridos; • Provocar pérdidas mínimas debido al poco valor económico, emblemático u operacional del activo.	11 – 30
Interés moderado. El interés del adversario se centra en causar daños relevantes, que abarcan: • Causar muertes (menos del 30%) • Causar pérdidas debido al alto valor económico, emblemático u operacional del elemento o activo, reflejadas en afectaciones hacia dicho elemento o activo. • Suspensión de las actividades (por meses) en las instalaciones (producción, generación de servicios, etc.)	31 – 60
Interés alto. El interés del adversario se centra en causar daños graves, que abarcan: • Causar muertes (menos del 60%) • Causar pérdidas debido al alto valor económico, emblemático u operacional del activo, reflejadas en la pérdida total del activo. • Suspensión de las actividades (por años) en las instalaciones (producción, generación de servicios, etc.)	61 – 90
Interés muy alto. El interés del adversario se centra en causar daños catastróficos, que abarcan: • Muertes (más de 60%) • Causar pérdidas debido al alto valor económico u operacional del activo, reflejadas en la pérdida total del elemento o activo, y por los daños agregados a esta, es decir, afectaciones o pérdidas de otros elementos o activos, abarcando gran parte de las instalaciones o toda la instalación. • Suspensión indefinida de las actividades en las instalaciones (producción, generación de servicios, etc.)	91 – 100

Tabla 18. Escala propuesta para determinar el grado de atracción de los activos para las amenazas

4.3 Grado de vulnerabilidad de los activos con respecto de las amenazas

Igual que en la determinación del grado de atracción de los activos, para hacer lo propio con el grado de vulnerabilidad de los activos o elemento con respecto de las amenazas, se sugiere seguir con lo establecido actualmente por la metodología, y se recomienda, también, definir unidades de medición que permitan asignar un valor al grado de vulnerabilidad, de la escala establecida, que va de 0 a 100, cuyo rango es categorizado en función de las líneas de defensa (si existen) o de las capas del sistema de seguridad física que el adversario sería capaz de superar con la intensión de alcanzar al elemento o activo y causar daño(s). La tabla 19, presenta la propuesta para la evaluación de este rubro.

Grado de vulnerabilidad	Valor
El adversario no lograría superar la primera línea de defensa, de existir; es detectado e inmediatamente neutralizado; los elementos disuasivos lo llevan a desistir de un ataque.	0
El adversario sería capaz de superar la primera línea de defensa, de existir, sin llegar al activo; sería detectado, los elementos de retardo serían suficientes en demorarlo para que las fuerzas de respuesta actuaran.	1 – 25
El adversario sería capaz de superar líneas intermedias de defensa, de existir, sin llegar al activo; sería detectado, los elementos de retardo serían suficientes para impedir que avanzara y aunque las fuerzas de respuesta tardarían, se neutralizaría al adversario; o bien, sería detectado, y aunque los elementos de retardo no serían suficientes para impedir que avanzara, las fuerzas de respuestas actuarían rápidamente neutralizando el adversario.	26 – 50
El adversario sería capaz de superar la última línea de defensa, de existir, sin poder llegar al activo; sería detectado, los elementos de retardo no serían suficientes para demorarlo y aunque las fuerzas de respuesta tardarían en actuar, se impediría que llegara al activo o elemento.	51 – 75
El adversario sería capaz de llegar al activo superando la última línea de defensa, de existir, y todas las capas del sistema de seguridad para provocar un daño	75 – 100

Tabla 19. Escala propuesta para determinar el grado de vulnerabilidad de los activos con respecto a las amenazas

4.4 Impactos económicos en caso de pérdida o afectación de los activos

Para la determinación de impactos, al igual que en los dos pasos anteriores, se recomienda seguir lo establecido actualmente por la metodología, en este sentido se determinarán las consecuencias que se tendrían si una amenaza alcanza o logra dañar a su objetivo. Ahora bien, en la construcción de escenarios, se debe describir la secuencia de eventos no deseados, con la finalidad de entender con mayor profundidad dichas consecuencias, por ejemplo, al considerar los impactos agregados o encadenados, que son causados indirectamente.

Estas consecuencias pueden ser medidas de diversas maneras, sin embargo, para la metodología CIDETES, lo más representativo es determinar el valor económico de dichas consecuencias. En este sentido los costos de las pérdidas pueden ser directos e indirectos, y en ellos se debe considerar:

- Costos por "sustitución permanente", que se refieren a los costos por reemplazar de forma permanente al elemento, si se trata de una herramienta de producción, o bien, si el activo es un producto, se puede optar por no sustituirlo, absorbiendo el costo de producción y las ganancias no obtenidas. En este caso, para determinar el costo se debe considerar:
  - ✓ Precio de compra o costo de producción;
  - ✓ Fletes y gastos de envío, y;
  - ✓ Costos de instalación y hacerlo funcional.

- Costos por "sustitución temporal", que se pueden presentar por la necesidad de adquirir elementos sustitutos en espera de reemplazos permanentes, pretendiendo reducir entre otras cosas: pérdida en ventas, sanciones, decomisos, etc. Para ello se debe considerar:
  - ✓ Costo de arrendamiento o alquiler, y;
  - ✓ Costos por mano de obra (por ejemplo, horas extras)

- Costos "derivados", considerados cuando existen salidas de actividades que son entradas de otras, y debido a las afectaciones se presentan tiempos de inactividad, o bien, equipos y personal son subutilizados.

- Costos por "pérdidas de ingresos", que se pueden dar cuando el capital que se va a utilizar para adquirir sustitutos temporales o permanentes, corresponde a inversiones que, en otras condiciones, se realizarían en diversos tipos de valores que le generarían ingresos, de esta manera, dichos ingresos deben ser considerados como parte de la pérdida. Para determinar esto se puede utilizar la siguiente fórmula:

$$I = \frac{i}{365} \times P \times t$$

En donde:

I = ingreso ganado
i = tasa porcentual anual de retorno
P = Capital disponible para la inversión
t = tiempo (en días) en la que P está disponible para la inversión

Un seguro cubre en parte, las posibles pérdidas que se pueden presentar, aunque en muchos casos lejos del total, además de incluir un costo de compra o primas de emisión relacionadas con los elementos asegurados, cantidades, que en la medida de lo disponible, deben ser restadas de la cantidad cubierta.

Se debe considerar, entonces, el peor de los casos en vista de la pérdida máxima probable, de ocurrir un evento no deseado, para ello se puede utilizar la siguiente fórmula:

$$K = (Cp + Ct + Cr + Ci) - (I - a)$$

En donde:

K = criticidad, el costo total de pérdida
Cp = costo de reemplazo permanente
Ct = costo de la sustitución temporal
CRM = costos totales relacionados
Ci = costo por pérdida de ingresos
I = seguro o indemnización
a = monto de la prima del seguro

4.5 Impactos económicos causados por las deficiencias o fallas en los elementos del sistema de seguridad física

Actualmente este análisis se realiza al considerar algunos de los elementos del sistema de seguridad física como activos o elementos críticos, sin embargo, se sugiere realizar este análisis por separado. Con esto se puede justificar la posible inversión en los elementos del sistema de seguridad física.

Por ejemplo, en la tabla 20 y 21, se muestra el siguiente caso ficticio: después de determinar los impactos económicos, en el paso anterior, de la amenaza "robo" sobre los activos 1, 2, 3, 4 y 5, se encontró que en un momento determinado se pierden $1,000,000.00, sin embargo, al hacer el análisis sobre los elementos del sistema de seguridad física involucrados, se tiene que debido a las fallas de la barda perimetral el robo se da en un 70%, debido al acceso sur el 20% y debido al acceso norte el 10%, lo que representan pérdidas de $700,000.00, $200,000.00 y $100,000.00 respectivamente, debido a las fallas de los elementos del sistema de seguridad física.

Impacto económico causado por la amenaza robo sobre los activos		**Amenaza**
		Robo
Activos Críticos	**Activo 1**	$100,000.00
	Activo 2	$500,000.00
	Activo 3	$200,000.00
	Activo 4	$150,000.00
	Activo 5	$50,000.00

Tabla 20. Ejemplo de un caso ficticio sobre el impacto económico causado por la amenaza robo en 5 activos

Elemento del sistema de seguridad física	Porcentaje de Robo, causado por el elemento del sistema de seguridad física	Impacto económico debido a las fallas o deficiencias del elemento del sistema de seguridad física
Barda Perimetral	0.70	$700,000.00
Acceso Sur	0.20	$200,000.00
Acceso Norte	0.10	$100,000.00

Tabla 21. Ejemplo de un análisis sobre los impactos económicos causados por las deficiencias o fallas de elementos del sistema de seguridad física.

4.9 Determinación de la condición normativa, futura y deseada del riesgo;

Después de obtener el valor del riesgo para cada elemento y las condiciones asociadas a éste, con la finalidad de estructurar la problemática asociada a dicho concepto, se recomienda realizar el análisis sobre las condiciones que debieran de cumplirse o existir, en el rubro de seguridad física, es decir, el estado normativo, el cual será contrastado con los resultados obtenido en las etapas anteriores, es decir las condiciones reales asociadas al riesgo.

Uno de las objetivos de este paso es proporcionar una idea del valor que tendrá el riesgo en el mediano y largo plazo, se sugiere la construcción de escenarios futuros, los cuales pueden ser tendenciales y/o catastróficos, en los primeros se parte de la hipótesis de que no se realizará una intervención que cambie el rumbo de la situación encontrada, y en los últimos se parte de la hipótesis de que sucede lo indeseable, ubicando al sistema afectable en estado de desastre.

Otro objetivo de este paso es establecer las condiciones ideales sobre el riesgo, siguiendo la misma idea de los escenarios futuros, solo que en este caso se partirá de la hipótesis de que se cuenta con estructuras potencialmente deferentes a las actuales que hacen que el sistema afectable se encuentre siempre en un estado normal.

Una vez encontrado el posible valor del riesgo tendencial y/o catastrófico se confrontará con el valor deseado, se identificarán las discrepancias entre uno y otro, y se analizarán las causas de dichas discrepancias.

El grupo de expertos determinará bajo que variables realizará estos análisis, se sugiere poner énfasis en el sistema de seguridad física y la vulnerabilidad de los elementos críticos.

4.10 Generación de indicadores de riesgo

Este paso surge como una inquietud por contar con indicadores que permitan expresar resultados referentes al riesgo obtenido en la evaluación; un resultado interesante es comparar diferentes sistemas con relación al riesgo asociado a cada uno de ellos, sin embargo, no es posible hacerlo simplemente con este valor, puesto que cada sistema posee características distintas, su valor (capital), su entorno social o su entorno ambiental.

El primer indicador propuesto trata de cuantificar el riesgo de un sistema en relación con su valor en términos monetarios (capital), de la siguiente manera:

$$RS = Suma\ Total\ del\ Riesgo\ \times \frac{Suma\ Total\ de\ las\ pérdidas\ económicas}{Capital\ o\ Valor\ de\ la\ empresa}$$

Un segundo indicador propuesto, obtiene el valor total de los impactos en los rubros económico, social y ambiental, teniendo de esta manera, una referencia del impacto global que se tendría en cada sistema estudiado. Se sugiere asignar una ponderación en relación a la importancia de estos impactos, así se tendría la siguiente expresión:

$$\text{Impacto total} = \alpha\ \text{Ie} + \beta\ \text{Is} + \gamma\ \text{Ia}$$

Donde:

Ie = Impacto económico
Is = Impacto social
Ia = Impacto ambientas
α = ponderación de la importancia para el impacto económico
β = ponderación de la importancia para el impacto social
γ = ponderación de la importancia para el impacto ambiental
$\alpha + \beta + \gamma = 1$

Etapa 5. Propuestas para el tratamiento del riesgo

Al igual que en la etapa anterior se propone reestructurar algunas de las instancias actuales de la metodología y agregar otras. A continuación se muestra la relación de modificaciones y adiciones hechas en esta etapa:

Etapas Modificadas	*Etapas Agregadas*	*Etapas sin cambios*
➢ *Equipamiento.*	➢ *Propuestas tecnológicas y normativas;* ➢ *Evaluación del riesgo considerando las propuestas establecidas;* ➢ *Cálculo de la rentabilidad con las propuestas establecidas*	

De acuerdo a esto, la etapa estará conformada por los siguientes pasos:

5.1) Propuestas tecnológicas y normativas;
5.2) Evaluación del riesgo considerando las propuestas establecidas;
5.3) Cálculo de la rentabilidad con las propuestas establecidas;

En los siguientes párrafos se describen las etapas que han sido modificadas y agregadas, siguiendo con el orden establecido.

5.1 Propuestas tecnológicas y normativas

En este paso, se propone integrar tanto las propuestas tecnológicas establecidas en la el *equipamiento*, como lo referente al ámbito normativo al plantear la reestructuración de planes, programas y procedimientos.

5.2 Evaluación del riesgo después de las propuestas

Una vez realizados los pasos 5.1 y 5.2, se tendrá el monto de la inversión requerida para reforzar el sistema de seguridad. Se recomienda entonces, calcular nuevamente el riesgo, en función de las mejoras que se tendrían en el sistema de seguridad con dicha inversión, y de esta manera tener una justificación de la importancia de la inversión. Al obtener los dos valores del riesgo, se podrá realizar una comparación de ambos valores y tener, finalmente, un índice de la reducción del riesgo debido a las propuestas establecidas, a través de la siguiente fórmula:

$$Reducción\ del\ riesgo = \frac{Valor\ del\ riesgo\ después\ de\ las\ propuestas}{Valor\ del\ riesgo\ antes\ de\ las\ propuestas} \times 100$$

5.3 Cálculo de la rentabilidad

La inversión que se realizará en el sistema de seguridad como resultado de las propuestas establecidas debe considerar, por un lado, los ingresos perdidos por destinar dicha inversión en el sistema de seguridad física y no en otros valores que redituarían en ganancias, y por otro, los costos propios de prevención, referentes a los costos totales correspondientes al sistema de seguridad, tomando en cuenta:

- Los gastos de personal (sueldos, salarios y beneficios).
- Todas las partidas de gastos, tales como teléfono, correo, viajes, membrecías, servicios adquiridos, etc.
- La parte proporcional del costo de capital, correspondiente a la depreciación de los elementos del sistema de seguridad.

Esta inversión en adquisición e implantación de tecnologías, así como en elementos normativos, requiere un análisis sobre el beneficio económico que representa realizar dicha inversión. Una forma es demostrar que las posibles pérdidas que pudieran ocurrir sin el sistema de seguridad no se presentarán, y que los costos asociados a esas pérdidas son mayores que los asociados al sistema de seguridad; por otro lado resulta conveniente demostrar que si los costos de las pérdidas que se producen a pesar de la inversión en el sistema de seguridad, así como los costos asociados el sistema de seguridad son menores, en conjunto y por un periodo determinado, que los costos que se habrían producido sin el sistema de seguridad, entonces la inversión habrá sido exitosa.

De esta manera, es necesario realizar una segunda estimación sobre las pérdidas que se pueden presentar a pesar de haber invertido en las propuestas establecidas, obteniendo así, los montos globales evitados. Por otro lado se debe tratar de identificar y evaluar las recuperaciones como resultado de invertir en dichas propuestas, ya que este valor representa parte de la rentabilidad de los costos que se realizarán.

La consideración de estos aspectos, permitirán entonces, medir los gastos realizados en el sistema de seguridad en un periodo determinado, por ejemplo, en un año, a través de la siguiente ecuación:

$$ROE = \frac{AL + R}{CSP}$$

En donde:

AL = Pérdidas evitadas
R = Recuperaciones hechas
CSP = Costo del sistema de seguridad
ROE = Rendimiento de los gastos realizados (return on expenditures)

De esta manera un análisis del resultado de esta ecuación permitirá establecer que:

- ROE = 1, significa que por lo menos el sistema de seguridad se sustenta por sí mismo.
- ROE < 1, el sistema de seguridad causa más pérdidas.
- ROE > 1, el sistema de seguridad agrega valor.

Etapa 6. Construcción de un plan para la reducción de riesgos

Para esta etapa se retoma lo realizado por la metodología en el diseño del programa de inversiones y presupuestos, sin embargo se pretende ir más allá, al buscar transformar las propuestas para el tratamiento del riesgo, encontradas en el paso anterior, en un conjunto de elementos específicos a través de:

- Definición de los elementos normativos, estratégicos y tácticos: ideales, objetivos, estrategias, alcances y metas;
- Formulación de los elementos operacionales: políticas, programas y proyectos;
- Planeación de los recursos, definiendo el personal requerido, el presupuesto, etc.

Etapa 7. Control

En esta etapa en primer lugar se realizará la *planeación de la implantación*, consistente en el diseño de procedimientos para la toma de decisiones y la organización para la realización del plan.

Posteriormente se realizará una *revisión* en la que se comparará lo planeado con lo real a través de una evaluación de los resultados obtenidos y una retroalimentación con las etapas anteriores, con la finalidad de corregir y mejorar lo establecido en programas, presupuestos y en general en el plan, y de esta manera, determinar su eficiencia en términos del logro de objetivos y metas, la identificación de errores, así como establecer los cambios y ajustes pertinentes.

Para lograr lo anterior se requiere:

7.1 Definir indicadores que permitan juzgar el estado actual del sistema y el avance logrado.

7.2 Diseñar e instrumentar un sistema de información con la finalidad de recabar, procesar y analizar los datos.

DISCUSIÓN DE RESULTADOS Y CONCLUSIONES

CAPÍTULO 4

Como parte final de este trabajo de investigación, los resultados y conclusiones se presentan entorno a cinco puntos que han guiado su elaboración:

1. El análisis comparativo entre las metodologías;
2. Las fortalezas y debilidades de la metodología CIDETES;
3. Las propuestas de adecuación a la metodología CIDETES;
4. La forma en que la metodología CIDETES es robustecida en su teoría y práctica;
5. El alcance propuesto al inicio de la investigación.

Sobre la comparación entre las metodologías se tienen las siguientes consideraciones:

- En relación con lo establecido por la Investigación Interdisciplinaria de Desastre sobre los rubros que deben ser contemplados por cualquier metodología de estimación de riesgos (determinación de calamidades, descripción de calamidades y estimación de los daños probables), se encontró que son abordados en mayor o menor medida por todas las metodologías, la que más profundiza en ellos es la metodología SVA; la metodología CIDETES, por su parte, aborda muchos de los aspectos considerados por las demás metodologías en la cobertura de esto rubros, sin embrago, no son documentado, o bien, no se encuentran estructurados como parte de la metodología;

- Ninguna de las metodologías abarcan aspectos referentes a la instrumentación y control, que les permitan ser consideradas como un apoyo importante en la toma de decisiones;

- Se le da poca importancia a la infraestructura crítica, la metodología SVA es la única que la identifica;

- Los criterios, escalas y unidades de medición definidos y empleados generan subjetividad y ambigüedad que puede ocasionar pérdidas de tiempo, errores de percepción e incluso impactar negativamente en los resultados del estudio;

- En general, el riesgo no es conceptualizado desde un enfoque sistémico y cibernético que permita identificar y construir los elementos asociados a éste como un todo, en este sentido los sistemas afectable y perturbador son caracterizados parcialmente, mientras que el sistema de gestión no es tomado en cuenta.

Con relación a la metodología CIDETES, después de haberla aplicado (en campo), analizado estructural y funcionalmente, y comparado con las demás metodologías, sobre sus fortalezas se puede mencionar:

- Es la única metodologías que construye un mapa de riesgos, el cual permite ubicar gráficamente las diversas áreas y activos asociados con el valor del riesgo encontrado, además de facilitar la ubicación de los equipos tecnológicos que son propuestos;

- Es la única que considera, como parte de su estructura, la programación de inversiones y presupuestos, que proporciona un aporte sobre los costos que se tendrán si se implantan las propuestas que resulten de aplicar la metodología.

Mientras que sobre sus debilidades se encontró:

- En la etapa sobre la "*definición del universo o sistema objeto del estudio de riesgo*", se pretende aplicar un enfoque sistémico, sin embargo, solo se realiza un listado de los elementos del sistema afectable, que corresponde entonces a un enfoque reduccionista que impide conceptualizar como un todo al sistema afectable;

- En la etapa sobre la "*Identificación y definición de amenazas*", al análisis que se realiza no se encuentra estructurado y no es documentado, lo que ocasiona una percepción limitada de este elemento;

- Sobre la "determinación del grado con el que los elementos representan un objetivo para las amenazas", la "determinación del grado de vulnerabilidad de los elementos con respecto de las amenazas" y la "determinación del impacto en caso de pérdida de los elementos", no se definen unidades de medición, dificultando la ubicación del valor que será asignado;

- El análisis que se realiza sobre el sistema de seguridad es limitado, pues sólo se centra en el estado físico de los elementos, y la definición de sus criterios es errónea y ambigüa en algunos casos, lo que causa confusión al momento de evaluarlos.

De esta manera se identificaron aspectos en los que se pueden establecer adecuaciones, además de elementos que pueden ser incluidos o agregados, y con ello enriquecer a la metodología CIDETES, así para este fin, con base en lo establecido por la IID, lo encontrado en las otras metodologías y lo experimentado en campo, se re-estructuró la metodología, iniciando con una etapa de preparación y 7 etapas principales, en las cuáles básicamente se propuso lo siguiente:

- En la etapa 1: *caracterizar al sistema afectable* en dos pasos, a través de los cuales, se conceptualiza al sistema y se identifican los elementos de interés incorporando la obtención de su criticidad, en donde se resalta la importancia de la definición de criterios y unidades de medición por parte del grupo de expertos;

- En la etapa 2: *caracterizar al sistema perturbador*, a través de la identificación y evaluación de amenazas y adversarios, con la finalidad de conocer los mecanismos de producción y estimar su probabilidad de ocurrencia, esta última como una función de la

motivación y la capacidad del adversario, resaltando la importancia de que el grupo de expertos defina las unidades de medición.

- En la etapa 3: *caracterizar al sistema regulador*, con la finalidad de entender y ubicar el papel e importancia del sistema conducente en el fenómeno de desastres, al determinar y describir su estructura organizativa y sus funciones, así como la identificación de los elementos normativos gestionados en materia de seguridad (reducción y prevención riesgos);

- En la etapa 4: evaluar el riesgo; se incluye formalmente como parte de la metodología la *evaluación del sistema de seguridad*, enfocándose en su efectividad y en el impacto en la seguridad del sistema afectable, y no solamente en el estado físico de los elementos de dicho sistema, se redefinieron los criterios y escalas considerados, resaltando la importancia de que el grupo de expertos defina las unidades de medición. Posterior a esta evaluación bajo un enfoque de construcción de escenarios se pretende obtener las condiciones actuales y pasadas relacionadas con el riesgo.

  El grado de atracción con que los activos representan un objetivo para las amenazas, el grado de vulnerabilidad de los elementos con respecto de las amenazas y los impactos económicos en caso de pérdida o afectación de los elementos o activos, fueron modificadas al categorizar el rango de la escala y definir unidades de medición, en el último paso se establecieron los costos que deben ser considerados para la obtención de dicho impacto económico.

  Otros pasos agregados en esta etapa fueron: los *impactos económicos causados por las fallas o deficiencias de los elementos del sistema de seguridad física* con la finalidad de justificar la inversión en el sistema de seguridad; la *determinación de la condición normativa, futura y deseada del riesgo*, en donde se construyen escenarios futuros con la intensión de identificar discrepancias y analizar sus causas, al comparar las condiciones actuales y pasadas con las normativas, así como las tendenciales o catastróficas con las deseadas; y la *generación de indicadores de riesgo*, a través de los cuales sea posible comparar diferentes sistemas.

  El cálculo del riesgo y la obtención del mapa de riesgos, pasos que complementan esta etapa 4, no fueron modificados.

- En la etapa 5: establecer las propuestas tecnológicas y normativas, evaluar los riesgos considerando las propuestas establecidas y calcular la rentabilidad de dichas propuestas.

- En la etapa 6: construir un plan, como resultado de la transformación de las propuestas para la reducción de riesgos.

- En la etapa 7: planear la implantación del plan, y comparar lo planeado contra lo real, con la finalidad de detectar errores y establecer los cambios pertinentes.

Estas propuestas de adecuación a la metodología CIDETES, junto con lo establecido en el marco teórico, la han robustecido de la siguiente manera:

- Teóricamente a través de la IID, que aporta los elementos que permiten sentar las bases cognoscitivas para enmarcar los estudios relacionados con la evaluación de riesgos, y proporciona una visión holística de la problemática asociada a los eventos no deseados de seguridad;

- En la práctica, el enfoque de la planeación como un proceso básico en la conducción ha permitido incorporar los elementos de instrumentación y control en la estructura de la metodología, que hacen de ella un instrumento de apoyo importante para el sistema de control o conducente en la toma de decisiones relacionadas con el manejo de riesgos;

- El empleo del enfoque sistémico y cibernético, a través del proceso de conducción permiten la conceptualización de los sistemas involucrados (afectable, perturbador y de gestión) y redefinir el objeto de estudio de la metodología, dejando de centrarse sólo en elementos parciales de cada uno de ellos;

- En la caracterización del sistema afectable, la justificación sobre qué activos o elementos son críticos, con base en la definición de las funciones críticas, la infraestructura crítica, las posibles consecuencias y el valor del activo (económico, emblemático u operacional), así como el empleo de modelos lógicos (como los árboles de fallas), proporciona al estudio un sustento práctico importante.

- Otro aspecto que se fortaleció se refiere a la caracterización del sistema perturbador, ya que se establece una secuencia de pasos que permiten analizar de forma estructurada a las amenazas, lo que a su vez, permite también estimar la probabilidad de ocurrencia con una mayor asertividad, por otro lado, involucrar al experto en la definición de criterios, escalas y unidades de medición, garantiza un resultado con mayor fiabilidad.

- La caracterización del sistema de gestión es un aporte que permite entender de una mejor manera las fortalezas y debilidades que existen sobre el manejo y tratamiento sobre el sistema afectable, además de identificar los posibles canales de comunicación que faciliten la obtención de información para llevar a cabo la evaluación de riesgos.

- La evaluación del sistema de seguridad física enfocada en su eficiencia y en el impacto en la seguridad del sistema afectable, permite tener un conocimiento sustentado, acerca del grado de vulnerabilidad y por ende sobre el control del riesgo que puede existir en un momento determinado; la aportación que da un diagrama de secuencia de adversarios, es que permite identificar de una forma más clara las posibles vulnerabilidades que pueden ser aprovechadas para llegar a un elemento o activo.

- En general, sobre el aspecto de los criterios, escalas y unidades de medición para realizar la evaluación, el énfasis sobre la importancia de su definición como soporte al proceso de evaluación, permite evitar pérdidas de tiempo y certeza en el estudio.

- Los costos a considerar para la determinación de los impactos económicos, refuerzan los aspectos que se tienen que tomar en cuenta.

- La realización de un análisis sobre los impactos económicos causados por las fallas o deficiencias de los elementos del sistema de seguridad física, sin considerarlos como activos o elementos críticos, enfatiza la importancia del sistema de seguridad física.

- La construcción de escenarios para determinar las condiciones actuales del riesgo permite agrupar algunos pasos de la etapa 4 y analizar la vinculación amenaza-activo para cada paso, y no por cada paso analizar la relación amenaza-activo, lo cual originaba que entre una paso y otro, se perdieran elementos considerados para la misma relación amenaza-activo, o bien, se perdiera tiempo en retomarlos;

- La determinación de la condición normativa, futura y deseada del riesgo, representa un aporte que le proporciona un carácter proactivo a la metodología.

- La obtención de indicadores de riesgo permitirá realizar la comparación entre diferentes sistemas a los que se aplique la metodología.

- La realización de una evaluación del riesgo después de las propuestas y un cálculo sobre la rentabilidad de la inversión en el sistema de seguridad física, permite justificar las propuestas establecidas e incentivar a llevar a cabo la implantación de dichas propuestas.

Finalmente, sobre el alcance definido en la investigación se logró:

- Conceptualizar la metodología como instrumento de planeación en la evaluación del riesgo, al reestructurarla bajo el proceso de conducción e incorporar elementos de instrumentación y control, que permitirán proporcionar sustento al sub-sistema de toma de decisiones del sistema de gestión, al visualizar al sistema conducido, establecer un entendimiento de la problemática asociada al riesgo que identifica estados futuros de las condiciones asociadas al riesgo, proponer las posibles soluciones, transformar dichas soluciones en un plan que define objetivos de cambio, políticas, estrategias y las acciones más adecuadas para alcanzarlos, así como su respectivo control.

- Sustentar teóricamente a la metodología bajo un enfoque sistémico y cibernético, a través de la Investigación Interdisciplinaria de Desastre, puesto que al conceptualizar fenómenos asociados a eventos no deseados de seguridad por medio del proceso de conducción, le permite a la metodología, la construcción de los tres sistemas involucrados: el afectable, el perturbador y el de gestión

REFERENCIAS

American Petroleum Institute, National Petrochemical & Refiners Association. (2004). Security Vulnerability Assessment. Washington, D.C.: API Publishing Services.

Análisis de riesgos: El Método Mosler. (n.d.). Consultado el 5 de noviembre de 2010, página web http://www.forodeseguridad.com/artic/segcorp/7220.htm.

Benitez, R. (2009). La crisis de seguridad en México. Nueva Sociedad (220), 173-189.

Cháidez, A., & Rodriguez, G. (2010). Serie de investigación sobre seguridad nacional. Septiembre 2008 - Agosto 2009 . México: Colectivo de Análisis de la Seguridad con Democracia CASEDE.

Chanona, A. (2007). Hacia la redefinición de la seguridad nacional. Ponencia en el seminario internacional México: La seguridad nacional en la encrucijada. Colegio de México.

Comité Conjunto de Estándares Australia / Estándares de Nueva Zelanda OB-007 de Administración de Riesgos. (2004). Estándar Autraliano / Neo Zelandés. Administración de Riesgos.

Crece la industria de la seguridad privada. (2010). Seguridad en América (61), 72.

De la Barreda, L., & Sayeg , C. (n.d.). Análisis de la percepción de inseguridad ENSI-4/URBANA. México: Instituto Ciudadano de Estudios Sobre Inseguridad.

Facultad De Ingeniería. (2005). Centro de Investigación y Tecnología de Seguridad. Gaceta UNAM (3785), 3.

Fuentes, A. (1995). Un sistema de metodologías de planeación, Cuadernos de Planeación y Sistemas, División de Estudios de Posgrado. México, D.F.: Facultad de Ingeniería, UNAM.

García, M. (2001). The design and evaluation of physical protection systems. United States of America: Butterworth-Heinemann .

García, M. (2006). Vulnerability Assessment Of Physical Protection Systems. United States of America: Butterworth-Heinemann .

Gelman, O. (1996). Desastres y protección civil Fundamentos de Investigación Interdisciplinaria. México: Instituto de Ingeniería, UNAM

Hillson, D. (2009). El debate de la definición. Consultado el 15 de noviembre de 2010, página web risk-doctor: http://www.risk-doctor.com/pdf-briefings/risk-doctor52s.pdf

Instituto Ciudadano de Estudios Sobre Inseguridad ICESI. (n.d.). Cuadernos del ICESI 8. Victimización, incidencia y cifra negra en México, Análisis de la ENSI-6 . México

Instituto Ciudadano de Estudios Sobre Inseguridad ICESI. (2009). Sexta encuesta nacional sobre seguridad. ENSI-6 . México.

Instituto de Gestión de Proyectos. (2000). Guía Fundamental Para La Gestión de Proyectos. PMBOK GUIDE . Newton Square, Pennsylvania, United States Of America.

International Organization For Standarization. (2008). Risk management — Principles and guidelines on implementation.

México lidera armado de autos blindados en AL. (2010). Consultado el 06 de julio de 2010, página web El Universal.mx: http://www.eluniversal.com.mx/nacion/177956.html

México Unido Contra la Delincuencia. (2010). Encuesta Nacional Sobre la Percepción de Seguridad Ciudadana en México. México.

Poder Ejecutivo Federal. (2007). Plan Nacional de Desarrollo 2007-2012 . México.

Pulido, J. (2005). Gestión de riesgos. Consultado el 28 de noviembre de 2010, página web Instituto Nacional de Administración Pública, España: http://www.inap.map.es/NR/rdonlyres/4C9D956A-277C-405D-BA80-36CB6B92B7C4/0/PULIDO.pdf

Sánchez, G. (2003). Técnicas Participativas Para la Planeación, Procesos breves de intervención. México: Fundación ICA.

Sandia Corporation. (n.d.). A Risk Assessment Methodology (RAM) .

Vera, R. (2010). Un negociazo a prueba de balas. Consultado el 11 de septiembre de 2010, página web Proceso.com.mx: http://www.proceso.com.mx/rv/modHome/detalleExclusiva/81429