LA SEGURIDAD PRIVADA DESDE LA GESTION DEL RIESGO

ARTHUR EDGARDO ALVAREZ JIMENEZ

Especialización Administración de la Seguridad

Abril de 2012

UNIVERSIDAD MILITAR NUEVA GRANADA

Facultad De Relaciones Internacionales, Estrategia Y Seguridad

Especialización en administración de la seguridad

BOGOTÁ, D. C.

2012

Contenido

pág.

LISTA DE FIGURAS

pág.

Síntesis

Hacia el año 1993 con la ley 62 es creada la superintendencia de vigilancia y seguridad privada adscrita al ministerio de defensa Nacional, "le corresponde ejercer el control, inspección y vigilancia sobre la industria y los servicios de vigilancia y seguridad privada" [1] La industria de la Seguridad privada en Colombia represento en el año 2010 ingresos superiores a 4,6 Billones de Pesos, dentro de las cuales las empresas de vigilancia representan el 81,6% de las ventas, "Es decir que por cada 100 pesos vendidos las empresas de vigilancia venden 82 pesos" [2] con un margen operacional del 5.3%, Así mismo a lo largo de estos 19 años el sector ha evolucionado, al igual que la manera como se ha analizado la problemas en seguridad y los peligros a los que están expuestos tanto las empresas a nivel interno como los clientes de las mismas empresas, en lo cual la superintendencia de vigilancia con el objetivo de ejercer un control más detallado de los servicios que prestan las empresas de vigilancia y seguridad privada en el país, mejorar la calidad de los mismos, y ofrecer a los usuarios una metodología clara y directa sobre las reglas operativas que deben seguir este tipo de servicios, la SuperVigilancia viene implementando una serie de protocolos operativos unificados para cada uno de los subsectores dentro de los cuales ya se han publicado los protocolos para el sector financiero residencial y de vigilancia electrónica.

Es acá donde toma importancia la Jefatura o gerencia de operaciones de las empresas de vigilancia y su enfoque en la gestión del riesgo, no solo de los riesgos

---

[1] Superintendencia de Vigilancia y Seguridad Privada. ¿Quiénes somos? [en línea]. Noticias Destacadas. Recuperado de: http://www.supervigilancia.gov.co/index.php?idcategoria=1027&download=Y. Consultado en: Abril de 2012.

[2] Superintendencia de Vigilancia y Seguridad Privada. Recuperado de: http://www.supervigilancia.gov.co/?idcategoria=61645# Consultado en : Abril de 2012

físicos en los puestos de trabajo, sino en cada uno de los procesos ya que aunque las cifras son muy buenas, las empresas de seguridad en sus primeros años de operación reportan un alto índice de pérdidas y fallas en sus procesos desde la gestión gerencial hasta los procesos de mejora continua. Igualmente son muy pocas las pequeñas empresas que aportan valor a sus clientes en la prevención de pérdidas.

Introducción

Dentro de la presente guía se busca establecer las bases fundamentales para ejercer una correcta Gestión Gerencial en el área de operaciones de las empresas de vigilancia y seguridad privada, las cuales se deben enfocar en la gestión del riesgo tanto de los procesos internos de la empresa, como en los puesto de servicios de cada uno de los clientes de la empresa de vigilancia, , dejando claro que el alcance y el aporte a la organización de cada jefatura depende de un adecuado análisis de riesgos de cada proceso dentro de la empresa, las medidas aplicables para disminuir estos riesgos y el monitoreo constante para verificar la efectividad de estas medidas, así como los estudios de seguridad física que se hacen a cada uno de los clientes y el aporte en la prevención del delito y en la prevención de pérdidas.

Esta guía es aplicable a empresas de seguridad privada, y su desarrollo está fundamentado en la experiencia en el ejercicio del cargo, los fundamentos dados dentro de la especialización en administración de la seguridad en experiencias y buenas prácticas aplicadas por empresas que son líderes en el mercado de la seguridad privada y en libros y documentos que en la materia existen en la actualidad.

Conceptos Básicos

Dentro de los conceptos básicos que debe poseer un profesional de seguridad está el de saber claramente que un programa de seguridad física es aquel que se debe tener dentro de la empresa y está compuesto por lo siguiente: Elementos de detección, elementos de retardo y elementos de respuesta.

Como ejemplo las cámaras y los sensores son elementos de detección, las mallas, las barreras naturales y artificiales se denominan elementos de retardo, y los elementos de respuesta son los vigilantes, o personal humano, la fuerza pública, los Caninos, y los procedimientos o protocolos, siendo importante resaltar que se llama barrera positiva a los seres humanos que son los únicos que poseen la cualidad de detectar, retardar y responder, los elementos tecnológicos como los sensores poseen mayor capacidad de detección que un ser humano, sin embargo los seres humanos poseen la capacidad de responder, por lo que el profesional de seguridad debe saber no solo saber ubicar y coordinar los tres elementos sino administrar los recursos y realizar un seguimiento adecuado para tener un programa de seguridad que sea efectivo y que además sea costo beneficioso.

En esta guía se plantea y se resaltara la importancia tener claridad en los diferentes términos que se expondrán a continuación siendo el primero el tipo de seguridad que poseen una gran cantidad de empresas que a pesar de tener una de compañías de seguridad, la misma no es la más ideal, ya que solamente se presta el servicio como factor disuasivo más como un aliado estratégico para la prevención de pérdidas.

"FRAGMENTADA: Agregando ingredientes sin un programa coherente, es decir bajo el criterio errado que más cámaras, más sensores, más vigilantes es más seguridad, pero sin una coherencia entre ellos.

REACTIVA: Respondiendo únicamente a los siniestros, solamente cada vez que sucede alguna perdida implementamos alguna medida.

UNIDIMENSIONAL: Basada en una sola medida, ejemplo: solo seguros o solo vigilante.

EMPAQUETADA: Instalando sistemas de seguridad porque fue el paquete que me ofreció la compañía de seguridad y es lo que todos comúnmente hacen.

INTEGRAL: Basada en el análisis de riesgos y evaluación de vulnerabilidades, con cobertura sobre todos los aspectos de la empresa."[3]

Que es la seguridad Física

Es el Sistema de contramedidas tangibles, especialmente diseñadas para proteger de amenazas previamente identificadas, los activos físicos, operacionales y por ende la vida de las personas en una organización.

Bajo este criterio es importante tener en cuenta que los objetivos de la seguridad física son controlar el acceso, prevenir la interrupción de las operaciones, y en caso que ocurriera tener un plan de continuidad del negocio, y reducir el miedo al crimen, ya que es importante trabajar en ambiente seguros.

Programa de Seguridad Física

El programa de seguridad Física debe tener Políticas y procedimientos es decir los objetivos de seguridad a mediano y largo plazo, como por ejemplo la reducción de pérdidas en un determinado porcentaje, personas capacitadas para monitorear,

[3] Seminario Gerencia de Seguridad Avanzada. Tomo 2. ANDROSS.

administrar e implementar el sistema, Barreras o dispositivos de control de acceso, equipo de detección, y alarmas y comunicaciones.

Registros: Reporte de Incidentes pasados, y tener en cuenta que quien no conoce la Historia está condenado a repetirla, pues es muy importante aprender de los errores de los demás o de los nuestros, pero que los mismos no se vuelvan a cometer.

El modelo denominado Protection IN-Depth Model plantea que una adecuada protección en profundidad consta de dos tiempos los cuales son Tiempo de Demora y Tiempo de respuesta, y estos a su vez contienen los tres componentes que son detección, retardo y respuesta. (Es importante aclarar que llamamos barrera positiva a la que es capaz de cumplir con estos últimos tres ítem, y el único capaz de cumplir este objetivo es el hombre).

Cuando se diseñe un programa de seguridad no se debe profundizar no solo en las restricciones, denegaciones y limitaciones, sino que se debe generar un buen ambiente de trabajo, para que las personas no solo se sientan seguras sino que realmente lo estén, para una seguridad física sea valiosa y sirva para reducir el miedo al crimen debe ser medible y no solamente generar ilusiones o falsa seguridad.

Las contramedidas deben estar acordes al entorno, adoptadas bajo medidas reales dentro de las cuales las que más aportan para reducir el miedo al crimen son la iluminación, control de parqueaderos, mallas, CCTV, alarmas.

El Estudio de Seguridad

El primer paso de un estudio de seguridad es el análisis de los riesgos. Una vez las metas y las responsabilidades han sido definidas y una organización ha sido creada para sacarlas adelante, el deber inmediato de la gerencia de seguridad es identificar áreas de pérdidas potenciales y desarrollar e instalar medidas apropiadas de seguridad. Este proceso de estudio de seguridad es llamado análisis de riesgo.

Incluido en este acercamiento está el concepto de seguridad como una función completa e integrada de la organización. Una parte de este trabajo es el estudio de la seguridad física para identificar áreas de problemas potenciales y vulnerabilidades.

Esta vista completa de la función de prevención de pérdidas se contrapone a algunas costumbres de. Mirar la seguridad como puntos parciales y aislados, tales como:

Seguridad según el análisis de un solo riesgo, como por ejemplo el riesgo de intrusión.

Seguridad fragmentada; en donde vamos avanzando según las necesidades.

Seguridad reactiva, que solo se toman medidas cuando se presenta algún evento, pero sin tener en cuenta el análisis de riesgos.

Administración de Riesgos

El primer paso en el análisis de los riesgos es el estudio de la amenaza. Un sistema integral de seguridad es una operación de alto costo, pero, comparado con invertir dinero en investigaciones y en el desarrollo de la empresa, que es invertir en el futuro de la empresa, invertir en la prevención de las pérdidas es solamente gastar dinero en prevenir algo inevitable. Aunque las dos inversiones presentan riesgos, gastar el dinero en un producto es dinámico y especulativo y esto es un riesgo más interesante. Los riesgos a la propiedad son generalmente vigilados o considerados un mal necesario. Aún cuando el riesgo es identificado, los gerentes prefieren operar bajo la teoría del riesgo calculado. Los riesgos recientes, particularmente provenientes del terrorismo, y han obligado a las empresas a asumir actitudes proactivas frente a su seguridad. Las dos posibles soluciones, que realmente deberían ser complementarias, son (1) invertir en prevención de pérdidas y (2) tomar un seguro.

Un programa de administración de riesgos comprende los siguientes cuatro pasos básicos:

Identificación de riesgos o vulnerabilidades particulares y específicas

Análisis de los riesgos, que incluye la probabilidad e impacto de un evento

Optimizar las alternativas de la administración de riesgos las cuales pueden ser:

Evitar, que es tomar medidas necesarias para que no ocurra, como por ejemplo no mover carga en carretera después de las 6:00 pm.

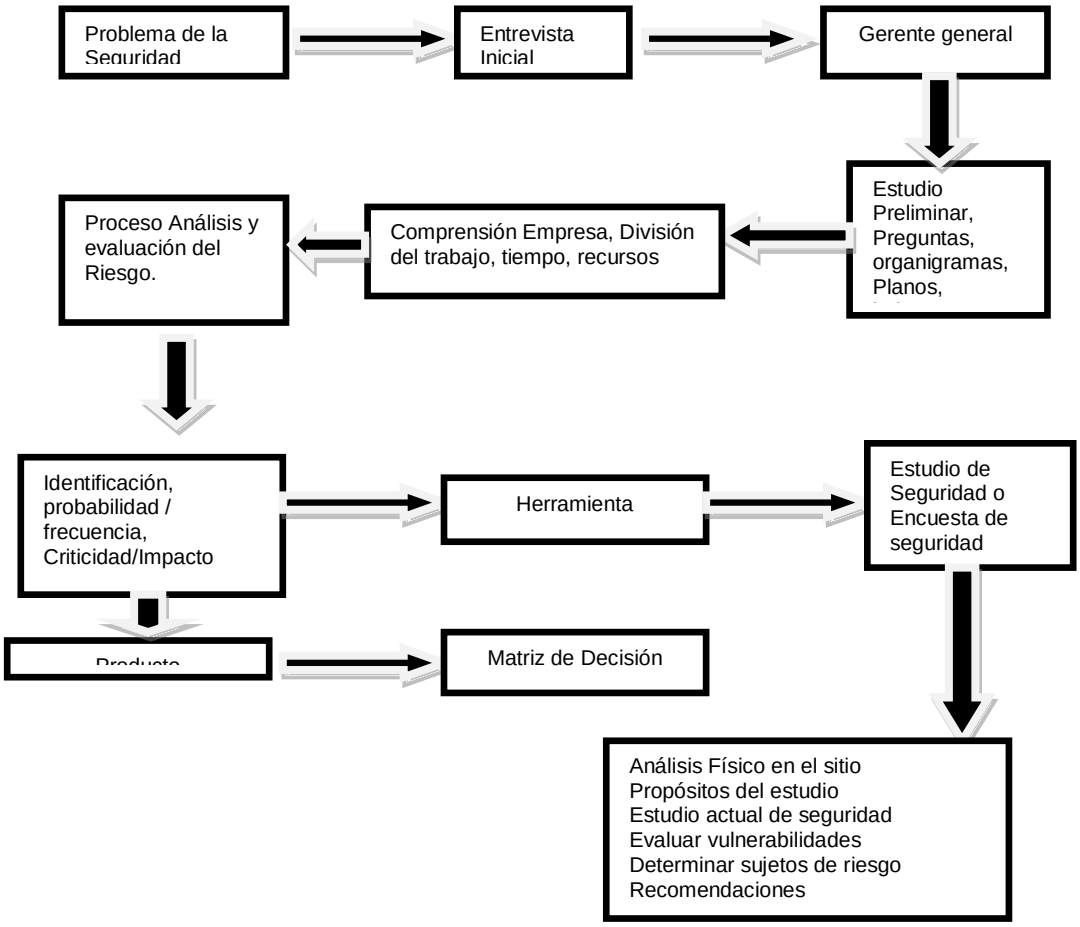
Reducir, tomando medidas que en caso de ocurrencia el impacto sea menor, por ejemplo cuando se transporte carga, haciendo parada únicamente en sitios que ofrezcan seguridad.

Distribuir: Como por ejemplo llevando la carga en varios camiones, o en distintos tipos de transporte, o lo que comúnmente hacen las familias árabes, que cuando viajan los dos miembros más importantes de la familia lo hacen en distintos vuelos.

Transferir: Como por ejemplo mediante pólizas de seguros.

Asumir: que en caso de ocurrencia asumo las consecuencias del riesgo, o la combinación de todas las anteriores.

Proceso General de la Seguridad



Gráfica 1. Mapa del estudio de seguridad. Fuente: Ingeniero Arthur Edgardo Álvarez Jiménez. Autor del presente proyecto. 2012.

Ejemplo: En una empresa de lácteos la maquina más importante es la maquina Pasteurizadora, que tan probable es que la puedan sabotear.

Estructura de la Gerencia de Riesgos

Gráfica 2. Estructura de la Gerencia de Riesgos. *Fuente: Ingeniero Arthur Edgardo Álvarez Jiménez. Autor del presente proyecto. 2012*

Conceptualización Básica y normatividad legal en Seguridad privada

El gerente de Seguridad debe tener claro la normatividad legal vigente, para el caso de Colombia los decretos 356 de 1994 y decreto 2535 de 1993 y sus modificaciones incluida la ley 019 de Enero de 2012, sin embargo se debe hacer una reflexión acerca si verdaderamente se aplica lo contenido en la norma, y cuál es la responsabilidad y el alcance de la jefatura de operaciones frente a estas normas, y de igual manera se debe tener claridad frente a los proyectos de ley que se encuentran actualmente en el Congreso y su impacto a las pequeñas y medianas empresas del sector de la seguridad privada.

Igualmente la gerencia de operaciones debe estar en capacidad de determinar la diferencia entre peligro, amenaza, y riesgo, y que es vulnerabilidad, que son conceptos totalmente distintos y que tienden a ser confundidos, a manera de ejemplo en una corraleja la amenaza es el Toro, el peligro es que el toro me realice una cornada, y el riesgo es el de una lesión hasta la muerte por ingresar a la corraleja. Por otro lado el gerente de operaciones debe tener clara la ecuación del riesgo la cual está determinada por el producto entre amenaza y vulnerabilidad, y la norma 5254 de gestión del riesgo.

Dentro del proceso de conceptualización la gerencia de operaciones debe saber determinar los diferentes tipos de sistemas de gestión, y para qué sirven y el valor agregado que aportan a la organización.

Sin importar con cual sistema cuente la empresa se deben tener en cuenta los siguientes los cuales están asociados a la gestión del riesgo: HSSEQ, Health (Salud). Prevenir enfermedades profesionales, Safety (Seguridad), Prevenir accidentes. Security (Protección), Proteger y prevenir perdidas. Environment (Medio ambiente). Mitigar el impacto ambiental. Quality (Calidad), Satisfacción del cliente.

Analisis de Riesgos por procesos dentro de las empresas de seguridad

Dentro del análisis de riesgos a los proceso de la organización se debe determinar en primer lugar cuales son los procesos más comunes dentro de la empresa, y afines al objeto social que se desarrolla, dentro de los cuales se analizaran en profundidad los siguientes procesos: Estratégicos, operativos y de apoyo, dentro de los procesos estratégicos se deben analizar el proceso de Gestión gerencial y planificación estratégica de los sistemas de gestión, dentro de los procesos Operativos se deben analizar los procesos de gestión de relaciones con el cliente, y el proceso de gestión de operaciones, y dentro de los procesos de apoyo se debe analizar el proceso de gestión de talento humano, todos bajo el enfoque y análisis de los riesgos de cada uno.

La identificación del riesgo se puede desglosar por partes así: Amenaza. Que es la identificación de los factores a los cuales se encuentra expuesta la organización, y se debe hacer una descripción o listado global de eventos, es decir el cómo podría materializarse la amenaza dentro de la organización, bajo hechos potenciales o reales. La modalidad, que se refiere al modus operandi que los grupos delincuenciales podrían utilizar para cometer sus actos ilícitos o la manera que pueden actuar aquellas personas que tiene algún tipo de inconformismo con la empresa. Los controles existentes, que son los diferentes controles operacionales dispuestos por la empresa para minimizar la posibilidad de ocurrencia de eventos que afecten la seguridad de la misma, se debe hacer un análisis DOFA de estos controles.

El análisis del riesgo puede ser analizado desde el punto de vista de la probabilidad y la consecuencia, siendo la probabilidad la posibilidad de que ocurra un evento o resultado específico, medido cualitativa y cuantitativamente por la relación entre los eventos o resultados específicos y el número total de eventos o resultados posibles. Esta depende en

gran medida de la eficacia de los controles internos en los procesos. Dentro de éste concepto se manejan cinco tipos de probabilidades, a las cuales dependiendo de cada organización y sus políticas internas se le designaran valores de medida, en el nivel 1 Raro es que puede ocurrir solamente en circunstancias excepcionales, nivel 2 improbable, que ha ocurrido muy pocas veces, podría ser una vez cada cinco años, nivel 3 posible, que ha ocurrido pocas veces, podría ser dos o tres veces en los últimos cinco años, nivel cuatro probable, que puede ocurrir probablemente varias veces en el año, y nivel 5 casi cierto, que se espera que ocurra varias veces durante el año.

Y la consecuencia que es el resultado de un evento expresado cualitativa o cuantitativamente, como por ejemplo una pérdida, lesión, desventaja o ganancia, puede haber una serie de resultados posibles asociados con un evento., a los cuales a manera de ejemplo se dieron los siguientes valores de medida, nivel 1 insignificante, las consecuencias no afectan de ninguna forma a la empresa. Las pérdidas o daños no son significativos, nivel 2 menor, las consecuencias afectan levemente el funcionamiento de la empresa, pérdidas y daños pequeños con relación a la capacidad económica de ésta, nivel 3 moderada, las consecuencias afectan de manera parcial el funcionamiento de la empresa, pérdidas y daños medianos con relación a la capacidad económica de ésta, nivel 4 mayor, las consecuencias afectan de manera total la imagen, el funcionamiento de la empresa en forma temporal, pero no de una manera irrecuperable, pérdidas y daños mayores, nivel 5 catastrófica, las consecuencias afectan totalmente a la empresa generando daños irrecuperables.

Dentro del proceso de gestión de relaciones con el cliente se puede tomar como un ejemplo de riesgo, la pérdida de clientes, dentro de las amenazas posiblemente detectables están una mala atención a las quejas y reclamos, la no existencia de un

protocolo de servicio al cliente, y el mal servicio prestado por el personal asignado al servicio, entre otros.

Para la evaluación del riesgo se puede hacer la siguiente clasificación: Aceptable, quiere decir que la consecuencia no implica una gravedad significativa, por lo que no amerita la inversión de recursos generalmente y no requiere acciones adicionales para la gestión sobre el factor de vulnerabilidad considerado, diferentes a las ya aplicadas en el escenario. Sin embargo deben seguir monitoreándose para garantizar que siguen siendo aceptables, Tolerable, significa que, aunque deben desarrollarse actividades para la gestión sobre el riesgo, pudiendo ser a mediano plazo, generalmente amerita la inversión de recursos, Inaceptable, se requiere siempre desarrollar acciones prioritarias a corto plazo para su gestión, debido al alto impacto que tendrían sobre la empresa, requiere la inversión de recursos.

Dentro de los riesgos fácilmente identificables se tienen los siguientes: para el proceso de Gestión del talento Humano, la amenaza es el personal deshonesto, otra amenaza es el personal que aunque tenga las certificaciones no tienen las aptitudes para el cargo, la descripción para el primero sería la materialización de hurtos internos con complicidad del personal de seguridad, que son detectados cuando los mismos son en gran cuantía o se vuelven continuos, inclusive muchas compañías ni si quiera tienen un valor estimado de las mermas, y otras inclusive duran años con robos continuados sin que los mismos sean detectados, la descripción para el segundo podría ser la contaminación de la carga por un inadecuado control o perdida de bienes o información por la intrusión de personal no autorizado, las modalidades utilizadas podrían ser por falsedad en documentos, complicidad interna, confabulación, y la segunda porque existe una realidad en el mercado que la venta de diplomas en seguridad privada, y que es frecuente inclusive

en algunos casos bajo el aval de las mismas gerencias, con el concepto que las academias siempre dictan lo mismo.

Dentro del estudio de seguridad y la gestión de la gerencia de operaciones se debe hacer un DOFA de los controles existentes, esto sería un primer paso para ir determinando las posibles contramedidas para disminuir la probabilidad y las consecuencias del riesgo.

Para el proceso de gestión de operaciones, una amenaza es la delincuencia común, la descripción es la perdida de bienes bajo cuidado y custodia, y la reputación de la compañía de Seguridad si el hecho reviste trascendencia o es de público conocimiento, las modalidades utilizadas van desde la misma complicidad interna, la intrusión, suplantación de autoridad, suplantación del mismo personal de seguridad, materialización de los descuidos del personal de seguridad por parte de la misma delincuencia, así como la falta de un programa integral de seguridad física, al igual para estos riesgos debemos hacer el mismo análisis DOFA de los controles existentes, un análisis de vulnerabilidades y efectividad de las medidas existentes.

Hasta este punto solamente se ha expuesto una buena práctica para la identificación de los riesgos, pero es la experiencia y las experiencia de las misma compañías de seguridad las que pueden ayudar a determinar y analizar casos reales (Casuística).

Ahora se pasa al punto de analizar los riesgos, que es como se mencionó anteriormente, que es darle valor cualitativo y cuantitativo a la probabilidad y las consecuencias, con el ánimo de establecer la aceptabilidad de los mismos.

Esta zona de aceptabilidad seria de 1 a 4 aceptable, de 5 a 12 tolerable, y de 15 a 25 inaceptable. Se pondrá como ejemplo para este caso: El caso del personal deshonesto, es importante tener en cuenta las estadísticas y los hechos en que se presume con una

alta probabilidad que hubo deshonestidad, se podría evaluar porcentualmente y la relación de perdidas versus valor en ventas, esto con el ánimo de determinar el impacto en la empresa, y para la valoración de las consecuencias, como ha impactado estos hechos, de esto podemos sacar varias conclusiones y buenas practicas que se deben aplicar en las empresas de seguridad por parte de los jefes de operaciones, como lo es el llevar un registro detallado de estos hechos, en caso que se lleve analizar las mejoras, y en caso que no se lleve que se reconstruya con base en los informes, y que se asuma esto como función dentro de las jefaturas.

Para el tratamiento del riesgo se pueden realizar varias actividades las cuales son derivadas de la identificación y el análisis del riesgo, las cuales pueden ser: 1) No afrontar el riesgo, al no proceder con la actividad que tiene posibilidad de generar riesgo siempre que sea aplicable. 2) reducir la probabilidad de la ocurrencia, tomando acciones tales como: inspección y procesos de control, mantenimiento preventivo, procesos adecuados de selección, formación estructurada y técnicas de control. 3). Reducir las consecuencias tomando acciones tales como: Planes de contingencia, separación o reubicación de una actividad y recursos, reducción de la exposición a fuentes de riesgo. 4) Transferir el Riesgo, a través de la participación de otras partes, por ejemplo con pólizas de seguros. 5) Retener el riesgo, después de haber reducido o transferido los riesgos, puede haber riesgos residuales que se deben retener, los riesgos también se pueden asumir cuando las contramedidas son más costosas que el impacto que me puede generar la materialización del riesgo, por ejemplo cuando las mermas en un almacén son en una proporción muy mínima.

Téngase en cuenta que los anteriores riesgos descritos fueron analizados individualmente, sin embargo se debe indicar que las medidas aplicables pueden disminuir

el nivel en todos los riesgos analizados con anterioridad, por lo que es aplicable que una sola medida bien aplicada puede ayudar con la disminución del riesgo o sus posibles consecuencias.

Para una adecuada gestión del riesgo se debe hacer una lista de riesgos y hacer un análisis en profundidad de cada uno de ellos, utilizando como buena práctica los mismos parámetros de los riesgos anteriormente analizados, y que para mayor detalle se resume en la tabla anexa denominada matriz de análisis y tratamiento del riesgo.

Prevención de Perdidas

Tal como lo señala el decreto 356 en su artículo 73 "La finalidad de los servicios de vigilancia y seguridad privada, en cualquiera de sus modalidades, es la de disminuir y prevenir las amanezcas que afecten o puedan afectar la vida, la integridad personal o el tranquilo ejercicio de legítimos derechos sobre los bienes de las personas que reciben su protección, sin alterar o perturbar las condiciones para el ejercicio de los derechos y libertades públicas de la ciudadanía y sin invadir la órbita de competencia reservada a las autoridades."[4]

Es en la prevención de estas amenazas donde la gerencia de operaciones juega un papel determinante, ya que de la efectividad de las recomendaciones que surjan de un adecuado estudio de seguridad y del análisis de los riesgos tanto a los procesos como a los clientes de la empresa depende en gran parte el crecimiento de una organización al aportar valor a los clientes.

Los sistemas de Gestión y controles en seguridad

Más que implementar sistemas de gestión, argumentando que es la tendencia del mercado, se debe entender el aporte y el valor agregado que cada sistema a aporta a mi proceso y a mi organización, anterior a la ley 1150 de 2007 que elimino el requisito de

[4] Artículo 73, decreto 356 de 1994. Estatuto de Vigilancia y Seguridad Privada.

exigir los sistemas de gestión como requisito o factor de puntaje en los procesos de contratación con el estado, muchas compañía veían este sistema como un mero requisito, sin embargo después de esta ley la tendencia en la implementación se hace de manera más concienzuda.

Existen sistemas de gestión como el que se implementa bajo la norma ISO 9001-2008, sistemas de gestión en control y seguridad como BASC, sistemas de protección al medio ambiente, o sistemas tales como RUC, que se enfocan en la prevención de enfermedades y accidentes profesiones, por lo tanto dentro del seminario el alumno recibirá los conceptos de cada sistema, conocerá su impacto en el mercado y en caso de no tener ninguno de ellos implementados en la empresa, podrá definir por cuál de todos estos sistemas puede comenzar.

Detección, Retardo y Respuesta

Como ejemplos de detección están los sensores, las cámaras de CCTV, las barreras fotoeléctricas, Ejemplos de Retardo están las barreras perimétricas, los muros, las cercas eléctricas, y la concertina, la respuesta es el equipo de seguridad, es decir los vigilantes, y los protocolos establecidos.

El programa de seguridad PPT.

El programa de seguridad Física está compuesto por 3 componentes, tecnología, Personas y procedimientos, y unos componentes adicionales que cuando fallan los tres anteriores se denominan emergencias, manejo de crisis e investigaciones.

El gerente de operaciones debe estar en capacidad de realizar un programa de seguridad para una instalación en específico y plantear soluciones y mejoras a los sistemas en seguridad existentes.

EJEMPLO MATRIZ DE RIESGO

IDENTIFICACIÓN DEL RIESGO			
AMENAZA	**DESCRIPCIÓN**	**MODALIDAD**	**CONTROLES EXISTENTES**
Personal con antecedentes que pretenda ingresar a la organización para cometer actos ilícitos	Mediante la falsificación de los documentos que acreditan la identidad y los antecedentes judiciales. Lo cual podría generar **pérdidas económicas o de bienes a la compañía o a los clientes**	Falsificación de documentos, y suplantación de identidad.	>Verificación de antecedentes ante la procuraduría, >Verificación de la autenticidad del Documentos de antecedentes Judiciales.

ANÁLISIS DEL RIESGO						
PROBABILIDAD			CONSECUENCIAS			RIESGO
CUALITATIVA	DESCRIPCIÓN	CUANTITATIVA	CUALITATIVA	DESCRIPCIÓN	CUANTITATIVA	
POSIBLE	En la actualidad no existe un soporte del registro, sin embargo se ha presentado un caso en Noviembre de 2010. Se deja como accion de mejora dejar el registro del personal que presenta proceso de selección	3	MAYOR	En caso de llegarse a presentar y no fuera detectado la consecuencia seria Mayor ya que la persona muy probaqblemente vendria a cometer un ilicito cuyo monto podria superar los $ 30.000.000=	4	12

PLAN DE TRATAMIENTO DEL RIESGO										
AMENAZA	OBJETIVOS	META	INDICADOR	ACCIONES DE CONTROL	RESPONSABLES	FECHA	Después de acciones tomadas			
							prob.	Cons	RIESGO	% Reducción
Personal con antecedentes que pretenda ingresar a la organización para cometer actos ilícitos	Evitar que personal con antecedentes Judiciales o Disciplinarios ingrese a la compañía	Que no ingrese ninguna persona con antecedentes Judiciales o Disciplinarios ingrese a la compañía. (REDUCIR LA PROBABILIDAD DE OCURRENCIA)	INFORMACION SUMINISTRADA POR TALENTO HUMANO. Verificar con Ing. Hector Dario	* Adicionalmente a las medidas de control ya establecidas se debe realizar la verificacion de antecedentes a traves de el FRENTE DE SEGURIDAD EMPRESARIAL DE LA DIJIN de todo el personal aspirante a algun cargo en la compañía, atendiendo las recomendación emanadas de esta entidad.	DEL PROCESO., DRA. ERIKA JOHANA PEREZ, JEFE DE TALENTO HUMANO ANSE LTDA. DE LA AFILIACION: ARTHUR EDGARDO LVAREZ GERENTE DE RIESGOS	SEPTIEMBRE DE 2011	1	4	4	67%

Protección a personas (VIP)

Existen dos amenazas evidentes dentro de la protección a personas, el terrorismo y el secuestro, los cuales han llamado la atención de las empresas con el fin de prevenir situaciones extorsivas que pueden tener altos costos en dinero, imagen y producción, bandas de crimen organizado alrededor del mundo buscan alianzas con grupos terroristas para obtener objetivos políticos o económicos.

Esta situación obliga a mejorar día a día las técnicas y tácticas utilizadas para elaborar planes de seguridad para reducir las probabilidades de que las personas sean víctimas de la extorsión el secuestro o del terrorismo, sin embargo de manera independiente de las medidas que estas personas reciban un gran porcentaje de su seguridad depende de sus propias acciones, conductas y cultura de seguridad que posea.

La mayoría de las personas que han sido secuestradas no habían aceptado recibir un esquema de protección por tener la creencia que con esto se invade su privacidad y representan un cambio en su estilo de vida y el de su familia, además de los costos económicos, sin embargo en países como Colombia esto ha venido influyendo en un cambio de actitud en este sentido.

Un programa de protección personal requiere los siguientes pasos:

- Identificar la amenaza específica, se debe incluir probabilidad de secuestro y asesinato.
- Deben aplicarse medidas razonables de seguridad en el sitio de trabajo de la posible víctima.
- Debe considerarse la protección en la residencia.
- Procedimientos y cultura de seguridad para los viajes dentro y fuera del País.

Igualmente se deben hacer listas de chequeo de vulnerabilidades, listas de chequeo para desplazamientos, seguridad en caso de Emergencia, Seguridad en la información, Seguridad en la oficina, Seguridad en la residencia, Seguridad en sitios de reunión y en análisis de implementar el bajo perfil en ambiente hostil.

Planeación de Emergencias

La planeación de emergencias tiene tres objetivos principales:

- Protección de la vida de las personas
- Protección de la propiedad en general
- Restauración de las actividades y operación

El sistema de administración de emergencias o aplicación de la respuesta a esta emergencia, debe tener enfoque táctico orientado a la respuesta, una estrategia de desarrollo orientada a la respuesta, se mantiene en una esfera de acción limitada, e incluye la manera de abordar el mantenimiento de la operación.

El propósito de la planeación:

- Anticipar problemas
- Proveer planes de acción
- Reanudar el funcionamiento normal

Consideraciones del plan:

- Requiere tiempo de preparación.
- Debe ser escrito
- Definir responsabilidades y acciones
- Debe ser simple

Para el desarrollo de un completo proceso de planeación y administración de emergencias. Inicialmente se desarrollan unos objetivos primarios, como son: El diseño de una política general de emergencias, se determinan los riesgos frente a cada peligro (incendió, bomba, secuestro, explosión, desastre natural), se desarrolla la estructura de la organización de emergencias.

Conclusiones

Esta guía desde la perspectiva de la gestión del riesgo contribuye de manera efectiva con la labor del día a día de su trabajo, ya sirve para adquirir la habilidad para identificar los riesgos críticos para los clientes y para la misma organización, y para evaluarlos y darles el tratamiento efectivo y costo beneficioso, lo cual trae como aporte la mejora continua.

Se da claridad en la diferencia entre estudio de seguridad, programa de seguridad y planes de protección, y en qué momento se debe aplicar cada uno.

El gerente de riesgos debe conocer cuál es la aplicación de cada uno de los sistemas de gestión aplicables a las empresas de seguridad y como contribuye cada uno en beneficio de la empresa, y las nociones básicas para integrar sistemas de gestión de calidad.

Con esta guía el gerente de riesgos aclara los conocimientos básicos en cuanto seguridad privada según estándares internacionales y que muy seguramente aportaran con sus nociones en seguridad privada.

Referencias

Broder, J.; Butterworth–Heinneman. (1998). *Risk Analisis & Security Survey*.

Pedraza, G. (2002). *El proceso General de la gerencia de seguridad. Cero Incidentes*. Bogotá.

Bibliografía

Material academia Andross. Tomo I, II y III para la preparación del examen CPP.

Material de ASIS INTERNACIONAL para la preparación del examen CPP.

Cardona Rey, P. Dirección Por misiones Pablo Cardona Rey

Vallejo Rosero, S. (2005). *Manual del estudio de Seguridad*. p. 168

Guía Colombiana de la Seguridad Privada. (2006). Primera y Segunda edición.

Material y ayudas técnicas entregadas dentro de la especialización en la Administración de la seguridad.