Capítulo 6

La gestión de riesgos de seguridad empresarial

Julián Andrés Puentes Becerra*

* Magíster en Seguridad y Defensa Nacional, especialista en Administración de la Seguridad, profesional en Ciencias Militares, certificado CPP y PSPS por ASIS International. Docente e Investigador Grupo de investigación GISIC. Correo electrónico: julian.puentes@epfac.edu.co

CÓMO CITAR

Puentes Becerra, J. A. (2020). La gestión de riesgos de seguridad empresarial. En Y. Rico, D. López Cortés, & A. Cerón R. (comps.), *Enfoques y gestión en Seguridad Integral* (pp. 161-185). Escuela de Postgrados de la Fuerza Aérea Colombiana. https://doi.org/10.8667/9789585996199.06

Colección Ciencia y Poder Aéreo N.º 16
ENFOQUES Y GESTIÓN EN SEGURIDAD INTEGRAL

CAPÍTULO 6.
La gestión de riesgos de seguridad empresarial

https://doi.org/10.8667/9789585996199.06
Bogotá, Colombia
Noviembre, 2020

RESUMEN

El trabajo del gerente es crear un entorno laboral que fomente la realización de actos por parte de otros, en busca del cumplimiento de metas tanto personales como de la compañía. Los gerentes deben ser capaces de inspirar, motivar, y dirigir el trabajo de los demás. En ese sentido, la gestión de riesgos de seguridad empresarial aborda todos los aspectos de seguridad en la organización, contribuyendo a la continuidad del negocio mediante la implementación de indicadores clave de desempeño para justificar económicamente los programas de seguridad. Esto evidencia que cada contramedida implementada tiene un impacto positivo en la reducción del riesgo puro. Sin embargo, la seguridad corporativa ha sido asumida por personas que han aprendido empíricamente. Su experiencia vinculada a las organizaciones de seguridad del Estado les ha dado más que un fino sentido común, un criterio para determinar cuándo algunas situaciones podrían considerarse dañinas para la organización. Aun así, este saber empírico ha llevado a algunos responsables de la seguridad a aprender a partir de los errores, que al final resultan en pérdidas considerables para la organización, pérdidas que no solo afectan activos físicos, sino también activos operacionales e intangibles.

La gestión de riesgos en la seguridad empresarial es un asunto serio y estratégico. Debe ser asumida como tal por profesionales que hayan demostrado sus competencias a través de la formación en el campo específico de la seguridad corporativa, en los riesgos que tienen el potencial de afectar la continuidad del negocio, en certificaciones internacionales que refieran buenas prácticas y en experiencia acumulada en roles como tomador de decisiones. De esta manera, se hace relevante describir el rol de la labor de gestión de riesgos de la seguridad empresarial, desde la función del responsable de seguridad como gestor de los programas de seguridad, consultor de alta gerencia y miembro del comité directivo de la organización, sin abandonar su participación activa en los comités o redes de profesionales.

PALABRAS CLAVE

Gestión de recursos; prevención de riesgos; procesamiento de la información, seguridad industrial; supervisión.

Introducción

Desde la investigación descriptiva aplicada a este caso de análisis, se abordó la realidad de situaciones, eventos, personas, grupos o comunidades que utilizan la gestión de riesgos para administrar programas de seguridad. Se revisaron diversos referentes y modelos de seguridad en los que se ha aplicado este tipo de metodología, para descubrir cómo las organizaciones se han podido beneficiar. Así mismo, se investigó sobre cómo esta aplicación se convierte en el mejor insumo para la creación de un cuadro de control, que muestra resultados a manera de indicadores clave de desempeño para los profesionales de seguridad, especialmente cuando la práctica de la gestión de riesgos de seguridad empresarial crea asociaciones entre la seguridad y aquellos que poseen activos en riesgo, considerando todos los dominios de riesgo de seguridad de manera integral (ASIS International, 2019). Lo anterior, entendiendo que la gestión de seguridad corporativa no es una tarea que se realiza al margen de las organizaciones, o del espíritu de las mismas. Es necesario acudir a referentes documentados sobre la gestión de organizaciones, gestión de la seguridad y gestión corporativa para encontrar el balance perfecto y los puntos de convergencia, para que la gestión de riesgos de seguridad empresarial tome un valor relevante. El mundo actual está lleno de incertidumbre, es un mundo que cambia a un ritmo cada vez más acelerado, en el cual la vida, la sociedad, la economía, los patrones climáticos, las relaciones internacionales y los riesgos son cada vez más complejos (Talbot & Jakeman, 2009).

Las iniciativas frente a la gestión de riesgos no son nuevas. Existen antecedentes formales y documentados como el Committee of Sponsoring Organizations of the Treadway (COSO), COSO I de 1992 y el Estándar Australiano de Administración de Riesgos, AS/NZS 4360:1999, que Colombia adoptó bajo el nombre de Norma Técnica Colombiana

NTC-5254:2006. Más adelante, se desarrolló una segunda generación de COSO II del 2004, COSO III del 2013 y la norma ISO 31000:2009 (Risk management o Gestión de riesgos), que en la actualidad cuenta con una segunda versión, ISO 31000:2018. Debido a la importancia que cada organización le ha venido dando a la gestión de riesgos, su impronta se ha hecho un motivo de estudio e investigación, hasta el punto de considerar hoy una tercera generación, COSO Enterprise Risk Management (ERM) 2017 y Enterprise Security Risk Management de ASIS International 2018. Ese mismo motivo ha promovido en Colombia la creación de programas de formación a nivel de pregrado y posgrado, que buscan mejorar las competencias de los profesionales de todas las áreas, que hoy en día desarrollan su actividad en el complejo sector de la seguridad.

En tal sentido, este capítulo pretende ser una guía que permita alinear todos los conocimientos adquiridos en una sola dirección, además de servir de consulta en el desarrollo de la actividad profesional. Con un enfoque basado en riesgos, los responsables de la seguridad corporativa podrán establecer las situaciones de alta probabilidad y de alto impacto para ser gestionadas desde los programas de prevención que incluyen, la seguridad física, la seguridad del personal, la seguridad de la información la seguridad de las operaciones y la seguridad reputacional; también programas de control como manejo de crisis, y programas de recuperación como investigaciones y administración de seguros.

Enfoque basado en riesgos[1]

La última década se ha destacado por cambiar el enfoque respecto a cómo los profesionales abordan los problemas de seguridad. De hecho,

1 Un enfoque basado en riesgos es descrito por la International Standarization Organization (ISO, 2014).

es común relacionar el concepto de gestión de riesgos en aplicaciones de seguridad. Muchos profesionales han utilizado el concepto de "enfoque basado en riesgos" para desarrollar su trabajo, no obstante, muy pocos logran aplicar las metodologías utilizadas para trabajar con base en los términos de estadística y probabilidad.

Al tomar un enfoque basado en el riesgo, la organización se hace proactiva más que puramente reactiva, al prevenir o reducir los efectos no deseados y promover la mejora continua. La acción preventiva es automática cuando el sistema de gestión se basa en el riesgo y, al considerar el riesgo en toda la organización, se mejora la probabilidad de lograr los objetivos establecidos, el resultado es más consistente y los clientes pueden confiar en que recibirán el producto o servicio que esperan.

De entrada, las empresas planean objetivos organizacionales a largo, mediano o corto plazo, utilizando métodos para identificar y alcanzar metas, tales como la planeación estratégica, que se divide en tres partes. Por un lado, el entendimiento claro y la buena articulación de la misión del departamento, por otro, una descripción detallada de los asuntos más importantes del departamento y, tercero, una parte que involucra el establecimiento de planes de acción (Sennewald & Baillie, 2015). Así mismo, determinan cuáles podrían ser los obstáculos que dificulten que la organización cumpla estos objetivos tal como se consideraron, qué tan probable es que eso suceda y qué tan grave sería para los intereses de la organización, si esto llegara a ocurrir.

Lo descrito anteriormente es el enfoque basado en riesgos. Cada área o cada proceso establece cuáles son los objetivos específicos que contribuyen al logro de los objetivos organizacionales y, así mismo, cada área o proceso determina qué obstáculo (riesgo) podría afectar el cumplimiento de dicho objetivo. La aparición anticipada (o no) de

estos obstáculos (riesgos) podría tener orígenes dolosos o deliberados que deben ser gestionados desde el área de seguridad corporativa bajo la aplicación de metodologías objetivas y apropiadas para la gestión de riesgos de seguridad empresarial. En el origen de estos riesgos, sin duda, tiene una participación intencional del ser humano, un perpetrador (amenaza) que pueda encontrar y aprovechar debilidades (vulnerabilidades) y hacerse a un beneficio, produciendo un daño (consecuencia) (García, 2008), siendo la anterior una aproximación conceptual a las definiciones conocidas de riesgo. También, se encuentran expresiones asociadas a estos ejercicios en las aplicaciones de estadística de la Teoría de Juegos, toda vez que estos son juegos de suma cero: si alguien gana, es porque alguien pierde (Amster & Pinasco, 2014).

Ahora bien, los practicantes de seguridad, y particularmente aquellos que tienen responsabilidades asociadas a la identificación, análisis y evaluación de riesgos, infortunadamente han asumido la aplicación de la gestión de riesgos como práctica consuetudinaria que pasa por alto las técnicas objetivas y, en especial, aquellas que se relacionan con el cálculo de la probabilidad y el impacto o consecuencias, como las contempladas en documentos científicos o productos del estado del arte. Una relación de técnicas de valoración de riesgos puede ser encontrada en la norma ISO 31010:2019, desde la cual podrá contribuir a las fases descritas en la guía que proporciona la norma ISO 31000:2018 de la siguiente manera:

- Determinar el alcance, contexto y criterios, podría realizarse con técnicas como la tormenta de ideas, SWIF (Estructura Que Pasa Si, por sus siglas en inglés), técnica Delphi, índices de riesgo, matriz de Debilidades, Oportunidades, Fortalezas, Amenazas (DOFA) y el

análisis Político, Económico, Socio-Cultural, Tecnológico, Ecológico y Legal (PESTEL).

- Para identificar riesgos, de la misma manera, se pueden aplicar técnicas como tormenta de ideas, SWIF (Estructura Que Pasa Si, por sus siglas en inglés) y la técnica Delphi.
- El análisis de riesgos puede ser abordado desde las metodologías MonteCarlo, LOPA (Capas de Protección, por sus siglas en inglés), árboles de fallos, de consecuencias, ánálisis Markov, técnicas bayesianas, entre otros.
- El tratamiento podría modelar las opciones propuestas en técnicas como HACCP (Análisis de Peligros y Puntos Críticos de Control, por sus siglas en inglés), escenarios multicriterio, y BIA (Análisis del Impacto en el Negocio, por sus siglas en inglés).

Una manera de abordar el problema y generar medidas de tratamiento se basa en la organización de la gerencia de seguridad, vinculando las habilidades técnicas a las habilidades gerenciales, toda vez que las primeras incluyen actividades propias de la administración (planear, organizar, dirigir, coordinar y controlar). Cobra vital importancia este componente en la medida en que aquel Gerente de seguridad primero es gerente (habilidad administrativa) y luego es de seguridad (habilidad técnica) (Sennewald & Baillie, 2015). La habilidad técnica se refiere específicamente a la actividad de la seguridad, ligada a los propios modelos de seguridad, que a su vez son modelos de prevención en los que se encuentran la seguridad física, seguridad del personal, seguridad de la información (o ciber-seguridad), seguridad reputacional y seguridad de las operaciones. Así mismo, modelos de control o mitigación, como la gestión de crisis, y modelos de recuperación como las investigaciones y los seguros, tal como como se muestra en la figura 1.

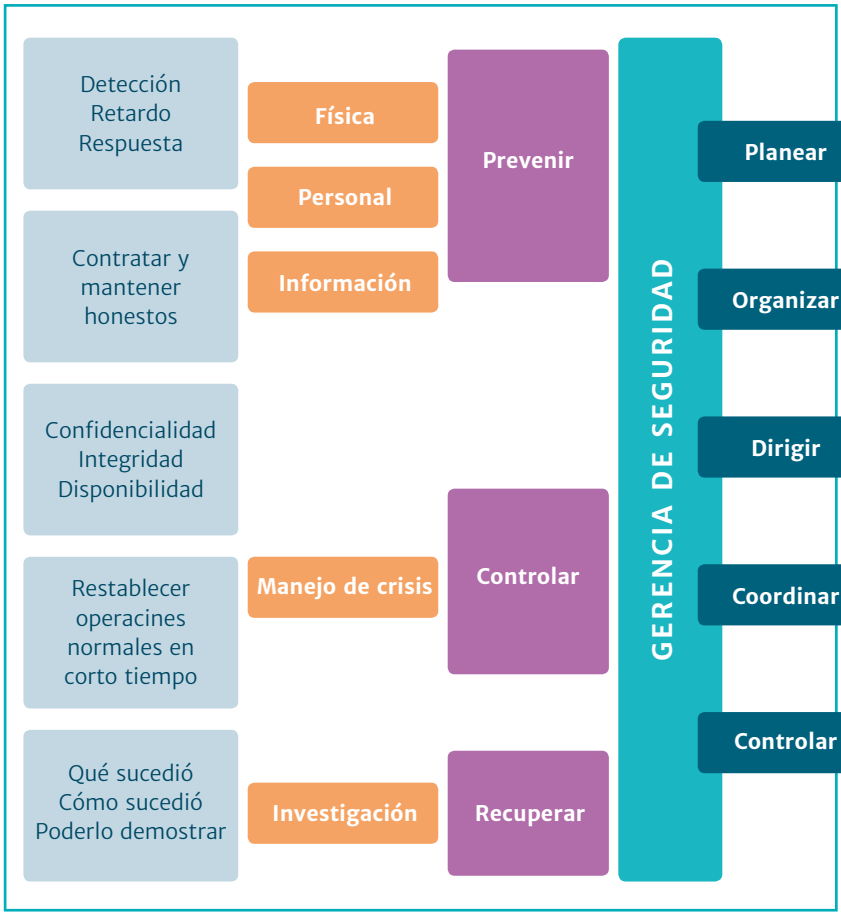


Figura 1. Relación habilidades técnicas vs. habilidades gerenciales
Fuente: *elaboración propia.*

Modelos de prevención

En este contexto, prevenir es reducir la probabilidad de que un evento de pérdida ocurra, es anticiparse a un ataque de un adversario o perpetrador, ya sea interno, externo o interno trabajando para un externo (García, 2006). Estas situaciones conllevan a implementar contramedidas para que dicho adversario no tenga éxito. Los escenarios donde

se prevé que puede encontrar vulnerabilidades y que sean aprovechadas, se asocian a todos los procesos de la organización y pueden dividirse para su estudio en los siguientes modelos de seguridad:

1. Seguridad física.
2. Seguridad del personal.
3. Seguridad de la información.
4. Seguridad de las operaciones.
5. Seguridad reputacional.

Seguridad física

Tiene como objetivo negar el éxito del adversario toda vez que este pueda tener intenciones, motivaciones y capacidades para hurtar, sabotear o lesionar a alguien. Para esto, son consideradas contramedidas que logran detectar y demorar a un perpetrador, mientras la respuesta de la fuerza de seguridad se despliega para interrumpir a dicho adversario en su progreso al activo de interés. La combinación de la eficacia en las medidas de detección, retardo y respuesta que se cuantifican a través del modelo Estimative Adversary Sequence Interruption (EASI) (García, 2008). Este proporciona como resultado la Probabilidad de Interrupción, es decir, qué tan probable es que el perpetrador pueda ser interrumpido, considerando las medidas de seguridad existentes. La eficacia del sistema se puede representar utilizando únicamente la Probabilidad de Interrupción (PI), o mediante el uso de ambos, PI y Probabilidad de Neutralización (PN) en los sitios en donde una respuesta inmediata va a confrontar físicamente al adversario (ASIS International, 2012c). La eficacia del sistema se considera en conjunto con los sistemas de detección, retardo y respuesta, al funcionar de manera simultánea, como lo muestra la figura 2.

Nota: beginnig security survey = encuesta de seguridad de inicio; risk assessment= valoración del riesgo; identification with sensors = identificación con sensores; delay with barriers= retardo con barreras; guards in response= guardas en función de respuesta; execution of the plan= ejecución de proyecto; survey to assess= encuesta para evaluar la eficacia.

Figura 2. Modelos de seguridad y funciones de seguridad física
Fuente: *elaboración propia.*

Seguridad del personal

Se enfoca en el cuidado de los empleados, protegerlos de amenazas externas, de la propia organización, de otros empleados y de sí mismos. Se deben establecer parámetros sobre la protección ejecutiva para procesos de investigación pre-empleo, y así asegurar la contratación de los mejores candidatos sin involucrarse en prácticas discriminatorias, ser honestos con los candidatos a través de la capacitación y el gobierno corporativo ejemplarizante, generar un correcto proceso de desvinculación para limitar motivaciones personales que puedan

causar riesgos asociados a la pérdida de imagen por escándalos y revelación de secretos comerciales. La seguridad del personal incluye también la prevención de la violencia en el lugar de trabajo, la prevención del consumo de sustancias controladas y el libre derecho a la asociación, así como la revisión de procedimientos que puedan volver susceptibles a los empleados a cometer algún acto deshonesto, como el fraude dado por la oportunidad en el desarrollo de funciones. Estos programas están diseñados para orientar a la gerencia y a los empleados en aspectos relacionados con la naturaleza, tipos y áreas más vulnerables a las pérdidas en la organización (ASIS International, 2012a).

Seguridad de la información

Comprende la protección de datos contenidos en medios físicos, informáticos e incluso los dispuestos en el ciber-espacio. Por ende, la ciberseguridad se contempla en este segmento. La seguridad de la información busca reducir las oportunidades de afectación de la integridad de los datos (previniendo su manipulación), la disponibilidad de la información (previniendo la restricción a su acceso, aun con ese atributo) y su confidencialidad, dado que se expone a la revelación de secretos comerciales, corporativos o incluso de seguridad nacional. Infortunadamente, los ataques a la seguridad de la información, en su mayoría, no dejan evidencia física que pueda dar información real y actual sobre un ataque, el uso de herramientas como la ingeniería social y el malware, ponen en situación de vulnerabilidad a los sistemas. Sin embargo, la información no solo está en el medio lógico, los documentos físicos y la información de la que se apropian los empleados en la naturalidad de su trabajo a partir de la necesidad de saber, también tienen que ser protegidos. El uso de tecnología demanda un desafío de mayores competencias para el responsable de la

seguridad corporativa. En términos de intercambio de información, el mundo está interconectado como nunca antes. Debido a este nivel de interconectividad global, las amenazas a los activos de información han llegado a ser más difusas, difíciles de reconocer y pueden actuar más rápido, lo cual quiere decir que el nivel de riesgo está aumentando (ASIS International, 2012b).

Seguridad de las operaciones

Podría ser el más cambiante de los modelos de seguridad, dado que este implica la protección de la esencia del negocio (*core business*) y su cadena de suministro puede estar relacionada con bienes o servicios. Una operación empresarial podría ir desde la producción y comercialización de productos manufacturados (bienes), hasta el suministro de educación, consultoría, entre otros servicios. Sin embargo, el estudio de estas operaciones ha logrado identificar entradas, procesos propios de la organización, salidas y procesos de terceros, que aunque ajenos, comprometen la responsabilidad de la organización. De esta forma, establecer un modelo de seguridad en la cadena de suministro (*Security Supply Chain*) es fundamental. Organizaciones y compañías privadas que rastrean su material y que pueden compartir datos de la trazabilidad en la cadena de suministro son capaces de identificar las potenciales pérdidas de alto valor a través de registros de la empresa, redes informales, fuentes de aplicación de la ley, documentos de código abierto y otros medios (Burges, 2013). De la misma manera, es posible identificar puntos críticos de control para prevenir eventos de sabotaje, contaminación, falsificación o contrabando. Una manera holística de comprender la operación completa de la organización es establecer su cadena de suministro, sus entradas, sus salidas y la relación de las partes (eslabones) con el todo (cadena), tal como lo representa la figura 3.

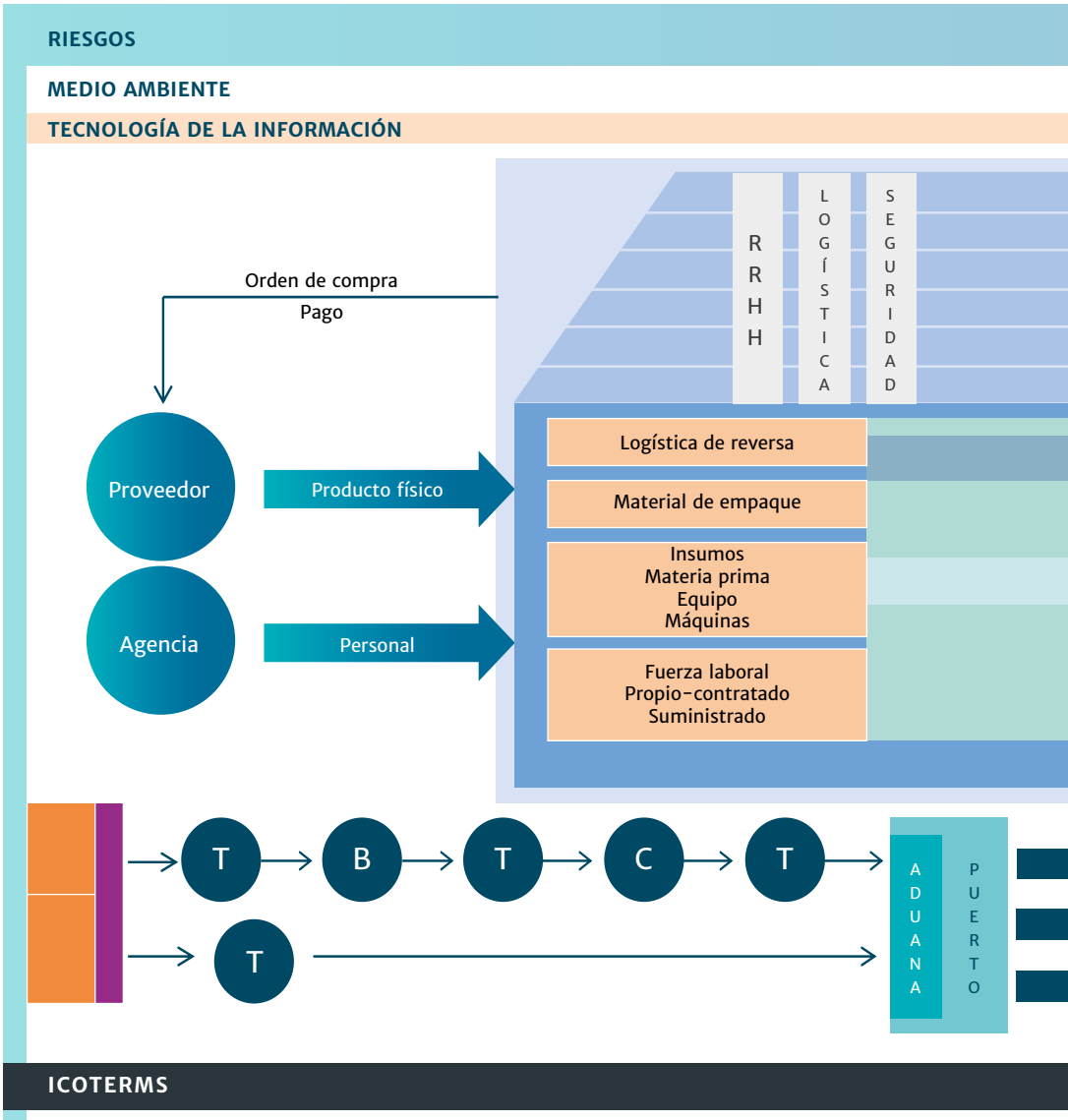
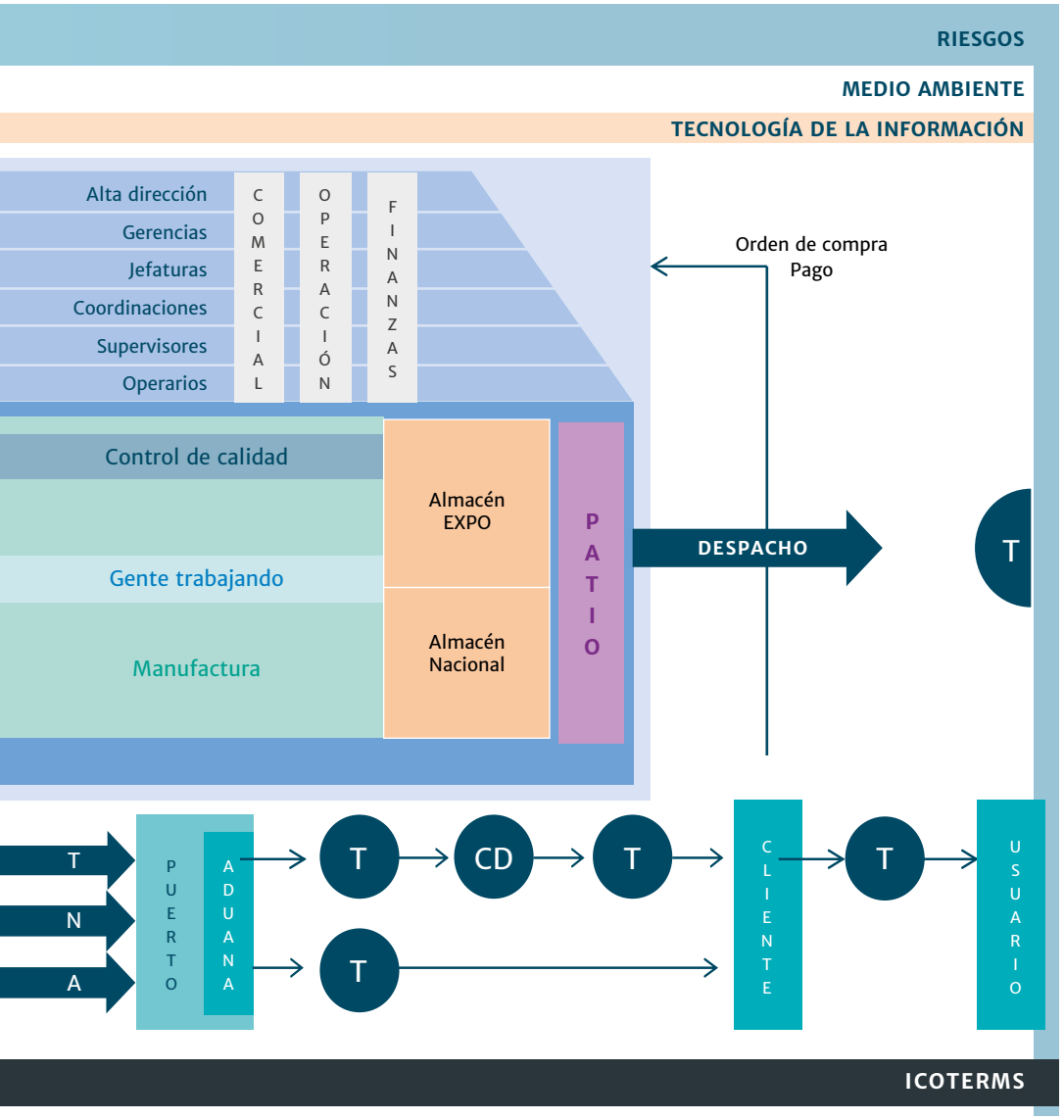


Figura 3. Cadena de Suministro
Fuente: *elaboración propia.*


RIESGOS
MEDIO AMBIENTE
TECNOLOGÍA DE LA INFORMACIÓN
Alta dirección
Gerencias
Jefaturas
Coordinaciones
Supervisores
Operarios
COMERCIAL
OPERACIÓN
FINANZAS
Orden de compra
Pago
Control de calidad
Gente trabajando
Manufactura
Almacén EXPO
Almacén Nacional
PATIO
DESPACHO
T
T
N
A
PUERTO
ADUANA
T
CD
T
T
T
CLIENTE
USUARIO
ICOTERMS

Seguridad reputacional

Es el modelo de seguridad más crítico en la organización. Mientras los activos físicos pueden llegar a recuperarse por indemnizaciones, trabajo extra o recapitalización por los socios, la reputación es el valor intangible que no solo las personas cuidan con esmero, sino también las organizaciones. La reputación organizacional se puede ver afectada por eventos asociados a la corrupción, soborno, fraude, lavado de activos y financiación del terrorismo, actividades que tienen como característica relevante la participación dolosa o accidental de un miembro de la organización, actividades que requieren una preparación especial y un conocimiento fino de un proceso particular de la organización en el que se encuentran vacíos, no se aplica la segregación de responsabilidades o se concentra la toma de decisiones. Una vez publicada la información relacionada con estos eventos, la capacidad de limitar los daños se convierte en una tarea poco exitosa. Aunque la preocupación es corporativa, el nivel estatal también está expuesto. Precisamente, la Organización para la Cooperación y el Desarrollo Económico (OCDE) y la Organización de Estados Americanos (OEA) firmaron en el 2007 un memorando de entendimiento para instaurar un marco de cooperación para las iniciativas anticorrupción. Este acuerdo apoya los objetivos comunes de modernización del Estado, prevención y represión de la corrupción, y promoción de la aplicación de la Convención Interamericana contra la Corrupción de la OEA en 1996 y de la Convención de las Naciones Unidas contra la Corrupción en el 2003 (BDO-Global, 2019).

Modelos de control

Los modelos de control se relacionan con la reducción del impacto/consecuencia en el escenario de la mitigación. Este programa se asocia al

manejo de crisis en su propósito de reanudar las actividades a "modo normal", tal como lo hacía la organización antes del acto disruptivo. Las emergencias y contingencias inesperadas suceden con una regularidad desalentadora. Cuando ocurre un desastre u otro tipo de emergencia, se deben tomar varias decisiones mientras el suceso continúa en desarrollo y se desconoce la verdadera dimensión de la situación (ASIS International, 2012d). Los modelos específicos de seguridad que permiten abordar los programas de control podrían tener una estructura denominada "Plan de manejo de crisis" que considera un "Marco de referencia" y un "Plan de continuidad del negocio". El primero se refiere a aspectos teóricos y de referencia organizacional como propósito, justificación, alcance, objetivos, miembros de los comités, datos de contacto, entre otros. El Plan de continuidad del negocio, aborda los momentos relevantes de la operación: antes, durante y después. Antes, refiere a planes de resiliencia organizacional, que prepara a la organización para soportar actos disruptivos, perturbadores o indeseables. Durante, se relaciona con planes de mitigación del incidente, que se conocen, en nuestro contexto, como planes de emergencia, cuyo objetivo es controlar la emergencia, mitigando las pérdidas durante la presencia del evento disruptivo. Después, los planes de recuperación del desastre buscan reanudar las operaciones reduciendo los tiempos para volver a la normalidad de las operaciones. Una crisis tiene el potencial de detener de manera impactante la operación, puede inclusive afectar a aquellas organizaciones externas, públicas o privadas a las cuales se acudiría como parte de los acuerdos de ayuda mutua. Planear escenarios de crisis puede resultar tan obvio, que no se lograría dimensionar el efecto nefasto de su materialización. La planeación en "estados comunes" vuelve monótonos los ejercicios y hace perder de vista el compromiso de la organización por mantenerse viva en el mercado. El manejo de crisis es una actividad estratégica de la organización, involucra las

actividades sensibles, compromete la seguridad y salud de los trabajadores, pues su protección resulta subordinada a las decisiones de un comité influido positivamente por la tesis, los argumentos y contrargumentos del líder de gestión de riesgos de seguridad empresarial.

En ese sentido, el plan de continuidad de negocio se entiende como el plan para mantener en funcionamiento la operación del negocio en los niveles que pueda mantener las operaciones críticas. Esto implica un ejercicio de identificación de los procesos críticos de la compañía, y los estados tolerables de estos para diseñar las mejores contramedidas. Según ASIS International, el modelo comprende dos etapas. En la primera, fases de construcción, y en la segunda, actividades de mantenimiento (ASIS International, 2005). Según la norma ISO 22301:2019 (Sistemas de gestión de continuidad de negocio), se entienden las necesidades de preparación para la continuidad, en términos de una potencial interrupción de las operaciones considerando conceptos como máxima parada aceptable, máximo periodo tolerable de disrupción, mínimo objetivo de continuidad del negocio, punto objetivo de recuperación, tiempo objetivo de recuperación, análisis de impacto en el negocio y acuerdos de ayuda mutua (ISO, 2012).

Modelos de recuperación

Los modelos de recuperación también se asocian con la mitigación en el sentido de recuperar, en los casos que esto sea posible, los activos físicos perdidos o afectados por eventos que los modelos de prevención no lograron evitar, y aquellos que los modelos de control no lograron contener satisfactoriamente. Estos modelos son:

1. Investigaciones.
2. Seguros.

El propósito de las investigaciones es determinar qué sucedió, cómo sucedió, poderlo demostrar y ser la entrada para nuevas alternativas de prevención con el propósito de evitar su repetición. Las investigaciones pueden tener un objetivo diferente y, de allí, quién es el responsable de conducirla. En el contexto corporativo, la investigación o indagación administrativa se limita exclusivamente a determinar las causas por la cuales el evento de pérdida ocurre; mientras en la investigación criminal o judicial, la mayoría de los casos está a cargo de los organismos de seguridad del Estado y aplica protocolos específicos de cadena de custodia, busca identificar al responsable, al culpable y presentar las evidencias para su judicialización. Desde una perspectiva de gestión, es importante considerar el propósito de la investigación, tanto a nivel de operativo como a nivel estratégico. En el caso de nivel operativo, se establece el contexto dentro del cual se llevó a cabo el evento y se ayuda a mantener a la gente trabajando el caso particular. A nivel estratégico, con el propósito de una investigación, se determina la planificación, organización y equipamiento necesarios (ASIS International, 2010).

De otro lado, la seguridad indemnizatoria combina actividades de prevención y recuperación. Tradicionalmente, la oportunidad de asegurar activos ha estado condicionada a un requisito legal o contractual, y no por una iniciativa de seguridad como producto de la identificación de un evento de baja probabilidad y con un potencial de interrumpir de manera dramática la operación. Las pólizas de seguros, a través de las cláusulas de garantías, llevan al tomador de decisiones a aplicar medidas de autocuidado y de prevención que buscan la reducción de la probabilidad de ocurrencia del evento. Si estas no son aplicadas, la conclusión podría orientarse a una negación en la reclamación o indemnización. Más allá de los riesgos previsibles, la cobertura contribuye a la reducción económica de la pérdida, siempre que se hayan

tomado las medidas razonables para su no ocurrencia. Del mismo modo, las pérdidas que no se puedan reparar por vía económica, como la afectación de reputación o daño de imagen, no son consideradas en su extensión por este modelo. Las herramientas de gestión de riesgos son proactivas o reactivas, pero los seguros son una combinación de ambas. La actitud proactiva es la forma más conocida de transferir el riesgo y, de hecho, se considera un activo de la organización. También es reactiva porque los beneficios del seguro no se usan hasta después de que la pérdida ocurre (ASIS International, 2012a).

Así las cosas, la gestión de riesgos de seguridad empresarial considera todos los riesgos de la organización que tienen origen deliberado, así afecten la seguridad y salud de los trabajadores. Integra de manera transversal las preocupaciones de la organización por mantener en estados aceptables los riesgos identificados, una articulación adecuada de los diferentes modelos podría considerarse como lo indica la figura 4.

Relación costo/beneficio

Las medidas de seguridad que implementan las organizaciones deben ser presupuestadas, lo que significa un esfuerzo económico por parte del liderazgo ejecutivo. Habitualmente se habla de "inversión en seguridad", cuando en realidad se trata de un gasto. El primero, es el uso de una porción de la producción de un segmento para incrementar la producción del próximo periodo o aumentar el stock de capital, mientras el segundo incluye gastos de ventas tales como remuneraciones y comisiones pagadas al personal de ventas, propaganda, promoción, entre otras. Asimismo, comprende todos los gastos de administración tales como remuneraciones del personal administrativo, impuestos y

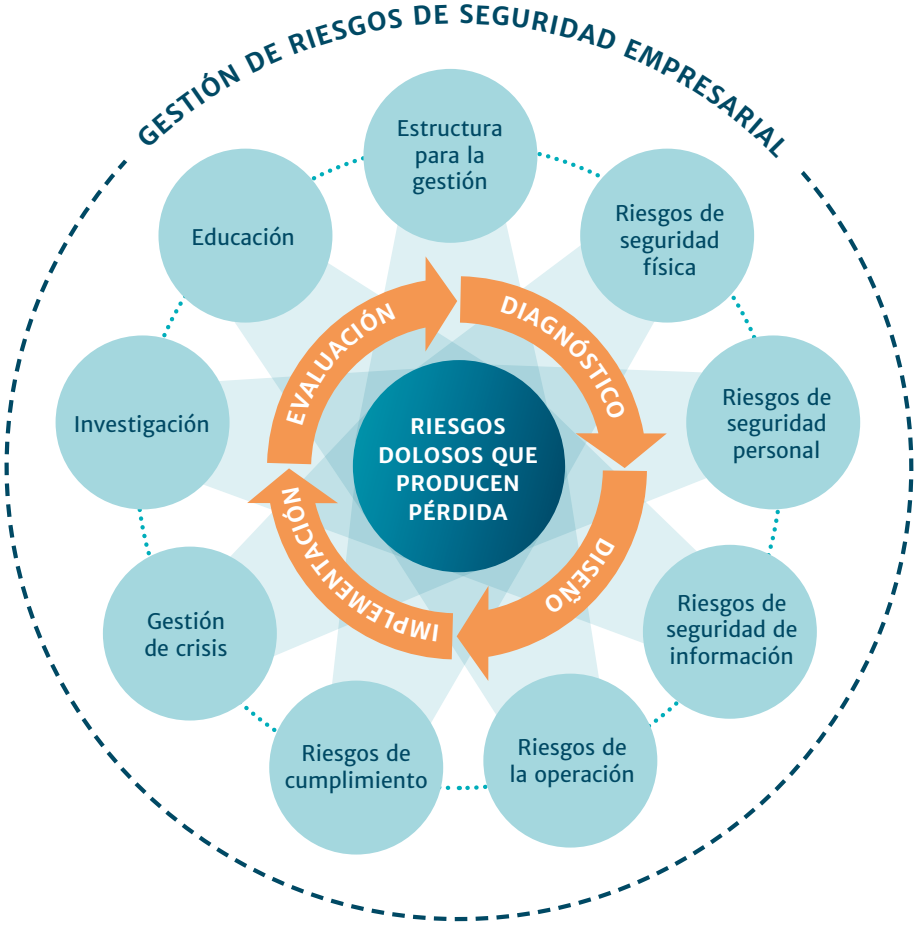


Figura 4. Integración de gestión de riesgos empresariales
Fuente: *elaboración propia*

suscripciones (Bolsa de Valores de Guayaquil, 2012). Ciertamente es un gasto que tiene un retorno y un beneficio.

La palabra "inversión" implícitamente trae conceptos de renta o utilidad, medidos por un medio estándar que es el dinero: "invierto 10 porque espero recibir más adelante 12, 13 o más". El liderazgo ejecutivo entiende que las erogaciones hacia la gestión de riesgos de seguridad empresarial pueden ser onerosas, como también entiende que por esta área de la organización no hay ingresos que se puedan traducir en ganancias líquidas; de manera que el desafío se orienta a justificar, desde el enfoque de la relación costo/beneficio, un programa de seguridad que intente reducir la probabilidad y limitar las consecuencias de manera razonable y al mejor precio. Del mismo modo, es un desafío para el líder de la gestión de riesgos de seguridad empresarial exponer a los tomadores de decisiones la necesidad de proteger la organización ante amenazas, ya que una aproximación al concepto de análisis de impacto en el negocio podría indicar lo que significa para la organización una pérdida significativa por no destinar recursos para su prevención, control o recuperación, casos como cisnes negros en un avión impactando edificios, o una pandemia que mantiene a una población mundial confinada en su casa, son claros ejemplos de la necesidad de preparase, aun para los escenarios poco probables. El éxito de la aprobación del presupuesto de seguridad se basa en la capacidad que tiene el líder de gestión de riesgos de seguridad empresarial para presentar un caso estructurado de negocio (*business case*) que hable el "idioma de los negocios". Construir un caso de negocios convincente para superar los desafíos y expresar la importancia del trabajo relacionado con el riesgo puede parecer desalentador, pero si vale la pena implementar el programa, vale la pena expresar su posición (OCGE, 2018).

La gestión de riesgos de seguridad empresarial formula una entrada que permite valorar los riesgos inherentes, convirtiéndose en una línea de base. El conocimiento del contexto y de la manera en que la organización opera permite definir el nivel de protección requerido de tal manera que este se vuelva en una referencia. Así, esta línea de base se convierte en el punto de partida y el nivel de protección requerida en el punto de llegada. En la relación costo/beneficio no solo se considera el costo de las medidas a implementar, sino el costo en términos del traumatismo que toda transición genera al implementar medidas estructurales, cuyo impacto se puede palear con un correcto proceso de gestión de cambio aplicado de manera permanente.

Conclusiones

La gestión de riesgos de seguridad empresarial se convierte en la herramienta más efectiva para conducir y monitorear todos los modelos de seguridad al interior de las organizaciones, considera una etapa de diagnóstico que permite establecer de manera objetiva y libre de sesgo las probabilidades de cada riesgo, así como los efectos negativos que este tendría en el momento de su materialización. La consideración del nivel de protección requerida, específica para cada organización, considera no solo el contexto sino sus objetivos, así se establecería una referencia en sentido de lograr el mejor escenario posible. Lo anterior da entrada a la etapa de diseño, en la que se conciben las mejores alternativas, tanto organizacionales como procedimentales y técnicas, una mixtura entre tecnología, procedimientos y personal, que tendrían como resultado la reducción de riesgo a estados aceptables (Patterson, 2016). La etapa de la implementación llega a considerar el costo asumido por la organización en relación con el beneficio recibido

de la materialización de robustos, pero dinámicos y flexibles modelos de seguridad, se genera un inventario de contramedidas por implementar que, organizadas razonablemente, se gestionan como un proyecto de alto impacto para la organización. Como etapa última y permanente se establece la evaluación, que permite mantener un estado de actualización recurrente, por lo que es necesario establecer medidas de seguimiento, a manera de indicadores claves de desempeño, que permitan validar que el esfuerzo de la organización tuvo un efecto en la reducción del riesgo inherente, a un costo razonable.

En este sentido, el enfoque basado en riesgos permite a los tomadores de decisiones decantarse por la mejor opción con niveles de certidumbre informados y orientar el esfuerzo de seguridad en áreas que verdaderamente lo necesitan, teniendo en mente que la admiración de los recursos en seguridad en realidad es la administración del recurso escaso. La gestión de riesgos de seguridad empresarial, entonces, contribuye a la estructura del profesional de seguridad, ya que le permite orientarse dentro del contexto empresarial, organizacional o corporativo, creando métricas e indicadores claves de desempeño con cobertura a todas las áreas susceptibles.

Referencias

Amster, P., & Pinasco, J. (2014). *Teoría de Juegos. Una introducción matemática a la toma de decisiones.* Fondo de Cultura Económica.

ASIS International. (2005). *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery.* ASIS International.

ASIS International. (2010). *Manual del Investigador Profesional.* (C. Ramirez trad.). ASIS International.

ASIS International. (2012a). *Protection Of Assest Manual: Security Management.* ASIS International.

ASIS International. (2012b). *Protection of Assets: Information Security.* ASIS International.

ASIS International. (2012c). *Protection of Assets: Physical Security.* ASIS International.

ASIS International. (2012d). *Protection of Assets: Crisis Management.* ASIS International.

ASIS International. (2019). *Enterprise Security Risk Management (ESRM) Guideline.* ASIS International.

BDO-Global. (2019). *El mapa del fraude corporativo en América Latina 2018/2019.* BDO-Global.

Bolsa de Valores de Guayaquil. (2012). *Diccionario de Economia y Finanzas.* Bolsa de Valores de Guayaquil.

Burges, D. (2013). *Cargo Theft, Loss Prevention and Supply Chain Security.* Butterworth-Heinemann.

García, M. (2006). *Vulnerability Assessment of Physical Protection Systems.* Burlington: Butterworth-Heinemann.

García, M. (2008). *Design and Evaluation of Physical Protection Systems.* Burlington: Butterworth-Heinemann.

International Standarization Organization, ISO. (2012). *ISO 22301:2012 Sistemas de Gestion de la Continuidad del Negocio.* ISO.

International Standarization Organization, ISO. (2014). *Documento N1222. ISO/TC176/SC2. Riesgo en ISO 9001:2015.* ISO.

OCGE. (2018). *The Winning Business Case.* Project Risk Leader.

Patterson, D. (2016). *Implementing Physical Protection Systems: A Project Management Guide.* CreateSpace Independent Publishing Platform.

Sennewald, C., & Baillie, C. (2020). *Effective Security Management.* Butterworth-Heinemann.

Talbot, J., & Jakeman, M. (2009). *Security Management Body of Knowledge.* John Wiley & Sons Inc.