N.º 16

COLECCIÓN C&PA

Colección Ciencia y Poder Aéreo

Publicación de la Escuela de Postgrados de la Fuerza Aérea Colombiana

Enfoques y gestión en Seguridad Integral

Yuber Rico Venegas
David Enrique López Cortés
Alejandra Cerón Rincón

— Compiladores —

Enfoques y gestión en Seguridad Integral

Enfoques y gestión en Seguridad Integral

Yuber Rico Venegas
David Enrique López Cortés
Alejandra Cerón Rincón
(Compiladores)

Escuela de Postgrados de la Fuerza Aérea Colombiana
Maestría en Dirección y Gestión de la Seguridad Integral
Grupo de Investigación CIPAER
Grupo de Investigación GISIC

Catalogación en la Publicación
Escuela de Postgrados Fuerza Aérea Colombiana

Enfoques y gestión en seguridad/Yuber Rico Venegas, David Enrique López, Alejandra Cerón R., compiladores; Alejandro Ortiz Ríos. [y otros nueve]. – Bogotá D.C.: Escuela de Postgrados Fuerza Aérea Colombiana, noviembre del 2020.
240 páginas. : il. 24cm. – (Ciencia y Poder Aéreo; No 16)

ISBN 9789585996182
E-ISBN 9789585996199

Parte 1 ENFOQUES SOBRE LA SEGURIDAD PARTE 2 GESTION EN SEGURIDAD
1. Cerón R, Alejandra - Ortiz Ríos, Alejandro 2. Cerón R, Alejandra - Hoyos, Carlos Alberto 3. López Cortés, David E 4. Ortiz Ríos, Alejandro - Parra, Oscar I. 5. Contreras Fernández, Arístides Baldomero 6. Puentes Becerra, Julián Andrés 7. Moncada N. Álvaro F. 8. Álvarez Calderón, Carlos Enrique - Ramírez Pedraza, Yesid Eduardo 9. Seguridad del Estado 10. Prevención de Riesgos 11. Colombia Fuerza Aérea Colombiana 12. Escuela de Postgrados de la Fuerza Aérea Colombiana.

HV8290.

DOI: https://doi.org/10.18667/9789585996199

Registro Catálogo SIBFA 115055

Libro de investigación
Evaluado por pares
Primera edición: Bogotá D.C. Colombia (Suramérica), noviembre del 2020
Colección Ciencia y Poder Aéreo N.º 16
ISBN: 978-958-59961-8-2
E-ISBN: 978-958-59961-9-9

Compiladores

Yuber Rico Venegas
David Enrique López Cortés
Luz Alejandra Cerón Rincón

Autores

Alejandro Ortiz Ríos
Álvaro Moncada Niño
Aristides Baldomero Contreras Fernández
Carlos Alberto Hoyos
Carlos Enrique Álvarez Calderón
David Enrique López Cortés
Julián Andrés Puentes Becerra
Luz Alejandra Cerón Rincón
Oscar Iván Parra
Yesid Eduardo Ramírez Pedraza

Versión digital - OMP: Biteca Ltda.
Impresión: Comercializadora Comsila SAS

Impreso y hecho en Colombia.

Carrera 11 N.º 102-50 Edificio ESDEGUE.
Bogotá, Colombia (Suramérica). Oficina 411
A.A. 110111
libros.publicacionesfac.com

Contenido

Introducción

En Colombia, los desafíos en materia de seguridad han promovido un cambio en la interpretación del problema, así como la implementación y gestión de planes políticos. Esto ha suscitado, a su vez, el interés de las agremiaciones de profesionales del sector por alcanzar altos niveles de conocimiento y capacitación para responder preventivamente a las nuevas amenazas que el contexto actual plantea.

Las instituciones que ofrecen programas de formación en seguridad, especialmente las de educación superior, comienzan a plantearse retos de investigación y formación enfocados en competencias que le permitan a la comunidad de la seguridad construir diálogos y decisiones acordes con las exigencias de los campos público y privado. De esta forma, se muestra el interés, tanto de las agremiaciones de profesionales como de los centros educativos, en construir estándares de calidad educativa basados en la innovación y la generación de conocimiento especializado para el sector de la seguridad.

En consecuencia, esta publicación de la Maestría en Gestión y Dirección de la Seguridad Integral (MADGSI) de la Escuela de Postgrados de la Fuerza Aérea Colombiana (EPFAC) reporta resultados de investigación basados en dos dimensiones de análisis. La primera se refiere

a algunos de los fundamentos conceptuales y metodológicos para la interpretación del dilema de la seguridad. En el pensamiento de la filosofía política y de las distintas ciencias sociales se halla la configuración de un debate central sobre las aproximaciones a la noción de seguridad. Los distintos paradigmas de las ciencias sociales presentan, por una parte, las visiones clásicas, orientadas a la reflexión central respecto al rol del Estado en los diferentes contextos de la seguridad; por otra parte, presentan las visiones contemporáneas que tienen en cuenta distintos niveles de influencia y de participación de actores tanto gubernamentales como civiles y del sector privado, los cuales conforman redes complejas de relaciones e intereses.

La segunda dimensión de análisis se enfoca en la discusión sobre la gestión y los posibles modelos para abordar las cuestiones relacionadas con la seguridad. Si en el pasado los desafíos de la seguridad fueron afrontados directamente, a través de la organización y la respuesta efectiva de las agencias encargadas, en la actualidad los dilemas relacionados se caracterizan por un alto grado de incertidumbre y volatilidad. La vulnerabilidad ante el riesgo es una constante. Así, por ejemplo, los países más desarrollados han dejado de preocuparse por el hambre de sus poblaciones. En cambio, se ocupan de problemas más silenciosos como la obesidad, la contaminación y la estabilidad de la economía. Por su parte, en los países con menos infraestructura productiva el hambre permanece presente y sin solución, generando un escenario propicio para fenómenos que en el corto plazo pueden alcanzar la dimensión de *amenaza* global. Este es el caso de las pandemias o del crimen organizado. Dichos complejos de riesgo requieren de la acción coordinada de actores de diversa índole para gestionar las potenciales amenazas.

Ahora bien, como resultado de la transformación del panorama de la seguridad, y debido a los diversos avances científicos y a la

tecnificación de las fuerzas productivas que afectan el estilo de vida de los ciudadanos, se han generado nuevos riesgos, difíciles de calcular y que deben ser enfrentados eficientemente. La capacidad de las grandes industrias para dimensionar y controlar el riesgo derivado de sus actividades se ha visto impedida, como lo ilustran los casos de accidentes por el manejo de energía nuclear. Sin lugar a duda, las tragedias para la humanidad y los daños que han causado (algunos de ellos irreversibles contra el medio ambiente y que ponen en riesgo la condición de la vida en el planeta), son móviles para una reflexión al respecto. En suma, se promueve un cambio social relacionado con una mayor conciencia de las consecuencias de las acciones humanas sobre el medio ambiente y la propia seguridad humana.

Los riesgos y desafíos de la seguridad presentes hoy en día la mayoría de las veces son imperceptibles, pues son el resultado de una producción industrial sin control y de la participación de diversos grupos sociales en economías ilegales o marginales. Los riesgos pueden estar relacionados con la exposición a elementos químicos tóxicos presentes en el ambiente, los ciberataques, la superproducción, los desequilibrios ambientales y hasta la amenaza de una destrucción atómica. El reto de la seguridad contemporánea se refiere a la insuficiencia del Estado para lidiar con los problemas subrepticios y estructurales de las sociedades modernas y globalizadas.

Otra característica de estos riesgos y desafíos es que, a pesar de que su origen sea local, con mucha facilidad pueden alcanzar una trascendencia global con implicaciones para los seres humanos, los animales y la vegetación. Problemas actuales como la tala indiscriminada de árboles son recurrentes y se presentan desde hace varios siglos. No obstante, en la actualidad dichas actividades alcanzan magnitudes globales debido a una industrialización igualmente global. Es decir que, aunque la tala de árboles no se dé en todas las regiones del

mundo, esta actividad "aislada" o circunscrita a algunas regiones sí llega a afectar a la vida en el planeta entero.

Estos riesgos hacen parte del proceso modernizador posindustrial, de la aparición de las tecnologías de la información y la comunicación (TIC), y de las nuevas dinámicas de la producción mundial deslocalizada. A su vez, es importante resaltar que otra clase de riesgos que han estado presentes en toda la historia de la humanidad, aún se mantienen como generadores de conflicto en sociedades de diversas regiones del mundo. Este es el caso de los problemas asociados con la salud de amplios sectores poblacionales que viven en condición de pobreza. Los diversos avances en investigación social y el desarrollo de programas de gobierno, así como la acción de las diferentes Organizaciones No Gubernamentales (ONG) presentes alrededor del mundo, no logran mitigar estos problemas.

Desde este punto de vista, las preocupaciones recurrentes en los planes de desarrollo de gobiernos y de diferentes instituciones sociales (que giraban en torno a la distribución de la riqueza, y la desigualdad) persisten, pero ahora son abordadas desde las nuevas perspectivas de la gestión política. La investigación científica de los riesgos y su gestión atrae la atención del público en general, que está atento a lo que está sucediendo pues tiene cada vez una mayor conciencia de las implicaciones y consecuencias derivadas de estos problemas.

En tal sentido, este libro presenta una discusión respecto al estado del arte de la seguridad integral con el propósito de favorecer el desarrollo de competencias en investigación y la formación de pensamiento estratégico en el área. Asimismo, esta investigación se convierte en un insumo para el fortalecimiento de competencias propias del ser, el saber y el saber hacer en el contexto de la seguridad integral.

El problema de investigación abordado en el texto se refiere a la comprensión que presentan los distintos enfoques de investigación

y análisis asociados a las temáticas incluidas en la seguridad integral. Esta investigación espera establecer vínculos con el ejercicio profesional de gestión de problemas de seguridad y avanzar hacia propuestas de gestión que permitan prever y anticiparse a las posibles amenazas y riesgos que enfrenta constantemente cualquier institución en un mundo volátil, cambiante, dinámico, complejo y lleno de incertidumbres.

Metodología de investigación

Este libro es el resultado de un proyecto de investigación de la Maestría en Dirección y Destión de la Seguridad integral (MADGSI), denominado *Impacto de las políticas de seguridad integral en el desarrollo y gestión del componente de investigación del currículo MADGSI*. Para desplegar las capacidades de profundización y alcance de un proyecto de estas características era necesaria la construcción de un estado del arte consistente e interdisciplinar. La revisión bibliográfica sobre las teorías, las metodologías y las epistemologías presentes en los debates clásicos y contemporáneos sobre la seguridad hizo evidente la necesidad de elaboración conceptual para la exploración de la seguridad integral.

Los capítulos que pertenecen a la primera parte de este escrito recorren discusiones epistemológicas y ontológicas de la seguridad integral a través de la revisión de textos pertenecientes a la sociología, a las relaciones internacionales y a la historia. A través de estas disciplinas, y desde distintos enfoques interpretativos, se hace una evaluación intuitiva de la realidad global actual. La segunda parte contiene estudios de caso de la gestión del riesgo y los procesos de la seguridad empresarial, de la cadena de suministros y de la seguridad del trabajo. Estos trabajos tienen un carácter descriptivo y analítico que abarca los procedimientos de la seguridad y sus vulnerabilidades.

Las reflexiones presentadas en esta investigación son necesarias para la evolución conceptual de la seguridad integral, la cual se postula como una posición viable para concebir los desafíos contemporáneos de la seguridad. El impacto inmediato buscado mediante esta revisión del estado del arte y de algunas gestiones específicas de seguridad no tradicional, es la reflexión sobre los conceptos y teorías enseñadas en los cursos y procesos de posgrados como los de la MADGSI.

Yuber Rico Venegas
Alejandra Cerón Rincón

PARTE 1

Enfoques sobre la seguridad

Capítulo 1

Aproximaciones contemporáneas a la noción de seguridad[1]

Alejandra Cerón R.*
Alejandro Ortiz Ríos**

1 Capítulo de libro resultado del proyecto de investigación titulado *Impacto de las políticas de seguridad integral en el desarrollo y gestión del componente de investigación del currículo* MADGSI, de la línea de investigación Seguridad Integral del grupo de investigación CIPAER, con código COL 0093003, de la Escuela de Postgrados de la Fuerza Aérea Colombiana.

* Doctora en Estudios Políticos y Relaciones Internacionales de la Universidad Nacional de Colombia. Magíster en Gestión de Organizaciones de la Université du Québec à Chicoutimi (UQAC), Canadá. Socióloga de la Universidad Nacional de Colombia. Docente e investigadora. Correo electrónico: luz.ceron@epfac.edu.co

** Especialista y magíster en Seguridad y Defensa Nacional de la Escuela Superior de Guerra de Colombia. Administrador Aeronáutico. Correo electrónico: alejandro.ortiz@fac.mil.co

CÓMO CITAR

Cerón R. A., & Ortiz Ríos, A. (2020). Aproximaciones contemporáneas a la noción de seguridad. En Y. Rico, D. López Cortés, & A. Cerón R. (comps.), *Enfoques y gestión en Seguridad Integral* (pp. 21-43). Escuela de Postgrados de la Fuerza Aérea Colombiana. https://doi.org/10.18667/9789585996199.01

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

CAPÍTULO 1.
Aproximaciones contemporáneas a la noción de seguridad

https://doi.org/10.18667/9789585996199.01
Bogotá, Colombia
Noviembre, 2020

RESUMEN

Los referentes conceptuales de la seguridad han sido construidos a partir de diversos enfoques de las ciencias sociales. Las relaciones internacionales han sido el campo más prolífico de estudios. Allí, la teoría realista y su paradigma filosófico lograron una influencia determinante en la definición de la cuestión, pues enmarcaron el problema de la seguridad en el terreno estratégico militar. Después del surgimiento de la globalización contemporánea, los dilemas políticos concernientes a las amenazas para la seguridad de los Estados y las sociedades, lejos de simplificarse, se presentan cada vez más como un entramado de redes de interacciones y niveles de poder yuxtapuestos. La configuración de este entramado ha obligado a que la reflexión se construya a partir de diálogos de saber transdisciplinares. La coherencia en este campo es dada por la convergencia de los temas de investigación, más que por los enfoques o las inclinaciones ideológicas de los autores.

PALABRAS CLAVE

Prevención de riesgos; seguridad del Estado; seguridad humana; sociedad contemporánea; teoría política.

Introducción

En un intento por nutrir la discusión y el discernimiento en torno a la seguridad contemporánea, la tarea de los académicos es ampliar los escenarios de argumentación y de conexión conceptual para propiciar un enlace con las prácticas y sucesos empíricamente verificables. En ese sentido, este texto se organiza para conjugar los avances teóricos y epistemológicos hechos por los teóricos de las relaciones internacionales con propuestas sociológicas novedosas. Este capítulo es el resultado de la imperiosa necesidad de reflexionar sobre los nuevos desafíos a los que se enfrentan la academia y la investigación posgradual, una reflexión necesaria para emprender procesos de innovación académica.

En primer lugar, se explicará el tránsito de las consideraciones teóricas y políticas de la seguridad tradicionales, centradas en el Estado, a las concepciones actuales. Estas últimas sostienen que ha habido una evolución en el concepto originada por las presiones sociales y por los desarrollos teóricos de diversas disciplinas. En segundo lugar, se presentará una descripción más amplia de las corrientes teóricas contemporáneas que se refieren a un panorama complejo de la seguridad. Este panorama, planteado por Barry Buzan y Ole Waever (2003), va más allá de la seguridad nacional. En tercer lugar, se describirá la propuesta sociológica de Ulrich Beck sobre la sociedad del riesgo para problematizar los límites conceptuales de la seguridad en las relaciones sociales observables. En cuarto lugar, se sostendrá que hay una relación entre la seguridad actual y la teoría de la sociedad del riesgo y se ampliará el horizonte del desarrollo teórico a partir de algunos cuestionamientos epistemológicos. En último lugar, se propondrán algunas conclusiones alrededor de las discusiones éticas de la seguridad y del riesgo.

De la concepción estatocéntrica a la compleja

La historia de la consolidación de la unidad política del Estado tiene un correlato interpretativo relacionado con el dilema de la seguridad. Desde su concepción misma, los principales problemas que debía enfrentar el Estado se referían a la seguridad. Por ejemplo, la pacificación interna de los territorios y su defensa externa eran los principales deberes de protección del Estado. Al menos esta fue la situación de Europa durante el siglo XV, como lo relata el profesor Marquardt:

> El Sacro Imperio Romano-Germánico se encontraba, paralelamente a la construcción y el establecimiento del "sistema constitucional de la paz eterna en la tierra", en una situación de política exterior en la que necesitaba defenderse contra las olas de ataque del Imperio Otomano, que usó eficientemente las nuevas técnicas de la artillería militar y se presentó de esta forma como un *gunpowder Empire* marcadamente superior (Marquardt, 2009, p. 29).

La conceptualización de la seguridad pareció entonces estar definida dentro de los límites de la seguridad nacional y, por lo tanto, las posibilidades de acción frente a las amenazas debían ser comandadas por el Estado. Lo anterior derivó en que los análisis de las ciencias sociales respecto a la seguridad se enmarcaran en un debate *estatocéntrico*.

Esta visión clásica, que fue el eje vertical para la construcción de las teorías relativas al problema de la seguridad, empezó a encontrar dificultades en su aplicación conforme avanzaba la historia contemporánea del Estado. La contención de los problemas de las sociedades posindustriales empezó a superar la lógica tradicional de las amenazas externas y del orden interno. De esta manera, junto con los avances teóricos y metodológicos de la sociología y de la filosofía política, los

académicos se encontraron en la necesidad de formular escenarios de comprensión más complejos, como las redes de interacción múltiples entre actores de diferente constitución a la del Estado (por ejemplo, los movimientos sociales o la naturaleza).

Dadas las dificultades de su aplicación en investigación de campo, la visión clásica de la seguridad comenzó a ser objeto de crítica por parte de los teóricos de la sociología y de las relaciones internacionales. Dentro de estos planteamientos críticos emerge la teoría de los complejos de la seguridad de Buzan (1981). Según esta teoría, la noción de seguridad debe evolucionar conforme cambian las relaciones sociales a través de la historia. Buzan y Waever describen cómo la definición pasó de una noción estatocéntrica a una más compleja: de preocupaciones de seguridad compartidas por dos Estados a procesos interconectados de *securitización*[2] y desecuritización percibidos por diversas unidades (Buzan & Waever, 2003). De este cambio de definición, se resalta la ampliación de los actores que perciben la seguridad (más allá de los Estados) y el espacio que gana la interpretación subjetiva sobre los componentes objetivos de la seguridad.

Buzan (2008) afirma en su teoría que el concepto de seguridad debe ir más allá del estudio del poder o de la paz. Si bien en los orígenes de la noción esos elementos fueron determinantes, en el mundo contemporáneo el análisis debe incluir otros factores, como los asociados a las dinámicas económicas, las dimensiones culturales, los impactos ambientales, entre otros. La combinación de estos elementos termina por caracterizar las relaciones complejas e interdependientes de la seguridad. Ante la ausencia de un análisis tradicional orientado

2 Terminó derivado del inglés *securitization*. Según Waever (1995), en esencia es una reacción contra los estudios tradicionales sobre seguridad.

en esta dirección, se puede apreciar que existen grandes desafíos en la construcción del concepto de seguridad.

La conceptualización contemporánea de la seguridad

Terminada la Primera Guerra Mundial existía un gran discurso político internacional que giraba en torno al término de seguridad colectiva. Sin embargo, los acontecimientos posteriores, sucedidos en el periodo entre guerras, mostraron el desinterés de los Estados por trabajar conjuntamente en el desarme militar y las acciones de pacificación mundial. Esto generó dudas sobre la legitimidad de ese discurso de pacificación que promovía acciones interestatales.

Las teorías liberales proveían al debate teórico sobre el Estado (en el marco de las relaciones internacionales) de un ideario institucionalista e incluso funcionalista. Desde estas perspectivas, provenientes de versiones clásicas del liberalismo filosófico, el papel del Estado frente a la anarquía del sistema internacional coincide con las posturas realistas: el conflicto interestatal está siempre latente debido a la naturaleza soberana del Estado. No obstante, el liberalismo buscaba la configuración de un organismo supraestatal que regulara el comportamiento de los Estados y, consecuentemente, la Sociedad de Naciones fue creada para bloquear las funciones negativas del Estado y garantizar la seguridad internacional (Hobson, 2003).

A pesar del fracaso del intento de la Sociedad de Naciones por pacificar los diferentes territorios del mundo, la idea de la seguridad permaneció enmarcada en la cuestión de lo militar. Esto limitó su ámbito de análisis, pues se dio una aproximación al entendimiento de las "situaciones de peligrosidad" controlables únicamente a través

de la política estatal. En consecuencia, los políticos de cada país limitaron sus discursos sobre la seguridad a los aspectos relacionados con la identificación nacionalista. El legado institucionalista de mantener el orden doméstico a través de una economía política que sirviera a la reproducción del sistema capitalista se mantenía con suficiente resistencia. Proponer en esa época un nuevo rumbo para el concepto de la seguridad no era una opción viable, ni en la teoría ni en la práctica, pues este concepto se guiaba por tradiciones institucionalizadas difíciles de cambiar.

Con el transcurso de los años, y debido a los nefastos resultados de la Segunda Guerra Mundial, la lógica del pensamiento acerca de la seguridad empezó a emplear otras dimensiones de análisis: se introdujeron temas económicos, políticos, sociales y ambientales. Sin embargo, en la actualidad aún no existe un consenso sobre qué significan estas ampliaciones del concepto. La naturaleza del concepto plantea grandes dificultades a la construcción de una definición consensuada.

Buzan elabora una recolocación de las diferentes definiciones elaboradas con la intención de clarificar y acotar los fines de las políticas de seguridad. Tales definiciones señalan las dimensiones principales relacionadas con la cuestión de la seguridad nacional, en especial

> la centralidad de los valores, la duración, la intensidad de las amenazas, y la naturaleza política de la seguridad como objetivo de Estado. Pero también pueden provocar el perjuicio de darle al concepto una apariencia de consistencia que no se merece (Buzan, 2008, p. 18).

En efecto, la constitución conceptual de la seguridad depende de una multitud de factores que alteran su significación y su relación con el autor de que se trate. La definición se establece a partir de un interés ideológico y desde un lugar de enunciación; por ejemplo, la academia o el gobierno, Europa o América Latina.

La idea contemporánea de seguridad parece ser demasiado compleja, es muy difícil de definir y genera debates interminables. Se requiere de "un análisis teórico para identificar los límites de su aplicación, las contradicciones en las que incurren y la importancia que puedan tener para [los actores relacionados] las innovaciones" (Buzan, 2008, p. 8). Las visiones contemporáneas insisten en superar la retórica clásica, enmarcada en la cuestión de la seguridad nacional, incluyendo otros ámbitos de actuación, como el ámbito internacional, y otras condiciones del entorno global. Esta superación se sustenta en la identificación del debate epistemológico de la seguridad. Una primera distinción proviene de la concepción objetiva, se trata de la distinción material del fenómeno, sea la amenaza o las capacidades del otro. Una segunda distinción es de carácter subjetivo, en principio relacionada con los lazos normativos e históricos entre actores, y luego con una interpretación de los componentes objetivos. Una tercera distinción es discursiva, declara la imposibilidad de entender la seguridad objetiva y subjetivamente y, consecuentemente, se entiende que la seguridad emerge discursivamente cuando se ponen amenazas a la agenda política (Buzan & Hansen, 2009, pp. 33-34). De esta forma, se infiere que la seguridad es un concepto primordialmente intuitivo que depende de objetos y eventos externos para su definición. Por antonomasia, la seguridad se define en tanto que afecta a los actores.

Además, Buzan comenta que la seguridad concierne principalmente al destino de la humanidad como colectivo, y solo después al ser humano como individuo. Por ejemplo, se puede señalar a las pandemias como hechos que pueden afectar la supervivencia del planeta si no se previenen a tiempo. Esta clase de problemas deben estar presentes en la agenda de seguridad de los Estados y, además, en el concepto mismo. Así como las epidemias o las pandemias afectan a los sistemas de salud de los países en los que se dan, a corto y largo plazo

también afectan otras esferas, como sus sistemas económicos y las interacciones sociales. De este modo, según la teoría de los complejos de la seguridad, hay cinco factores que afectan la seguridad de la humanidad como colectivo:

- Militares, que se refieren a la interacción de las capacidades armadas defensivas y ofensivas;
- políticos, traducidos en la estabilidad organizacional de los Estados, es decir, sus mecanismos de gobierno y las ideologías que dan soporte a la legitimidad;
- económicos, relacionan la idea de los recursos y los mercados que dan lugar a la realización material de las necesidades de la población;
- "la seguridad de la sociedad se refiere a la sostenibilidad, dentro de condiciones aceptables de la evolución, de los patrones tradicionales de lengua, cultura y religión e identidad nacional y costumbres; la seguridad medioambiental se refiere al mantenimiento de la biosfera local y global como sistema esencial de sustento del cual dependen todas las actividades humanas. Por tanto, el concepto necesita una definición inclusiva, pues es indispensable para las Relaciones Internacionales" (Buzan, 2008, p. 20).

Estos factores tienen una relación necesaria con la vida y la seguridad de los individuos. Así entendida, la seguridad se puede ver amenazada incluso por la actividad del mismo Estado. Las acciones de las diferentes organizaciones gubernamentales y las organizaciones no gubernamentales serán esenciales para enfrentar el problema de la seguridad desde un nuevo enfoque porque el más reciente objeto de la seguridad demanda acciones diferentes para garantizarla. Dependiendo de la especialidad de estas organizaciones, ellas aportarán

nuevas ideas para ampliar el concepto de seguridad y dirigirlo hacia ideas que se adapten mejor a las necesidades de las poblaciones. Así, se podrá perseguir efectivamente la seguridad en todos los ámbitos, y no solo en el ámbito de las capacidades y acciones militares.

Los dilemas de la seguridad identificados a partir del riesgo

Con el cambio en la concepción de la seguridad, también el lenguaje ha dado un giro lingüístico que se refiere a la identificación de riesgos sociales. Si las seguridades contemporáneas se enfocan en la protección de las sociedades y del individuo, los analistas y académicos de las relaciones internacionales deben enriquecer sus consideraciones con las teorías sociológicas y de la filosofía política. En la comprensión del funcionamiento de las sociedades y las relaciones de los sujetos con la sociedad, a través de las teorías de sistemas, de la teoría del actor-red o de la teoría de los campos del poder, se encuentran asociaciones e interacciones novedosas que atañen a la seguridad. El análisis sociológico de Ulrich Beck sobre la sociedad del riesgo da una respuesta alternativa al problema de la dependencia de las relaciones internacionales al análisis de las relaciones societales y domésticas.

En primera instancia, se debe mencionar que, debido al reparto de los riesgos y el incremento de estos, surgen las situaciones sociales de peligro. En ellas se evidencia que la desigualdad es un factor detonante de la inseguridad. Para un análisis de estos factores, Beck (1998) sugiere ver cómo quienes producen los riesgos en un primer momento también se ven afectados por ellos en un segundo. Surge allí lo que él denomina el efecto búmeran: nadie se escapa de los peligros, incluidos los de salud, de propiedad o de ganancia. Veamos el caso de

la contaminación de las fuentes de agua, esta no solo afecta a los bosques y a las diversas especies animales que habitan en ella, sino que también puede reducir el valor económico de la tierra.

Aunque parecería que solo se esperan consecuencias negativas con los riesgos, y que ellos no nos permiten lograr efectos positivos, hay sectores que de cierta manera se benefician de su existencia. Los riesgos no tienen una finalidad concreta, pero ponen en una encrucijada ética y política a los métodos y los medios para responder concluyentemente. A diferencia de otras necesidades, como el hambre, que se puede saciar con la acción directa de la alimentación, los riesgos civilizatorios, que son causados por la sociedad industrial y la operación extensiva del capitalismo, ponen a los humanos en una situación de extremo peligro pero no tienen una respuesta sencilla ni inmediata.

En medio de la complejidad del riesgo, algunos actores con capacidades superlativas de acción pueden sacar provecho de las transformaciones y de sus costos. Un ejemplo definitivo es el modelo del capitalismo verde, cuyos orígenes se relacionan con la idea de la economía verde y, en general, con la retórica que aboga por la posibilidad de una solución para los problemas ambientales sin dejar atrás los temas del desarrollo económico y social. Este capitalismo se plantea desde dos ideas fundamentales. La primera consiste en incentivar líneas de producción menos dañinas para el medio ambiente. La segunda se basa en la posibilidad de usar el mercado como una herramienta para resolver los grandes problemas ambientales. Este discurso, al que acuden muchas empresas como una imagen identitaria, pero que en sus prácticas no implica cambios trascendentales, no solamente no cambia los modos de producción, sino que profundiza las formas de explotación laboral y de contaminación ambiental.

Igualmente, factores asociados a los riesgos, como la ineficiente distribución de la riqueza, pueden ser determinantes para los dilemas

de la seguridad. Por ello, los ricos y los poderosos tienen la capacidad de adquirir seguridad respecto al riesgo, mientras que las personas de menos recursos se enfrentan a una más amplia concentración de riesgos. Por ejemplo, es mucho más grande el riesgo de mantenerse desempleado si no se tiene la educación suficiente para adquirir un buen empleo. Así mismo, los daños que producen las industrias se reparten de manera desigual debido a que algunos profesionales se ven más expuestos a diversas sustancias tóxicas, al igual que los habitantes de las zonas aledañas a esas fábricas.

Aunque algunos elementos tóxicos, o diversas condiciones a las que se encuentra expuesto cualquier individuo en cualquier parte del mundo, quisieran enfrentarse con el poder adquisitivo suficiente, o con la posesión de elementos que sirvan para protegerse de las amenazas y riesgos existentes, la mayoría de las veces esto no se puede realizar debido a que algunos riesgos son invisibles y su expansión no se puede controlar. Es más difícil evitar la propagación de los riesgos de la obra humana porque, aunque buena parte de ella haya sido creada gracias a desarrollos científicos, el ser humano pierde el control de fenómenos que entran en contacto con la complejidad.

Las consecuencias específicas de pertenecer a una clase también se evidencian en las capacidades para enfrentarse a las situaciones de riesgo. Una persona de bajos recursos tiene más problemas en la elección de su sitio de vivienda, su alimentación o su educación. Desafortunadamente, la pobreza expone al individuo a la posibilidad de un mayor riesgo. Algunos riesgos se podrían evitar fácilmente si se contara con mejores servicios públicos y una inversión pública más eficiente (Beck, 1998).

La desigualdad se evidencia aún más en casos extremos, en los que se requiere del apoyo total de los aparatos estatales. Cuando estos no funcionan correctamente, y por ende presentan grandes déficits,

afectan especialmente a aquellas capas de la población que no tienen la capacidad económica para soportar el riesgo. En este sentido, se encuentran en conflicto dos tipos de contratos sociales que fundamentan la sociedad moderna, el Estado y el mercado, para dar respuesta a la situación riesgosa. La contradicción fundamental entre uno y otro pone en evidencia la indefensión del Estado frente al funcionamiento de la economía. El Estado protege prioritariamente la acumulación del capital, en vez de la seguridad de las poblaciones más vulnerables. Es interesante subrayar que este movimiento se justifica discursivamente desde la postura de defensa de la estabilidad del sistema; el sacrificio de algunos para el beneficio de todos.

A causa de la presencia de los riesgos, aparecen nuevos conflictos sociales. Estos, debido a la sociedad de mercado desarrollada, se pueden convertir no solo en riesgos sino en oportunidades de mercado. En este punto hay una parte de la población que se ve afectada por los riesgos, ya que no tienen los recursos para adquirir las herramientas básicas o medicamentos, en contraste con la parte que sí se ve beneficiada económicamente. De este modo, dentro de la sociedad del riesgo están presentes quienes pueden producir la definición de riesgo y quienes la consumen. Se decide también cuáles de ellos se deben ocultar o revelar.

Beck afirma que la sociedad del riesgo se caracteriza por la *pauperización de la peligrosidad*, opuesta a la clásica pauperización material caracterizada por los académicos anarquistas y marxistas del siglo XIX. En la pauperización actual, nos encontramos con el problema de "que la latencia del riesgo es un mecanismo atemorizante, un *hecho a la expectativa*" (Beck, 1998, p. 58). Beck se está refiriendo a la emergencia de una especulación del peligro sustentada en un conocimiento científico, sólido y cuantitativo aparente que dirige a las masas a comportamientos programados.

Todo lo anterior lleva a que los peligros invisibles se vuelvan visibles. Así como los daños a la naturaleza, causados por el smog o por distintos químicos producidos por las industrias, se vuelven más perceptibles a la vista de toda la comunidad internacional; los virus también lo hacen, pues ya no solo afectan a una pequeña comunidad poco conocida, sino que tienen la capacidad de traspasar fronteras en cuestión de horas. Se empiezan a crear así políticas públicas para la prevención de este tipo de enfermedades, pues las campañas de prevención son más fuertes. De todas formas, algunas veces estas tienen una corta duración, duran mientras el problema está bajo la lupa internacional, pero luego empiezan a difuminarse hasta que se olvidan.

En contraste, para evitar los problemas que pueden surgir debido a la modernización, se pueden unir grupos de personas, pertenecientes a cualquier clase social, profesión o etnia, con el fin de contrarrestar las amenazas y hacer algo para detenerlas. La procedencia del grupo no es necesariamente relevante; se busca una unión para lograr el objetivo de actuar ante la situación de riesgo. Se produce una conciencia genérica y reactiva al problema, sustentada en bases éticas e ideológicas que permiten su reproducción. Sin embargo, esta respuesta corresponde a la dominación del miedo a la latencia. Alrededor de estos mecanismos se organiza la vida social y las actividades políticas.

¿Cómo se resuelve la ansiedad de la latencia? Beck ofrece dos caras del final de la latencia: el riesgo y su percepción. Los riesgos se alimentan de sus percepciones: no solamente la percepción respecto al lugar de su producción, sino respecto la manera de su propagación (Beck, 1998). Si la percepción es más grande que las condiciones y capacidades del riesgo, las percepciones del riesgo pueden ser más peligrosas que el riesgo mismo. Es decir, hay una relación fundamental entre el poder y el conocimiento. Por eso se observa que quiénes

manejan los medios de comunicación tienen un control sobre la propagación y la gestión de los riesgos.

La seguridad y el riesgo: ¿Existe una resolución epistemológica?

Los factores mencionados anteriormente han impactado profundamente en la conciencia política, tanto de los individuos como de las instituciones. Estos factores se perciben como sucedáneos en el tiempo y en el espacio, y determinan el futuro de las investigaciones en relación con el dilema de la seguridad. Actualmente, según Palomino et al. (2019), ningún Estado puede considerarse exento de las amenazas a la seguridad y, por el contrario, ha emergido una nueva conciencia política sobre el hecho de que los impactos negativos derivados de dichas amenazas tienen unas consecuencias inmediatas, y difíciles de controlar, en otros lugares del mundo.

La idea de una afectación mundial producto de las nuevas amenazas del mundo globalizado ha facilitado nuevas dinámicas de interrelación política entre Estados y otros actores políticos y sociales de relevancia internacional. En consecuencia, esto ha dado lugar al desarrollo de nuevas formas de cooperación y a la coordinación de planes y acciones de política pública para gestionar los riesgos derivados.

Las primeras manifestaciones con respecto a esta nueva forma de protección del entorno tienen como su hito fundamental el Protocolo de Kioto, creado en 1997. Este es un precedente para las acciones civiles organizadas y la creación de nuevas asociaciones y movimientos sociales para la defensa de los derechos animales y de los recursos naturales. Igualmente, es un precedente para la formulación de leyes nacionales e internacionales para la protección medioambiental. Estos

esfuerzos significativos, con respecto a la cuestión global e interdependiente del riesgo, han demostrado la creación de una conciencia internacional sobre la simultaneidad y correlación de las amenazas al medio ambiente. Esta conciencia demuestra a su vez la posibilidad de construir nuevas lógicas relacionadas con una visión política de los riesgos globales.

De igual manera, se observa el surgimiento de nuevas tendencias del mercado, como respuesta a las crisis financieras de la banca mundial en el siglo XXI, que han dado lugar a la creación de iniciativas como los mercados verdes, también denominados biocomercio. Estos están basados en la idea de generar productos, bienes o servicios que generen beneficios ambientales directos, incorporando prácticas ambientales innovadoras. A la postre, se han fortalecido y expandido las prácticas y los modelos de la economía cuyo objetivo es aumentar las expresiones de solidaridad en toda la sociedad. Con esto, se ha dado un énfasis especial a los sectores que se encuentran en situación de vulnerabilidad, caracterizados por el desempleo, pobreza y marginación.

Estas respuestas y resistencias sociales emergen como expresiones del escepticismo y de la negación de la universalidad de la racionalidad tecnocientífica que sustenta el incremento de los riesgos civilizatorios (Beck, 1998). Este movimiento se proyecta desde una audiencia que intuye y experimenta directa e indirectamente el crecimiento de los riesgos para la dignidad humana y la calidad de vida. En efecto, los países denominados subdesarrollados son los ejemplos por antonomasia de lo latente y de los riesgos factuales. La combinación de contaminación ambiental y hambruna desemboca en el cuestionamiento profundo de la racionalidad detrás del funcionamiento de los sistemas económicos y de la conformación de las sociedades industriales y consumistas. Ahora, si se quiere, la emergencia de estas

conciencias y organizaciones también resulta ser una amenaza y un riesgo para el sistema mismo.

Si volvemos a las distinciones epistemológicas de la seguridad de Buzan, mencionadas al principio de este escrito, en conjunción con la teoría de la sociedad del riesgo de Beck, se encuentran coincidencias claras entre las distinciones y su primacía sobre otras. Ya no es posible hablar con claridad prístina de la objetividad de los riesgos, sino de la relación del sujeto con el riesgo. Es más, la subjetividad del riesgo tampoco es fácil de distinguir: la dominación y la manipulación de la información no permite que el sujeto perciba el riesgo con transparencia. Allí es donde las variables de poder, saber e información son esenciales, tanto para conducir las percepciones como para el surgimiento del escepticismo.

No es posible concebir la seguridad sin los riesgos. Como bien lo afirma Buzan, la seguridad es un concepto que depende de un objeto externo: el riesgo. Además, la seguridad es considerada desde el sentir de los sujetos en relación con los objetos de riesgo. Esta relación precluye la experiencia individual y se corresponde con la historia de la dominación de la naturaleza por parte del hombre, así como de la dominación de otros hombres. En consecuencia, Beck (1998) alude a los factores de seguridad como resultados de la praxis, como la retroalimentación reflexiva de la experiencia.

Cuando el liberalismo filosófico afirma la necesidad de la existencia del Estado, se concibe primariamente un estado de naturaleza de los hombres, ellos son conflictivos y violentos. Por su parte, cuando se prescribe la anarquía internacional como inherente a las relaciones entre Estados, la praxis de la guerra internacional trae el riesgo inevitable de la repetición. El desarrollo de técnicas y tecnologías está íntimamente conectado al miedo del ser humano a la hibernación o a

estados latentes, de espera, pensemos en el desarrollo de las vacunas o en los seguros de vida.

El miedo instintivo y primitivo, que retroactivamente se racionaliza, permite y obliga al desarrollo de Estados y formas de seguridad. Hoy se ve cómo los riesgos trascienden las distinciones binarias fundamentales formuladas por la filosofía y las ciencias (Beck, 1998). Se entretejen relaciones complejas para el entendimiento renovado de los riesgos sistémicos, a su vez que se *unifican* los trabajos para enfrentarlos. En última instancia, el enfrentamiento a los inminentes riesgos civilizatorios conlleva a la confrontación del conocimiento científico y la praxis científica, y a la subsecuente exploración metodológica y práctica que permita solucionar problemas y reducir los riesgos más fundamentales.

Si la sociedad del riesgo está basada en el conocimiento especulativo, su relación con la seguridad es exploratoria y procesual, identitaria y contingente. En esta discusión, el concepto de securitización se vuelve esencial porque incluye el proceso de selección de los temas que se vuelven relevantes para la seguridad. Buzan y Weaver elaboran la teoría de la securitización a partir del fenómeno de adquisición de relevancia pública de un tema considerado como una amenaza para la supervivencia (Peoples & Vaughan-Williams, 2010). A través del proceso de securitización, el tema pasa de estar no-politizado a estar politizado, y luego es securitizado. Pasa de ser un tema irrelevante para la deliberación pública a ser una amenaza existencial. El proceso inverso se conoce como desecuritización. Por medio de este se pretende cambiar el orden de prioridades de una sociedad o del Estado (Peoples & Vaughan-Williams, 2010).

Para cada proceso hay temáticas generales y públicos interesados, agendas públicas e ideologías que intermedian en la deliberación.

En cada sociedad y Estado, las cualidades culturales y las normas sociales conducen a la determinación de los riesgos más importantes para los individuos y los grupos. En especial, cuando las contingencias políticas aumentan las alarmas sobre esferas interdependientes, la irritación de ciertos subsistemas podría conducir a la desnormalización de su funcionamiento o a la disrupción de las jerarquías. En otras palabras, respecto a la pauperización de la peligrosidad, si la percepción del riesgo produce un hecho que genera expectativa, se controlan las expectativas sociales y la organización de los grupos alrededor del miedo a la latencia.

Se debe concebir la manera como se organiza el poder en la sociedad: los lugares de producción de la información, de emisión de las comunicaciones y de efectuación de las respuestas a los riesgos. En un caso concreto, las universidades y los centros de investigación producen conocimiento científico y divulgan los resultados a sus pares; por su parte, algunos medios de comunicación traducen la información científica para un público más amplio. Por ejemplo, si un grupo de investigación de una universidad prestigiosa descubre la correlación entre el consumo elevado de azúcar y la mortalidad infantil, los grupos económicos involucrados con la producción de azúcar o de productos azucarados presionan para desmentir el estudio; o intentan disuadir a los consumidores para que no se abstengan de consumir. Por otra parte, los ciudadanos preocupados pueden organizarse para controlar el consumo de azúcar en infantes, su distribución o su producción. Otros ciudadanos pueden mostrarse escépticos e ignorar la recomendación de los expertos. Mientras los primeros se posicionan como un grupo moralmente superior, los segundos pueden argumentar la relatividad del conocimiento científico, o aludir a una conspiración económica. Las empresas podrían innovar, usando productos con menos azúcar o con estevia; alternativamente, podrían bajar los precios para

aumentar la demanda de los productos en circulación. Este es un caso de salud pública y de producción industrial en el que se evidencia el influjo de información, que pone en evidencia la latencia del riesgo, y la resistencia que ofrecen los sectores afectados para salvaguardar su reproducción. La salud de los infantes se securitiza al poner en discusión a los grupos de consumo afectados por el debate. El tema puede incluso llegar a instancias legislativas e institucionales.

Conclusión

¿Hacia cuáles acciones podría conducir el debate teórico de la seguridad contemporánea? Al enlazar la noción de riesgos de Beck con la de securitización de Buzan y Waever, se despliegan varias posibilidades de observación de los fenómenos sociales y políticos que ordenan la sociedad o que imponen desafíos a la normatividad social. Es claro que estas observaciones tienen consecuencias cognitivas, sobre la relación del sujeto con la naturaleza y la sociedad. Los riesgos y la sensación de seguridad controlan las inclinaciones comportamentales e ideológicas del sujeto. Se da así una interacción sustentada en el miedo. Si el sujeto le teme a lo desconocido, siente más presión sobre su vida, sabe que en cualquier momento un evento anunciado pueda suceder. Por supuesto, otros pueden aprovechar esta vulnerabilidad del sujeto para alterar las percepciones de la realidad u ofrecer respuestas.

Cuando se trata de la seguridad, se busca conectar al concepto con un objeto externo que, asimismo, está ligado a la intuición de un observador sintiente. Así que la seguridad no solamente está ligada al riesgo, sino a quién la percibe: un Estado, una comunidad, un individuo. Este entrelazamiento, en los distintos niveles de interacción, tiene unas implicaciones éticas para el ejercicio del poder. Para una ética de los riesgos, se debe considerar que "la insistencia sobre la sucesión

de causas no probadas potencia los riesgos" (Beck, 1998, p. 69). Es decir, conducir a determinados grupos sociales hacia acciones riesgosas sin tener una completa certeza no es otra cosa que experimentar con algunos grupos humanos.

Por otra parte, la atribución causal de consecuencias negativas a factores externos (para quitar responsabilidad a ciertos agentes) es una práctica bastante usada para enfrentar el riesgo. Ella hace uso de la falibilidad de los razonamientos y de los métodos científicos. Lo mismo sucede con el uso de las estadísticas y de los métodos probabilísticos, una especie de apuesta de la ciencia para el beneficio de la humanidad. Esos riesgos los experimentamos actualmente. Peligros agobiantes que podrían provenir de prácticas irresponsables de producción industrial masificada o de cambios naturales del planeta. Precisamente con este argumento se procede a buscar la ética dentro de las posiciones de los actores involucrados en la provisión de seguridad y el manejo los riesgos. Estos actores deberían asumir una posición responsable con la humanidad y con el planeta. Beck, en complemento, afirmaría la llegada del final de la contraposición entre naturaleza y sociedad (Beck, 1998), porque nos hemos encontrado con un mutualismo artificial: nosotros la necesitamos y ella nos necesita. Tal vez sea esa arrogancia la que nos lleve a nuevos riesgos, porque la humanidad necesita cuidar más a la naturaleza, en vez de servirse de ella.

Referencias

Beck, U. (1998). *La sociedad del riesgo: hacia una nueva modernidad*. Paidós Ibérica.

Buzan, B. (1981). Change and insecurity: A critique of strategic studies. *Change and the study of international relations: The evaded dimension*, 155-172.

Buzan, B. (2008). *People, States & Fear: An Agenda for International Security Studies in the post-Cold War Era*. ECPR Press.

Buzan, B., & Hansen, L. (2009). *The Evolution of International Security Studies.* Cambridge University Press.

Buzan, B., & Waever, O. (2003). *Regions and Powers: The Structure of International Security.* Cambridge University Press.

Hobson, J. (2003). *The State and International Relations.* Cambridge University Press.

Marquardt, B. (2009). *Historia universal del Estado* (Tomo 2). *El Estado de la paz interna y de la organización judicial en el caso de Europa (1495-1775)*. La Carreta Histórica.

Palomino, W., Cerón, A. y Barreto, R. (2019). *Geoeconomía: Nuevas amenazas a la soberanía hemisférica*. Escuela Superior de Guerra.

Peoples, C., & Vaughan-Williams, N. (2010). *Critical Security Studies.* Routledge.

Capítulo 2

Seguridad humana, reflexiones desde los paradigmas interpretativos[1]

Alejandra Cerón R.*
Carlos Alberto Hoyos**

1 Capítulo de libro resultado del proyecto de investigación titulado *Impacto de las políticas de Seguridad Integral en el desarrollo y gestión del componente de investigación del currículo* MADGSI, de la línea de investigación Seguridad Integral del grupo de investigación CIPAER, con código COL 0093003, de la Escuela de Postgrados de la Fuerza Aérea Colombiana.

* Doctora en Estudios Políticos y Relaciones Internacionales de la Universidad Nacional de Colombia. Magíster en Gestión de Organizaciones de la Université du Québec à Chicoutimi (UQAC), Canadá. Socióloga de la Universidad Nacional de Colombia. Docente e investigadora. Correo electrónico: luz.ceron@epfac.edu.co

** Profesional en Relaciones Internacionales y Estudios Políticos de la Universidad Militar Nueva Granada. Correo electrónico: u0902042@unimilitar.edu.co

CÓMO CITAR

Cerón R. A., & Hoyos, C. A. (2020). Seguridad humana, reflexiones desde los paradigmas interpretativos. En Y. Rico, D. López Cortés, & A. Cerón R. (comps.), *Enfoques y gestión en Seguridad Integral* (pp. 45-68). Escuela de Postgrados de la Fuerza Aérea Colombiana. https://doi.org/10.8667/9789585996199.02

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

CAPÍTULO 2.
Seguridad humana, reflexiones desde los paradigmas interpretativos

https://doi.org/10.8667/9789585996199.02
Bogotá, Colombia
Noviembre, 2020

RESUMEN

La noción de *seguridad humana* se relaciona con el respeto a la vida, los principios de integridad del individuo y el desarrollo socioeconómico. Estas relaciones impactaron el pensamiento tradicional de la seguridad, enfocado principalmente en la visión de protección del Estado. Así, se plantearon nuevas dimensiones de acción institucional que tengan como objetivo la protección del sujeto. En los ámbitos académicos, el concepto de *seguridad humana* empezó a aceptarse como una superación del Estado de pacificación. Se inició a proponer entonces un análisis enfocado en la intervención de los intereses económicos en el medio ambiente, en el uso de nuevas tecnologías, en la urbanización, entre otros fenómenos que tienen un impacto en la estabilidad y seguridad de un contexto amplio y complejo. Las consecuencias y las acciones en estos ámbitos traen nuevas amenazas para las sociedades humanas, dado que confluyen con otros factores que a la postre ponen en peligro la estabilidad del planeta.

PALABRAS CLAVE

Estado; interpretación; seguridad humana; seguridad internacional; sociedad del conocimiento.

Introducción

El cambio paradigmático de la seguridad nacional a la *seguridad humana* se explica a partir de la desestatización de la seguridad en tiempos de globalización. En este texto, partimos de la hipótesis de que el Estado ha perdido relevancia como el ente que concentra el poder y ha dejado de ser el tema central de discusión en la academia y en las políticas. A partir de dicha hipótesis, se pretende explicar cómo el concepto de *seguridad humana* se convierte en el más adecuado para describir la realidad compleja y para actuar de forma interagencial, interestatal y societal. Este ejercicio interpretativo es esencial para apoyar proyectos de investigación sobre la seguridad contemporánea y para integrar reflexiones sobre acciones concretas.

Este capítulo está compuesto por una reflexión introductoria sobre el surgimiento histórico de la *seguridad humana* y sobre la composición conceptual de esta propuesta teórica. Luego, se analiza el lugar del Estado en la *seguridad humana* y se cuestiona si él es suficiente para atender las necesidades de seguridad contemporáneas. En el apartado siguiente, se presentan otros actores económicos y sociales que comparten los escenarios de interacción con el Estado. Por último, se concluye el texto mostrando la necesidad del cambio de paradigma.

¿Cómo llegamos a la *seguridad humana*?

En el trascurso del siglo XXI, la comunidad internacional vio un cambio significativo en la caracterización de los fenómenos relacionados con la seguridad. Durante el siglo XX, el marco de referencia utilizado para comprender la naturaleza de la seguridad en las dos guerras mundiales

y en el período de la Guerra Fría comprendía solamente los límites de la seguridad nacional. El concepto de seguridad internacional se basaba en un sistema de Estados alineados por los intereses hegemónicos de los centros políticos y económicos, Estados Unidos y la antigua Unión de Repúblicas Socialistas Soviéticas.

En los últimos años del siglo XX, se presentaron distintas formas de conflictos e incertidumbres a nivel mundial que desbordaban la capacidad de análisis de los marcos conceptuales clásicos del realismo político. En estos nuevos escenarios de la seguridad participaron actores y grupos de diversa índole. A su vez, los fines y los medios que propiciaron estos escenarios derivaron en riesgos para la seguridad que demostraron la poca preparación y capacidad institucional de las autoridades para combatir diversas prácticas y sucesos. Aunque predominaron los hechos relacionados con la criminalidad organizada, los nuevos desafíos a la seguridad provenían de la construcción de nuevas lógicas que solo habían sido planteadas de manera tangencial por las políticas de Estado.

La Guerra del Golfo en contra de la República de Irak en 1990, el genocidio en Bosnia en 1995, la Guerra de Kosovo en 1998, los atentados a las Torres Gemelas y la consecuente respuesta de los Estados Unidos con la Guerra de Afganistán en el 2001 fueron los hechos sobresalientes que mostraron el cambio cualitativo de los dilemas de la seguridad. Se presentaron nuevas formas de coalición, diferentes a las configuraciones estatales, así como nuevos intereses por el control de los territorios para su explotación económica a través de redes del transnacionalismo. Las consecuencias nefastas que todos estos hechos tuvieron sobre la población civil crearon nuevos desafíos y, con ellos, surgió la necesidad de pensar en nuevos enfoques de interpretación y en una nueva agenda de investigación respecto al dilema de la seguridad.

Ante este panorama mundial, fue necesario un debate en torno a la reconceptualización de la seguridad. Este estuvo cimentado en el esfuerzo por comprender las nuevas relaciones sociales que daban lugar a escenarios caracterizados por la complejidad de factores y actores intervinientes. En las múltiples visiones que inspiraron la discusión de la época sobresalía la necesidad de pensar la seguridad mundial en función de proteger a los grupos sociales que se veían inmersos en un contexto de conflictos y amenazas constantes que terminaron por convertirlos en víctimas, lo que mostró su vulnerabilidad.

Fernández (2006) hace referencia a la *seguridad humana* desde una perspectiva *humanocéntrica*; una óptica más amplia, dado que este paradigma está basado en el desarrollo humano y se enfoca en aspectos que afectan alguna de las siete dimensiones de la seguridad. Asimismo, asegura que el espectro de amenazas a la seguridad de los Estados no coincide con el de las amenazas a la *seguridad humana* Esto se debe a un entramado de cambios en las últimas décadas por motivo de la globalización, las nuevas formas de comunicación y los movimientos migratorios. Estos factores han afectado los límites y la influencia de los Estados y han provocado el replanteamiento de las nociones fundamentales de la seguridad, como su objeto, su definición, las nuevas amenazas, etc.

Mientras que las concepciones clásicas de la seguridad sostienen que se debe proteger la soberanía y la integridad territorial del Estado, la concepción más amplia integra el eje de la solidaridad, que otorga a la seguridad la perspectiva humanista de buscar el bienestar para la población completa. Esto es, asegurar el acceso a cada persona a una justa cantidad de servicios esenciales para vivir y asegurarse de que se respete su dignidad y su vida.

Como un aporte diferencial en la conceptualización de la seguridad, en 1994 el Programa de las Naciones Unidas para el Desarrollo

(PNUD) presentó su informe sobre Desarrollo Humano (ONU, 1994). Este describía cómo la desaceleración del crecimiento económico mundial traía consecuencias severas para el bienestar de la población en general. En el informe se ilustraron situaciones históricas como la expansión progresiva de la pobreza extrema a nivel global y el impacto negativo que la acción humana con fines económicos tenía sobre el medio ambiente.

Para plantear políticas y planes de crecimiento económico, enfatizó el PNUD, era necesario mitigar los conflictos del mundo a partir de un nuevo enfoque de las relaciones de cooperación y desarrollo entre las naciones. La proyección del PNUD requería incluir como prioridad la seguridad humana, definida en términos de la multiplicidad de variables que intervenían en ella:

> La seguridad se encuentra unida al conflicto en otra dimensión: los problemas ambientales, la amenaza de enfermedades, el desempleo, el hambre, las violaciones de los derechos humanos, el narcotráfico, etc., son los problemas de las personas en particular, y de los Estados, en general. La seguridad humana, no es un concepto defensivo, como la seguridad territorial o militar, sino un concepto integrador, que reconoce con carácter universal la prioridad de la persona (ONU, 1994).

En su discurso, el PNUD abogó por una nueva postura del mundo frente al entendimiento y la expresión del conflicto, ya que sus consecuencias sobre la humanidad eran catastróficas. Se trataba del tránsito del pensamiento político de la *seguridad nuclear* al de la *seguridad humana*, definida como "el derecho a vivir libre de temor y de miseria" (Fuentes, 2012, p. 33).

A partir de estas reflexiones, en 1994 la Organización de las Naciones Unidas (ONU) empezó a referirse a la *seguridad humana* como

un enfoque que incluye temas como el respeto a la vida y otros principios de integridad del individuo. Esta característica impactó el pensamiento tradicional de la seguridad, enfocado principalmente en la visión del Estado, y abrió las perspectivas de acción a todas las personas, organismos e instituciones cuya labor sea la protección del sujeto social; un sujeto con proyectos de vida, necesidades biológicas y costumbres religiosas y seculares.

La noción de *seguridad humana*, en los ámbitos académicos, empezó a aceptarse como una superación del estado de pacificación (entendido meramente como la ausencia de violencia):

> La seguridad empieza a ser contemplada no solo desde el punto de vista de ausencia de violencia física sino, de garantía de derechos, oportunidades y calidad de vida de los asociados, condiciones afines al bienestar y desarrollo integral de cada ser humano (Ariza, 2010, p. 33).

De forma similar, y desde una óptica más cercana, la Secretaría Distrital de Planeación de Bogotá (Sánchez, 2017), que se basa en los conceptos del PNUD, considera que la *seguridad humana* tiene un carácter multidimensional, puesto que procura garantizar un máximo nivel de bienestar y una serie de libertades a todos los seres humanos. Entre las dimensiones involucradas se resaltan las siguientes:

1. Seguridad económica: garantizada por medio de la protección frente a amenazas como el desempleo y la pobreza crónica, además de la garantía de un ingreso justo.
2. Seguridad alimentaria: con esta se busca la protección frente a amenazas como la hambruna, mediante la accesibilidad a alimentos básicos.
3. Seguridad de la salud: protección ante la amenaza de enfermedades; acceso a servicios sanitarios básicos, y servicios de salud.

4. Seguridad ambiental: esta se asocia a la protección frente a amenazas de tipo medioambiental, desastres naturales, además de la protección de los recursos.
5. Seguridad personal: protección frente a amenazas de violencias física o psicológica y de acciones delictivas que pongan en riesgo la integridad personal.
6. Seguridad comunitaria: se asocia a la protección ante amenazas relacionadas con la intolerancia frente a diferencias étnicas, culturales o religiosas.
7. Seguridad política: protección ante amenazas de vulneración de los derechos humanos y derechos civiles (Sánchez, 2017, pp. 7-8).

Este enfoque ha logrado que paulatinamente se les reste importancia a los planteamientos militaristas basados en doctrinas de seguridad nacional. En vez de ello, se adoptan nuevas perspectivas que responden al amplio significado de la *seguridad humana,* la cual vincula los Derechos Humanos (DDHH) con el desarrollo. Además, propone que las amenazas a la seguridad no necesariamente afectan a la figura de Estado, sino a las personas, pues afectan distintas dimensiones de la actividad humana relacionadas entre sí. Por otra parte, Roznai afirma que el concepto "surge a mediados de los años noventa como una respuesta a la orientación neoliberal de los mercados y en medio de unas condiciones históricas que lo vinculan al fenómeno de la globalización" (Roznai, 2014 citado en Muñoz, 2018, pp. 26-27). En este análisis se hace una precisión fundamental sobre el origen ideológico de la *seguridad humana.* Más allá de la retórica de la justicia y de la igualdad, se alude a una necesidad económica de protección de los mercados y del individuo como productor/consumidor.

Con el transcurso del siglo XXI, este enfoque ha inspirado una producción bibliográfica considerable. Las investigaciones enmarcadas en

el análisis propuesto por el concepto de *seguridad humana* deben también adaptar marcos alternativos de interpretación de los problemas, construidos desde las escuelas hermenéuticas de las ciencias sociales. Estos marcos dan prelación a los matices particulares de las amenazas, las relaciones derivadas de los contextos particulares y, consecuentemente, los diferentes planteamientos que pueden derivarse (en términos de políticas y planes de acción del Estado y de las agremiaciones sociales interesadas).

El rol del Estado en el contexto de interpretación de la *seguridad humana*

Como lo menciona David Held (2002), el fin de la Guerra Fría trajo como consecuencia una descentralización de los sistemas de seguridad internacional. En primera instancia, la presencia militar de los Estados Unidos y Rusia en países extranjeros es actualmente mucho menor en comparación al siglo XX. En segundo lugar, la regionalización de los sistemas de seguridad es una tendencia a nivel global que, aunque no funcionan totalmente aislados de la "lógica comunitaria de la seguridad mundial", sí han construido pautas y normas de comportamiento específicas para cada región del mundo. Estas pautas dependen de las condiciones particulares de las regiones y de la inclusión de nuevos actores no estatales en el proceso.

Algunos hechos relacionados con esta forma de descentralización de los sistemas de seguridad a nivel global tienen que ver con el resurgimiento de conflictos regionales basados en reclamaciones identitarias. Como ejemplos de este nuevo patrón de seguridad se pueden mencionar los hechos relacionados con la disolución de los Estados

socialistas y el resurgimiento de reclamaciones de los pobladores de estas regiones basadas en identidades originarias. Así, la disolución de la URSS, Checoslovaquia y la República Federal Socialista de Yugoslavia dieron paso a la expresión de los orígenes étnicos y religiosos de las poblaciones en cruentas guerras locales. El resultado común de estos conflictos fue la extrema violencia y la precaria situación en que tuvieron que permanecer los sobrevivientes.

En esta forma de conflictos, fueron comunes la participación de grupos paramilitares, el tráfico de armas y la financiación de mercenarios, así como la utilización de prácticas terroristas y de nuevas tecnologías para hacer la guerra. Estas últimas hicieron evidente la incapacidad de los Estados para controlar las manifestaciones emergentes y las tensiones e inestabilidad con los bloques regionales vecinos. Para el caso mencionado (el de la disolución de los países del bloque socialista), las naciones de Europa occidental manifestaron abiertamente su preocupación por la inestabilidad política y social de los nuevos países, que generaban en la región un riesgo de conflicto armado latente y un riesgo migratorio. Desafortunadamente, la gran mayoría de esfuerzos de las acciones diplomáticas y democratizantes fueron infructuosos.

Las situaciones de inestabilidad en el globo hicieron manifiesta la necesidad de crear nuevos planes y estrategias en materia de seguridad que permitieran la participación de diversos grupos de interés. Con el liderazgo del Estado, se dio origen a un sistema de seguridad con mayor capacidad para la gestión de riesgos probables. Así, se logró una mayor participación de actores no gubernamentales y se crearon relaciones de interconexión acordes a los escenarios globales (en países en los que varios procesos de descolonización tenían lugar y se estaba dando la formación de nuevos Estados).

Sin embargo, los Estados con una mayor capacidad organizacional fueron los que pusieron las pautas para la toma de decisiones y

las subsecuentes acciones políticas. De esta manera, los Estados más dependientes accedieron a la conformación de redes que permitirían el enlace para la cooperación, protección y crecimiento mutuo, de la mano de organizaciones y movimientos sociales que fueron aumentando con la aparición de nuevos desafíos. Por esta razón, la política actual no solo está encaminada a cumplir objetivos de la política tradicional, sino a hacer frente también a otros factores de vital importancia, como los económicos, sociales y ambientales. Así,

> la contaminación, las drogas, los derechos humanos y el terrorismo se encuentran en un creciente número de aspectos políticos transnacionales que atraviesan las jurisdicciones territoriales y los alineamientos políticos existentes que requieren la cooperación internacional para su resolución efectiva (Held, 2002, p. 25).

Lo anterior es una muestra de que la seguridad, vista como protección del territorio y sus ciudadanos ante amenazas físicas (para enfrentar a las cuales se debe tener una buena organización militar), no responde a las temáticas primordiales en la actualidad. Existen otros desafíos que deben enfrentarse con novedades e innovaciones en los sistemas de seguridad. En otras palabras, el rol del Estado debe transformarse, de una seguridad militarista a una seguridad más amplia que cubra los diferentes aspectos y riesgos de la vida humana.

La multiplicidad de actores en el sistema ha provocado que algunos de estos, como las organizaciones internacionales, tengan mayor presencia en los Estados y generen mayores cambios sociales que sus propios gobiernos. Esto se debe en buena medida a las limitaciones y falencias que ellos poseen en la garantía del bienestar de su población. Sin embargo, en muchos casos son las organizaciones o movimientos cívicos quienes desencajan la posición de entidades estatales y debilitan su poder.

Sin lugar a duda, los Estados aún transitan por procesos organizacionales que conllevan a la creación de nuevos estándares y preocupaciones que pueden convertirse en políticas públicas. Los diferentes sectores influyentes en las políticas, junto con las redes transnacionales, han entrado en un proceso de institucionalización de la seguridad contemporánea. Por este motivo, han surgido nuevos modos de encargarse de la administración de los recursos, de la población, la información y el poder social en diferentes territorios.

Esta interconexión no sería posible sin el desarrollo de infraestructuras y nuevas tecnologías que permiten la transmisión de la información en cuestión de minutos y aceleran la interacción política entre los pueblos, creando vínculos inmediatos entre ellos. Medios como el sistema de telefonía, los vuelos inmediatos y personalizados y la gran infraestructura de internet, sin dejar a un lado las redes sociales y la prensa, han transformado la comunicación política, ya que la información puede traspasar fronteras fácilmente y se permite un acceso y una divulgación moderadamente práctica.

Los nuevos sistemas de comunicaciones, a pesar de sus beneficios en la comprensión de determinados eventos, implican también ciertas restricciones y ambientes de desigualdad en la política global para sectores específicos. Por ejemplo, las diferentes campañas sobre la prevención de enfermedades han contribuido de gran manera a reducir su propagación. También nos han permitido ser testigos de alguna forma de lo que pasa en África o en otros países por diferentes catástrofes o fenómenos. Sin embargo, quien no tenga los medios para informarse, o difundir su experiencia, a su alcance puede verse excluido de este sistema.

Hay un cambio fundamental en la producción económica que afecta el comportamiento del Estado, por sus objetivos políticos y por el manejo de la información. Manuel Castells (2010) describe el cambio

de marco que guiaba a la economía, antes de las revoluciones informáticas, a un capitalismo informacional. Esta transformación está acompañada por un cambio en la concepción del valor económico. Las empresas no buscan más el incremento de la productividad, sino la rentabilidad y el crecimiento del valor de las acciones. Asimismo, las instituciones del Estado buscarían, a partir de estas bases, mantener la competitividad de la economía (Castells, 2010).

Esta era informacional requirió de la adopción de los nuevos consumos tecnológicos y de la tecnificación del trabajo por parte de las estructuras sociales. Esto no implica una contradicción con la economía industrial, sino "una profundización tecnológica de la producción industrial" (Castells, 2010, p. 100). Con el crecimiento de la economía especulativa, a través de los mercados financieros, el objetivo principal es posicionar la empresa dentro de un mercado. Esto requiere de mantener una estabilidad y credibilidad del proceso productivo. La información proveída a los inversionistas busca transmitir seguridad sobre el crecimiento continuo; pero esta misma información puede reducir sustancialmente la confianza y, luego, el valor del producto. Por esta razón, las agencias calificadoras de riesgos toman tanta relevancia hoy.

El rol del Estado en este proceso de cambio, especialmente con la consolidación del modelo neoliberal, es precisamente el de asegurador. No regula, ni interviene más que en lo necesario; debe asegurar que el medio inversionista sea estable y confiable. Reducir conflictos sociales, organizar eficientemente las instituciones públicas y apoyar financieramente los emprendimientos de capital privado. El Estado se muestra hoy como el respaldo del riesgo de la economía especulativa.

Sin lugar a duda, la importancia del medio ambiente para la seguridad actualmente representa uno de los desafíos más urgentes del Estado y de la comunidad internacional. La influencia del medio

ambiente en la calidad de vida del ser humano es un factor cada vez más visible. Ahora que el ser humano es consciente de los perjuicios de sus actividades económicas sobre los ecosistemas, se da cuenta de que su reproducción trae consigo riesgos y amenazas que afectan al sistema social y económico de cada Estado. Esta situación compleja compromete al Estado a realizar acciones simultáneas, e incluso contradictorias, para satisfacer las demandas sociales de protección del medio ambiente y para respaldar a la economía especulativa y productivista.

El Estado es importante para la *seguridad humana* por su capacidad legal e institucional de organizar la vida social y económica de los pueblos. Además, es definitivamente un aliado del crecimiento económico y del orden interno, a través de las instituciones militares y de la planeación pública de las finanzas. En contraste, la complejización de la seguridad sobrepasa el rol tradicional del Estado frente a los procesos actuales de producción económica, de difusión de la información y de desastres naturales. Entonces, involucrar en la seguridad a otros actores privados y civiles, como muestra de una toma de responsabilidad colectiva, sin depreciar la autoridad del Estado, es una necesidad de nuestra época para satisfacer las exigencias que imponen los riesgos globales y regionales.

El papel de nuevos actores en la *seguridad humana*

El concepto de seguridad es polisémico, muta según el contexto social y político de una época determinada. Ulrich Beck (2002) plantea de manera asertiva que los retos y condiciones que enfrentan las sociedades del siglo XXI tienen nuevos factores determinantes relacionados con los procesos de la globalización.

La aparición de nuevos actores en el sistema internacional ha sido evidente en el marco de la globalización. Esto ha causado un gran impacto en la distribución de poder. Este hacía parte principalmente de las capacidades de un Estado y le brindaba una imagen y posición más impositiva y legítima para hacer valer sus intereses frente a otros Estados que no tenían el mismo nivel de competencia.

La pérdida de poder de los países, que ahora se concentra en nuevas entidades como los poderes transnacionales, organizaciones internacionales, mafias, gestoras de riegos y consultoras, implica un gran desafío en el ámbito comercial. Esto se debe a que la pérdida de poder lleva a pérdidas de las funciones vitales del Estado. Las nuevas instituciones tienen un poder significativo, con el que pueden hacer primar sus intereses pasando por encima de los poderes estatales o alterando la autonomía del Estado.

Ante este cambio en el equilibro de poderes, los Estados mantienen el monopolio del uso legítimo de la fuerza. No obstante, la forma de enfrentar las nuevas amenazas se ha ido desarrollando al paso que aparecen otros actores y estrategias. En definitiva, se dificulta la forma de enfrentar dichas amenazas por la dificultad de su identificación, ya que estas pueden estar presentes y operar en varios países simultánea e intempestivamente. Por esta razón el concepto de seguridad es redefinido en la agenda de cada Estado. Este no solo tiene que enfrentar las amenazas físicas a la comunidad, sino responder a riesgos ambientales, hambrunas, escasez y combatir la propagación de enfermedades (Strange, 1997).

Ante este panorama, el campo de estudio de las Relaciones Internacionales debe ser ampliado. Las empresas transnacionales han adquirido un buen grado de poder para asegurar el control del mercado, lo que confirma que el Estado ya no es el único actor con gran influencia en el sistema. Las transnacionales tienden a distribuir la oferta y

los precios a su conveniencia en el mercado, de modo que otras empresas no puedan competir y que la demanda no tenga diferentes opciones de consumo.

Es claro que la pérdida de la autoridad del Estado no sucede espontáneamente con la globalización después de la Guerra Fría, sino que viene de un proceso de fortalecimiento de otras fuentes de poder y de control de territorios, e incluso de poblaciones. El primer caso que ilustra esto es la presencia de autoridades con legitimidad local, de origen no estatal, y de economías ilegales. El segundo caso es la constitución de la política económica, que se sirve de múltiples autoridades y mercados (Strange, 1997).

En consecuencia, la autoridad de los Estados se reduce también debido a las variaciones en el sistema financiero y la aparición de nuevas tecnologías que no le permiten ejercer el control de su sistema económico nacional. Estos vacíos no han podido ser asumidos dentro del Estado, lo que conlleva a que aparezcan nuevas desigualdades y se profundicen otras. Este es el nivel de polarización que separa a los Estados que aún ejercen control sobre su destino y los que no. Lo que han perdido algunos gobiernos en materia económica lo han ganado otros Estados o algunas transnacionales. Susan Strange afirma que las corporaciones transnacionales no acaban con el Estado, pero ejercen una autoridad paralela con respecto a la dirección de la industria, la inversión, la innovación tecnológica, las relaciones laborales y la extracción fiscal del plusvalor (Strange, 1997). Adicionalmente, Strange explica cómo, junto con la reducción del Estado en términos económicos, se da una disminución de la protección a la sociedad (Strange, 1997); esto es lo que sucede en el caso de las pensiones o los servicios de salud, que son delegados a prestadores de servicios privados. Esta explicación se refuerza si se toma en cuenta la caída del estado de bienestar como modelo mundial de la administración del Estado.

Los gestores de riesgo son precisamente las empresas o Estados que pueden darse el lujo de investigar, crear y comercializar soluciones para los problemas aquí mencionados. Así, solo quien tenga el poder adquisitivo suficiente podrá obtener herramientas para la seguridad, mientras que el riesgo sigue estando ahí para aquellos que no puedan pagar. Beck describe cómo los riesgos imponen límites a la economía. Por ejemplo, los seguros privados distinguen entre los riesgos predecibles y las amenazas incontrolables. En este punto, la diferencia entre *security* y *safety* es fundamental. La primera refiere a una concepción general de la seguridad, y la segunda pasa a ser una "inocuidad técnica". De esta forma, Beck relaciona la búsqueda del beneficio económico de los capitalistas con la seguridad: se ejecutan medidas paliativas que evitan esfuerzos mayores. Es decir, el autor sustenta "la formación de burocracias de seguridad y la legalización de riesgos para los que no existirán paliativos" (Beck, 2002, pp. 87-88).

La necesidad de establecer un nuevo equilibrio de poder se manifiesta como consecuencia de la inestabilidad del poder. En este equilibrio, la combinación de fuerzas debe ser determinada para hacer frente a las necesidades que surgen en el sistema. Por tanto, se propugna por que los Estados recuperen el poder y control sobre su territorio, lo que permitiría reestablecer el vínculo de los ciudadanos con su gobierno. Así se evitaría llegar al escenario contrario, denominado "problema de pinocho"[2], o quedar bajo el mando de los nuevos actores (Strange, 1997, p. 183).

2 Susan Strange utiliza la metáfora de Pinocho para explicar cómo los hilos que sujetan a la marioneta se asemejan a los lazos que unen a los ciudadanos con el Estado. Si estos hilos llegaran a desaparecer, entonces nadie podría dirigir a Pinocho y, de igual forma, si los lazos del Estado con los ciudadanos desaparecieran entonces, nadie los dirigiría y ellos tendrían que decidir por sí mismos qué hacer.

Uno de los objetivos de la ONU es lograr la paz y la seguridad internacional, un mundo con más justicia y sin conflictos. Para ello, es imperativo reconocer la multiplicidad de cambios que se han dado en la última década en el sistema internacional. En suma, con dichos cambios se deben plantear y replantear enfoques y paradigmas que permitan entenderlos y dar solución a los nuevos desafíos. Mediante la Resolución 60/1 de la Asamblea General de la ONU se reconoció que "todas las personas, en particular las que son vulnerables, cuentan con derecho a vivir libres de temor y miseria, a disponer de iguales oportunidades para el disfrute de sus derechos y a desarrollar plenamente su potencial humano" (ONU, 1994, p. 10).

Esta declaración dio un paso fundamental para el reconocimiento de la importancia de una nueva aproximación teórica, como la de la *seguridad humana* en la ONU. La *seguridad humana* plantea respuestas multisectoriales para dar solución integral a las amenazas presentes en la vida de las personas. Mientras tanto, es necesario entender que en cada contexto estatal las amenazas, como sus causas y sus manifestaciones derivadas, varían. De allí que la *seguridad humana* deba proponer soluciones a la realidad local basadas en las necesidades de cada sociedad o gobierno. Sin embargo, existe el riesgo de que se instrumentalice el enfoque de *seguridad humana* y se lo convierta en una excusa para la militarización de diferentes políticas públicas, tanto en el plano nacional como internacional. Esto puede provocar que se proyecte solo en su carácter más restringido y securitizante (Pérez, 2016).

Para el PNUD (2010), la Cumbre de Desarrollo Social, que se desarrolló en 1995 en Copenhague, significó una gran oportunidad para que los Estados y la comunidad internacional dejaran a un lado el enfoque de seguridad nacional implementado durante los últimos cincuenta años y comenzaran a utilizar el enfoque de la *seguridad humana*. En ese orden de ideas, la Cumbre ofreció las siguientes consideraciones:

En principio, que el concepto de seguridad humana sea catalogado como problema fundamental de este siglo. También hacer un llamado de solidarización para contribuir a la seguridad humana mundial. De otra parte, exigir a los gobiernos que adapten medidas y políticas públicas en torno a la seguridad humana, pues deben velar porque sus ciudadanos tengan las oportunidades básicas, específicamente al acceso de servicios básicos y trabajo productivo y remunerado. Por último, también se considera que los países deben cooperar al máximo con esa iniciativa a escala nacional, regional y mundial para lograr un marco de cooperación internacional. Desde la misma perspectiva, también se acordó la revisión del marco normativo de las instituciones mundiales para su reestructuración "dándole prelación a la tarea de enfrentar los problemas referentes a la seguridad humana (pobreza, injusticia social y deterioro ambiental, etc.) para lograr un paradigma de desarrollo humano sostenible a largo plazo" (PNUD, 2010, pp. 45-46).

Conclusión

Con todo lo expuesto, hasta este punto se evidencia un cambio paradigmático en la concepción de seguridad. Incluso se podría decir que el concepto atraviesa todos los ámbitos de vida de cualquier ser humano. Por ejemplo, los derechos básicos de cualquier persona, como el derecho a tener una nacionalidad, implican ya una necesidad de seguridad.

Los cambios paradigmáticos se desatan en medio de la preocupación por el entendimiento del mundo y se relacionan con los profundos cambios estructurales que se experimentan en él, pero no se descartan totalmente las concepciones clásicas de seguridad. Sin embargo, las estructuras globales se sustentan en una idea homogeneizante de los grupos humanos: cuando se manifiesta una desviación, se encuentra una falla en la seguridad. De tal manera que la búsqueda de

principios que regulen los estatutos de seguridad se convierte en una panacea, una utopía, que conserva el carácter de imposibilidad cuando se evalúa la situación de desigualdad en el mundo:

> El paradigma de la seguridad humana muestra que todos los seres humanos están profundamente interconectados en un escenario global en donde las principales amenazas surgen de la falta de desarrollo humano en educación, salud, desigualdades económicas y falta de respeto a los derechos humanos (Font & Ortega, 2012, p. 170).

No obstante, en el intento por lograr una seguridad generalizada, la idea de bienestar termina por homogeneizar a las comunidades y a las sociedades. El resultado más factible es el de la individualización de la seguridad. Por un lado, con la importancia que han cobrado los conceptos de individuo y de individualidad, la *seguridad humana* procura el bienestar de cada uno. Es decir, cada sujeto de la sociedad global debe sentirse plenamente seguro. Esto implica la segunda parte del concepto: la seguridad, evidentemente, ya no es un problema únicamente de defensa y prevención contra la violencia física. Se revelan entonces elementos igualmente importantes, pero usualmente menos visibles, como el medio ambiente o el desarrollo económico. En consecuencia, con un concepto de seguridad al que subyace lo humano, no se puede ignorar un elemento que anteriormente parecía circunstancial: la dignidad.

Este último elemento sintetiza la multiplicidad de elementos y actores que componen la *seguridad humana*. Es decir, se ha pasado de la seguridad unidimensional, en términos de defensa estatal, a la seguridad compleja, que propone la protección de diferentes ámbitos en los que está inmerso el individuo. La *seguridad humana*, como seguridad compleja, se concentra en las variables que se perciben materialmente y que conducen al bienestar inmaterial del individuo:

> Este nuevo concepto responde a dos nuevas ideas: primera, que la seguridad debe centrarse en las personas; y segunda, que la seguridad de las personas se ve amenazada no solamente por la violencia física, sino por otras amenazas como la subsistencia o las condiciones de llevar una vida con dignidad. Además, el concepto tiene dos dimensiones, una cuantitativa, la satisfacción de las necesidades materiales básicas que aseguren la continuidad de la vida, y otra cualitativa, vinculada a la dignidad, lo que exige avanzar en la satisfacción de los derechos humanos (Font & Ortega, 2012, p. 170).

Según Font & Ortega (2012), los enfoques del concepto de seguridad han cambiado no solo por las percepciones del mundo y por la evidente necesidad de un cambio paradigmático, sino porque las grandes organizaciones también han respondido a los paradigmas y han intentado establecer políticas internacionales, ya sea por medio de declaraciones, resoluciones, etc. En resumen, los autores afirman:

> El Programa de las Naciones Unidas para el Desarrollo (PNUD) acuñó en 1994 el nuevo concepto de seguridad humana, desplazando el viejo enfoque de una seguridad centrada en proteger a los Estados a otro que pone a las personas como sujeto central de la seguridad. Este nuevo enfoque trasciende la amenaza por la violencia personal y pone en primer plano las amenazas a la subsistencia de las personas en unas condiciones de dignidad. El concepto amplía el ámbito del término de seguridad a la seguridad económica, alimentaria, de salud, medioambiental, personal, política y comunitaria (Font & Ortega, 2012, p. 170).

Finalmente, es posible afirmar que los paradigmas de corte interpretativo generan un cambio sustancial en la conceptualización del individuo. Esto permite que se amplíen las consideraciones en torno a las condiciones de vida que lo afectan. En el caso de la seguridad, y aunque todavía quede mucho por analizar, la posibilidad de construir

un único concepto unicausal, determinante y objetivo se aleja cada vez más de las conceptualizaciones, tanto prácticas como académicas, debido a los cambios del mundo, de las necesidades de los seres humanos y, lo más importante, de la visión que tengamos de nosotros como individuos.

Referencias

Ariza, N. (2010). La aplicabilidad del concepto de seguridad humana en América Latina y el Caribe: el desarrollo humano como fuente de seguridad. *Oasis*, 15. https://www.redalyc.org/pdf/531/53121459003.pdf

Beck, U. (2002). *La sociedad del riesgo global.* Siglo XXI.

Castells, M. (2010). *The Information Age* (Volume I). *The Rise of the Network Society.* Wiley-Blackwell.

Fernández, J. (2006). *La Seguridad Humana.* Ariel.

Font, T. & Ortega, P. (2012). Seguridad nacional, seguridad multidimensional, seguridad humana. *Papeles de relaciones ecosociales y cambio global*, *o*(119), 161 – 172. https://www.fuhem.es/papeles_articulo/seguridad-nacional-seguridad-multidimensional-seguridad-humana/

Fuentes, C. (2012). Seguridad Humana y Derechos Humanos: Referencias conceptuales y aplicabilidad en América Latina. En F. Rojas (ed.), *Seguridad Humana: Nuevos enfoques* (pp. 33-54). Flacso. https://www.flacso.org/sites/default/files/Documentos/libros/secretaria-general/Seguridad%20Humana.pdf

Held, D. (2002). *Transformaciones globales. Política, económica y cultura.* Mc Graw Hill.

Muñoz, T. J. A. (2018). Usos políticos del concepto de seguridad humana: securitización de la violación de derechos humanos y del subdesarrollo en el escenario internacional. *Territorios*, *39*, 21-46. http://dx.doi.org/10.12804/revistas.urosario.edu.co/territorios/a.6232

Organización de las Naciones Unidas [ONU]. (1994). *Informe sobre Desarrollo Humano 1994.* Oxford University Press.

Pérez, F. (2016). Seguridad Humana: ¿El complemento perfecto para nuestras estrategias de seguridad?. *Documento de Opinion, 118*, 1-15. http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO118-2016_SeguridadHumana_PerezFranco.pdf

PNUD (2010). *Informe regional sobre Desarrollo Humano para América latina y el Caribe 2010*. Nueva York: Galera.

Sánchez, D. (2017). *Índice de seguridad humana para las localidades de Bogotá 2014*. Secretaría Distrital de Planeación. http://www.sdp.gov.co/sites/default/files/3._actualizacion_indice_seguridad_humana_localidades_bog.pdf

Strange, S. (1997). *The Retreat of the State: The Diffusion of Power in the World Economy.* Cambridge University Press.

Capítulo 3

Hacia la articulación del pensamiento complejo y estratégico en la formación por competencias para la investigación en la seguridad integral[1]

David E. López Cortés*

1 Capítulo de libro resultado del proyecto de investigación titulado *Impacto de las políticas de seguridad integral en el desarrollo y gestión del componente de investigación del currículo* MADGSI, de la línea de investigación Seguridad Integral del grupo de investigación CIPAER, con código COL 0093003, de la Escuela de Postgrados de la Fuerza Aérea Colombiana.

* Doctor en Educación, Universidad Santo Tomás de Aquino. Docente investigador de la Maestría en Dirección y Gestión de la Seguridad Integral. Correo electrónico: david.lopez@epfac.edu.co

CÓMO CITAR

López Cortés, D. (2020). Hacia la articulación del pensamiento complejo y estratégico en la formación por competencias para la investigación en la seguridad integral. En Y. Rico, D. López Cortés, & A. Cerón R. (comps.), *Enfoques y gestión en Seguridad Integral* (pp. 69-102). Escuela de Postgrados de la Fuerza Aérea Colombiana. https://doi.org/10.8667/9789585996199.03

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

CAPÍTULO 3.
Hacia la articulación del pensamiento complejo y estratégico en la formación por competencias para la investigación en la seguridad integral

https://doi.org/10.8667/9789585996199.03
Bogotá, Colombia
Noviembre, 2020

RESUMEN

El presente capítulo aborda el pensamiento estratégico y complejo. Este debe estar articulado con las competencias en investigación. Así, en la formación de un gerente de la seguridad integral, como protagonista activo de su propio proceso de aprendizaje, el pensamiento estratégico y complejo le permitirá prever y anticiparse a las posibles amenazas y riesgos que enfrenta constantemente cualquier organización en un mundo volátil, cambiante, dinámico, complejo y lleno de incertidumbres.

PALABRAS CLAVE

Competencia; formación de profesionales; investigación; planificación estratégica; seguridad humana.

Introducción

El presente capítulo esboza una aproximación teórica descriptiva de la importancia del pensamiento estratégico. Este, acoplado con el pensamiento complejo y la formación de competencias en investigación, puede promover el desarrollo de actitudes y habilidades básicas para la solución de problemas propios de la seguridad.

El propósito formativo de la formación posgradual en seguridad es brindar al estudiante herramientas y desarrollar habilidades y competencias para hacer investigación. En el aprender haciendo, el aprender a aprender, el docente acompaña el proceso de investigación del educando y hace que lo aplique en la solución de problemas del entorno de la seguridad. Para Tobón (2013), las competencias son manifestaciones de un saber hacer específico que se materializa en un procedimiento y una estrategia para solucionar un problema en un contexto determinado. El desarrollo de una competencia se caracteriza por el aporte a la construcción de la realidad. La competencia integra al saber conocer, el cual permite observar, analizar y comprender para actuar según las necesidades del entorno.

Igualmente, para Gonczi y Athanasou (1996), las competencias se refieren a un conjunto de capacidades y destrezas que se desarrollan en las fases formativas (que preparan al estudiante para la vida laboral, en el desempeño en situaciones específicas).

Surge una serie de interrogantes que motivan el desarrollo de esta indagación; a saber: ¿Qué es el pensamiento estratégico?, ¿cuál es su relación con el pensamiento complejo?, ¿cuáles son las competencias en investigación que debe desarrollar un gerente de la seguridad integral en su formación académica? Para responder a estas preguntas se optó por un análisis teórico partiendo de diferentes autores versados

en los temas del pensamiento estratégico, pensamiento complejo y competencias en investigación.

Este capítulo presenta un enfoque cualitativo, de tipo descriptivo, con respecto al fenómeno educativo de la investigación (una competencia de vital importancia en la formación de un profesional de la seguridad integral).

Los propósitos de la formación en investigación en los programas de seguridad deben basarse en un currículo que dinamice la enseñanza particularmente basada en problemas. Esta metodología favorece el desarrollo de competencias en investigación, del pensamiento estratégico, complejo, y los relaciona con los contenidos teóricos mediante un análisis del contexto y sus necesidades para la solución de problemas. Por otra parte, quienes desempeñan la función gerencial de la seguridad deben disponer de un tipo de pensamiento muy particular para definir las acciones que se requieren para hacer segura a una empresa. Esto implica conocer el contexto en el que desarrolla su actividad empresarial.

De este modo, al enfrentar un problema de seguridad, cualquiera que sea su naturaleza, un gerente dirige su pensamiento estratégico a establecer conexiones cognitivas. El gerente relaciona conocimientos, experiencias previas, especialmente de tipo significativo, que lo llevan al razonamiento, la reflexión, el análisis y la contextualización, para construir una solución de manera eficaz.

En los últimos años, ha aumentado el interés por analizar la utilización del pensamiento estratégico en la seguridad. El propósito es evaluar qué tan adecuado es para la formación de un gerente en seguridad, teniendo en cuenta las nuevas amenazas y riesgos que las organizaciones criminales generan a diario, así como el terrorismo y los ciberdelincuentes (que aumentan de manera acelerada y abrumadora).

Según Robert (2006), el pensamiento estratégico le permite a un gerente en seguridad interpretar las variables de riesgo que puedan poner en peligro la existencia de una organización. Con esto puede anticiparse a las futuras amenazas de una manera multidimensional, si analiza la complejidad del contexto en el que se desarrolla el negocio y los factores que inciden en él. Actualmente, la seguridad desempeña un papel relevante en la protección de las organizaciones. Con su trabajo, un gerente en seguridad aporta a la protección del patrimonio y los activos de las organizaciones. Se requiere del uso de un pensamiento estratégico para enfrentar las constantes amenazas, como la delincuencia común, el crimen organizado, fenómenos naturales, pandemias como la COVID-19, terremotos e inundaciones, entre otros.

De ahí la importancia de aprender a pensar estratégicamente, ya que implica desviarse del enfoque gerencial tradicional en seguridad que no permite ver la complejidad de la realidad. El pensamiento estratégico debe iniciarse con el entendimiento de la realidad, que es compleja. Implica entonces un pensamiento, abierto a la complejidad, que no se adquiere espontáneamente, sino que es producto de la formación de un proceso de aprendizaje en investigación que parte de la observación del contexto de la organización.

Al hacer un acercamiento al pensamiento estratégico a partir de diferentes autores, se resalta que este se caracteriza por ser analítico, reflexivo, innovador. Él permite desarrollar un razonamiento creativo e integrador para solucionar un problema o situación, un todo, y permite también construir un camino desde la interdisciplinariedad.

Para Ohmae (2004), el pensamiento estratégico se caracteriza por la habilidad para fijar un objetivo y experimentar nuevas ideas. Emplea la innovación para lograr ventajas competitivas para una organización.

En seguridad, para enfrentar a las estructuras de crimen organizado que piensan día a día en la forma de burlar los sistemas de seguridad de las organizaciones; el pensamiento estratégico debe proveer los elementos para determinar cuáles pueden ser los puntos vulnerables de la seguridad. Esto permite emprender acciones preventivas y correctivas. Este tipo de pensamiento, según Sánchez (2007), se caracteriza por ser creativo, encuentra ideas que se salen del pensamiento cotidiano, habitual, tradicional, estático. En seguridad no se puede hacer todo de la misma manera siempre; se tiene que estar preparado para lo impredecible.

Asimismo, para Ronda (2005, citado en García de Mujica & Daza 2006), el pensamiento estratégico busca comprender, a partir del conocimiento del contexto, que es complejo, cómo anticiparse a una situación en particular. Esto se hace al relacionar las diferentes variables de riesgo que puedan poner en peligro una organización, lo que permite intervenir oportunamente. Este proceso es posible cuando se obtiene un conocimiento y la información necesaria de la realidad del ecosistema de la organización.

También, para Vivas (2000), el pensamiento estratégico busca comprender y pronosticar la forma más viable de enfrentar situaciones difíciles del presente para alcanzar una meta en el futuro. Esto se hace en un entorno inestable, en el cual no se pueden plantear estrategias simples para enfrentar fenómenos complejos. Allí, paradójicamente, el cambio es la única constante.

Según Krell (2009), el pensamiento estratégico integra los conocimientos, evalúa lo riesgos y, junto a una acción planificada, obtiene resultados. Por su parte, Jatar (2000) señala que el pensamiento estratégico parte de la observación de un contexto determinado, lo que permite un análisis de la realidad como un sistema complejo en el que intervienen múltiples elementos.

Para Castañeda (2001), el pensamiento estratégico es un proceso de razonamiento que está relacionado con el análisis de los elementos de un problema. Una vez identificados estos, se puede actuar sobre el problema para obtener una solución. Además, el pensamiento estratégico es abierto a la discusión y al análisis de planteamientos teórico-metodológicos. Este tipo de pensamiento se caracteriza porque rompe con lo lineal, lo estático, y lleva a la acción. Es muy apropiado para enfrentar el entorno cambiante y variable de las amenazas, los riesgos y las vulnerabilidades que surgen en las organizaciones en el contexto de la seguridad.

Al enfrentar un problema de seguridad, el pensamiento estratégico debe iniciar por un análisis del contexto y la identificación de los elementos que están interactuando. Algunos de ellos no se ven a simple vista, muchas veces son difusos y necesitan ser develados. Si quieren ser descubiertos, no pueden ser abordados a partir de una racionalidad lineal, tradicional y simple. Para Morin (2011), la simplicidad racional con la que en ocasiones se abordan los hechos o los fenómenos naturales tiende a separar lo que está ligado, a unir lo que es diverso o a pasar por alto lo que está unido. La realidad comprende múltiples aspectos que están en constante cambio (Álvarez & Kuratomi, 2005).

De ahí que sea fundamental que el gerente en seguridad sea creativo, innovador, esté abierto a abordar la investigación, la gestión y la creación de modelos en seguridad a partir de un paradigma estratégico y complejo. Este paradigma permite asegurar el futuro de una organización y superar amenazas y riesgos que solo se pueden percibir si se desarrolla este tipo de pensamiento.

El pensamiento complejo permite emplear y articular métodos, teorías y conceptos. Para Meriñez (2006, citado en Pernía, 2014), "el

pensamiento estratégico es un proceso de razonamiento aplicado a sistemas o problemas complejos, con miras a lograr un objetivo" (p. 31), a predecir efectos de las acciones y a juzgar la validez de estas en la prevención como pilar de la seguridad. El pensamiento estratégico permite crear y construir diversas soluciones utilizando la indagación y la innovación, con una mirada integral para la solución de problemas nunca antes enfrentados en la seguridad.

El proceso de formación de un gerente de la seguridad integral debe estar orientado a construir modelos de seguridad utilizando los paradigmas de esta disciplina. Esto posibilita la disminución de la incertidumbre en el cumplimiento de los objetivos y, además, de los acontecimientos que puedan llegar a destruir una organización o a causar un siniestro en el objeto del negocio. Por tal razón, el desarrollo de competencias en investigación se convierte en el camino que permite establecer, prevenir y anticiparse a situaciones de alto impacto que puedan poner en peligro a una organización. Dichas competencias permiten el manejo de crisis, la continuidad de negocios y la resiliencia organizacional.

Tanto el pensamiento sistémico como el complejo aplicado a la seguridad, rompe con el pensamiento lineal y simple de la formación tradicional, que encara un problema enfrentando de manera aislada sus componentes. La seguridad debe mirar el contexto y las múltiples variables que hacen parte del problema y enfrentarlas conjuntamente.

Cuando se aborda de manera aislada un problema, esta mirada impide descubrir la interrelación de las variables, que unidas forman un todo. Ese todo adquiere nuevas propiedades que no pueden verse y analizarse cuando se dividen y separan sus partes. Las partes por sí solas presentan propiedades distintas, que no permiten ver correctamente el problema y la articulación del conjunto.

El pensamiento complejo no mira las partes por separado, sino que las integra al contexto al estudiar el todo en su conjunto. Se asume que las propiedades de las partes solo pueden ser entendidas a partir de la comprensión de la dinámica del todo; es decir, la parte es una variable en una malla de relaciones que mantiene unido al sistema como conjunto.

No se asume que la dinámica del todo se pueda comprender a partir de la dinámica de las partes, sino que las propiedades de las partes (sean organizaciones, comunidades, individuos, etc.) solo pueden entenderse a partir de la dinámica del todo. En los sistemas de seguridad no existen las partes aisladas. Lo que se considera como parte es una configuración individual de una red de relaciones.

Así, el trabajo del gerente de la seguridad en una organización es crear, con la ayuda de la investigación, un medio estable controlando el mayor número de variables de riesgo posibles.

De ahí viene la importancia de la formación en competencias en investigación, unidas a un pensamiento estratégico y complejo. Esta formación genera una actitud gerencial estratégica para actuar de forma proactiva en la gestión y construcción de modelos de seguridad, que permitan prever y adelantarse a futuras amenazas y riesgos que puedan colocar en peligro a una organización.

La investigación es una acción del conocer del ser humano. Por medio de esta, él interpreta al mundo para construir la realidad. Ese proceso de construcción requiere un conocimiento profundo de una disciplina de estudio, como es el caso de la seguridad.

Por otra parte, la formación investigativa es la columna vertebral en la formación posgradual. Permite la creación de nuevo conocimiento, la solución de problemas reales en un contexto determinado, el diálogo de saberes, acompañado de la interdisciplinaridad. De esta

manera, tiene la capacidad de integrar conocimientos para aplicarlos al ejercicio profesional.

Al respecto, para Cecilia Fierro, Bertha Fortoul y Lesvia Rosas (2002), la manera de abordar la investigación en las instituciones educativas debe ser holística, transdisciplinar, debe darse en una continua relación con el contexto específico. De modo que investigar en las instituciones educativas requiere formular hipótesis de solución a problemas significativos del contexto del estudiante y llevarlos al aula de clase, proyectar los distintos pasos del proceso investigativo que llevan a la solución de un problema específico. Con este, el estudiante puede aplicar lo teóricamente aprendido, además de confrontar las hipótesis e ideas previas del educando con sus propios conocimientos y analizar conjuntamente el desarrollo del proceso de investigación.

En este punto es pertinente resaltar la importancia de los fundamentos metodológicos que debe contener el currículo en seguridad integral, y el adelanto epistemológico que debe hacer el docente para realizar la investigación. Esto supone un conocimiento profundo de su disciplina, un manejo didáctico de técnicas de investigación en el aula. Como actor vital en el marco del desarrollo de la investigación en seguridad, el docente es el líder académico para la formación de competencias investigativas en los estudiantes y el fortalecimiento de la cultura de la investigación en la formación profesional.

Finalmente, es importante precisar que un proceso de formación en competencias de investigación, es un proceso reflexivo y sistemático. En él se crean las condiciones a partir del currículo, la metodología de enseñanza y el compromiso del docente para que el estudiante, integrando el pensamiento estratégico y complejo, resuelva problemas del contexto de la seguridad.

El pensamiento complejo

Al abordar el tema de la formación en seguridad integral, se busca que el profesional responda a los diferentes escenarios o contextos de interacción, que tenga capacidad de análisis y síntesis para la resolución de problemas e imprevistos. Esto implica conocer los diferentes aspectos de la seguridad, los cuales le permiten diagnosticar la situación de seguridad en empresas y organizaciones públicas o privadas. Además, puede elaborar propuestas de gestión, análisis de riesgos y conocer mecanismos de prevención. Igualmente, se busca que el gestor de la seguridad pueda responder a los diferentes entornos de interacción en aspectos relacionados con la seguridad. De ahí que los procesos formativos en seguridad se deban ubicar en cada contexto de manera compleja.

Nuestro tema es el pensamiento complejo como modelo de conocimiento que está sustentado en la interconexión de las partes y el todo. Se trata entonces de la relación con la multidimensionalidad que encierran los fenómenos, situaciones, hechos naturales y sociales abarcados por los temas de seguridad. Así las cosas, el interrogante que surge es, ¿cuál es la importancia del pensamiento estratégico y complejo, articulado con la formación de competencias en investigación en la formación de un gerente de la seguridad integral? Para dar respuesta a esto, hay que abordar el contexto de la seguridad como la intersección de sus partes, partiendo del paradigma de la complejidad.

Cabe señalar que el anterior interrogante se puede abordar desde el currículo complejo por competencias, en articulación con el pensamiento complejo, estratégico y la investigación. En este currículo la complejidad se debe abordar como un elemento transversal en el análisis del contexto de la seguridad. Así pues, deben darse una inter y una

transdisciplinariedad en las asignaturas o módulos que hacen parte del plan de estudios en la formación de un gerente de la seguridad.

Por ejemplo, cuando un gerente enfrenta problemas de seguridad en una organización, la cual está expuesta a nuevas amenazas, nuevas vulnerabilidades, debe hacer un análisis del contexto partiendo de una mirada compleja. Para esto, debe tener en cuenta que los problemas de seguridad se dan en un ambiente natural, social, económico y político. Estos son algunos de los muchos elementos a partir de los cuales surge un ambiente. El análisis de esos elementos permite identificar amenazas y riesgos del ambiente específico de una organización.

El paradigma de la complejidad aplicado a la seguridad revela fundamentalmente una serie de variables que, al ser reagrupadas, llevan al descubrimiento del contexto particular del problema. La aplicación del paradigma se daría en el diseño de los sistemas de seguridad, los cuales deben tener componentes cada vez más sofisticados que se adapten a las necesidades actuales.

Ahora bien, el pensamiento complejo, articulado en un currículo por competencias, requiere de un nuevo tipo de razonamiento que no fragmente lo complejo del mundo, que no fraccione sus partes. Entender el funcionamiento de un mundo complejo es emprender un camino de reflexión, investigación y análisis de contexto. La integración de estos procesos con el pensamiento estratégico y la investigación, le permite al profesional de la seguridad afrontar la solución de problemas en su campo profesional a partir de un espectro más amplio.

Para entender la complejidad se debe partir de que existe un paradigma de la simplicidad, que tiene como fundamento epistemológico el aislamiento de los elementos y las variables. Estos son analizados por separado, en una metodología característica de los métodos analíticos y del currículo tradicional. Así, se busca poner en orden el universo, el cual se reduce a una ley que explica a la realidad singular.

En términos de Morin (2010), en el paradigma de la simplicidad se da una deconstrucción de la naturaleza, de sus ecosistemas, de un fenómeno o situación fáctica. Ninguno de estos se aborda como un todo. Los elementos que componen al fenómeno se analizan de forma aislada y no se unen para explicar su funcionamiento. De esta manera, se enseñan en las escuelas y universidades las asignaturas y módulos de forma aislada y separadas. De ahí la dificultad para resolver problemas en contexto y trabajar en equipo.

Asimismo, la educación tradicional ha estado permeada por mucho tiempo por el paradigma de la simplicidad. La forma como se construye el conocimiento no es la más apta para desarrollar competencias en investigación. El aprender consiste solo en repetir y recordar conceptos, sin aplicarlos en la solución de problemas. Además, no hay interdisciplinariedad entre las distintas áreas del saber, las cuales son enseñadas a los estudiantes sin una ilación lógica ordenada, sin un objetivo concreto. No hay un adiestramiento en la investigación que prepare al estudiante para la solución de problemas reales. Sin una aplicación de lo aprendido, los contenidos rápidamente se olvidan. Incluso cuando se trabajan problemas, hay una separación o división del todo: los elementos que lo forman se aíslan, no se unen, y se busca explicar aisladamente el fenómeno en estudio.

Cuando se piensa un problema de seguridad mediante el pensamiento complejo, se pasa de estudiar las partes del contexto por separado a estudiar el todo en su conjunto. Se asume que las propiedades de las partes solo pueden ser entendidas desde la dinámica del todo. Es decir que la parte es una pauta en una malla inseparable de relaciones que mantienen unido el fenómeno a un contexto, como un todo en un sistema.

En un sistema, cualquiera que sea su naturaleza, no existen las partes aisladas. La seguridad no es la excepción. Lo que se considera

como parte es una configuración de una red de relaciones. Cabe señalar cómo, mediante el pensamiento reduccionista que divide y separa el abordaje de muchas disciplinas en la formación profesional, la mayoría de los currículos, programas y planes de estudio (desde el preescolar hasta la educación superior) en los países latinoamericanos están organizados en disciplinas separadas y materias divididas y desconectadas. Más aún, las diversas disciplinas (separadas unas de otras) se componen de hechos y datos que, a su vez, están desligados unos de otros. La formación en seguridad no escapa a esta situación.

De acuerdo con González (1997), la propuesta del pensamiento complejo está presente en el análisis de la realidad. La complejidad es una característica presente en la naturaleza. Como un sistema, lo social no escapa a ella; es un sistema creado a partir de las relaciones económicas, sociales, políticas, producto de las relaciones humanas construidas por la cultura que se integra al contexto humano, que integra tanto al observador como a lo observado.

Detrás de la seguridad hay problemáticas sociales profundas. Para poder solucionarlas, se requiere abordarlas desde la complejidad, pues el paradigma de la simplicidad no es suficiente. La seguridad debe ser asumida mediante el paradigma complejo, que permite ver las amenazas y riesgos que enfrenta toda organización o empresa, en su actividad económica, como un todo.

Finalmente, en el proceso de formación de un gerente de la seguridad, el pensamiento complejo le ofrece una experiencia enriquecedora con gran importancia en la actualidad. Como una herramienta de reflexión, es ante todo un pensamiento que relaciona los elementos en contexto, lo cual es útil para la creación de modelos de seguridad en la medida en que se pongan en práctica los conceptos propuestos por Edgar Morin.

El pensamiento estratégico y la investigación: una competencia que debe tener todo gerente de la seguridad integral en el desarrollo y gestión de su trabajo

El proceso de formación de un gerente de la seguridad integral debe estar orientado a establecer y prevenir situaciones dañinas, confusas. Si se desconoce su alta probabilidad e impacto, ellas pueden poner en peligro a una organización. La pregunta que surge es, ¿cuál es el tipo de pensamiento que debe desarrollar un gestor de la seguridad integral que privilegie la investigación y la capacidad de entender una situación indeterminada?

La importancia de la investigación formativa en seguridad ha sido abordada y definida por diferentes autores. Para estos, la investigación es el proceso por el cual el profesional desarrolla competencias, destrezas, habilidades para resolver problemas en el contexto de la seguridad utilizando el método científico. Igualmente, toda investigación científica debe ser sistemática; es decir que los datos obtenidos se deben organizar, analizar e interpretar en relación con las hipótesis formuladas y con el plan de trabajo elaborado.

Así, el método investigativo en seguridad exige un proceso lógico para adquirir información de la realidad sobre un riesgo o una amenaza. Dicha información se sistematiza y procesa, utilizando el pensamiento estratégico y complejo, para llegar a unas conclusiones y soluciones que protejan una organización. Lo anterior permite afirmar que las actividades de investigación en seguridad que utilizan la metodología científica, articuladas con el pensamiento estratégico,

al análisis del contexto y la evaluación del riesgo mediante el pensamiento complejo, llevan a desarrollar una actitud crítica y analítica que es la base para una capacidad de predecir los riesgo y amenazas a la seguridad de cualquier organización.

Con la habilidad para identificar amenazas, los riesgos y sus fuentes, que no son evidentes a simple vista, surge entonces otro interrogante: ¿Cuáles son las competencias que la investigación en la seguridad integral privilegia? Desde luego, la preocupación más sobresaliente en la seguridad integral es predecir los efectos de los sucesos, amenazas y riesgos que pongan en peligro la seguridad de una organización, cualquiera que sea su naturaleza, pública o privada. De ahí que el papel de un gerente de la seguridad sea crear un contexto en el cual el riesgo para la empresa sea muy bajo. Se sabe que el riesgo nunca desaparecerá totalmente, pero se pude minimizar. Hay que estar preparado para enfrentarlo todos los días, lo cual genera una percepción de tranquilidad y un ambiente de seguridad.

Sin duda alguna, si los riesgos se materializan en daños, debe haber una respuesta inmediata. Esta se da solo si previamente se ha desarrollado un modelo de seguridad a partir de una evaluación de riesgos. El conocimiento del contexto en el que se desarrolla la empresa, examinado desde la complejidad, permite identificar las variables que son factores de vulnerabilidad. Lo anterior, articulado con el pensamiento estratégico y la investigación permanente, brindará las herramientas que permitan diseñar un plan de acción inmediato.

La estrategia se entiende como un plan de acciones para enfrentar un dificultad. Para Weiberger (2009), es una respuesta que incluye un sistema de soluciones y controles, que surge de conocer una organización en su interior y el hábitat en el que se encuentra. Para Delamer (2005), el pensamiento estratégico es pragmático y depende de las realidades del entorno. Este debe conocerse para poder anticipar

los problemas, para que cuando lleguen, haya una solución inmediata. Igualmente, para Davies (2000), el pensamiento estratégico se caracteriza por ser integrador de variables problemáticas. A partir de ellas se construyen múltiples soluciones. Este tipo de pensamiento se articula muy bien con el pensamiento complejo, que permite mirar el todo y sus partes para construir soluciones a partir del conocimiento del contexto y la movilización del conocimiento de varias ciencias o disciplinas, que en conjunto permiten enfrentar cada caso particular.

En la formación de un gerente de la seguridad integral, el pensamiento estratégico debe estar presente en la solución de diversos problemas y el abordaje de la seguridad como un sistema integrado por diversos elementos sociales, económicos, educativos, políticos, ambientales, entre otros. Las actividades enfocadas en estos elementos conducen al fortalecimiento de la seguridad y la atenuación, aceptación o transferencia del riego. El riesgo se define como un evento, suceso, acontecimiento (o incluso situaciones abstractas), del cual no se tiene certeza absoluta, que puede poner en peligro la infraestructura o los activos vitales o críticos de una organización por efectos del azar en un tiempo cercano.

Lo más importante es que un gerente de la seguridad integral debe ser capaz de entender e interpretar el entorno de la organización. Autores como Porter (1996) destacan la importancia de identificar las diferentes amenazas, debilidades y oportunidades de acción de una organización que le permiten anticiparse a los diferentes riesgos y tener la solución justo antes de que ocurran. Por otra parte, Delamer (2005) señala cómo la estrategia fue relacionada primero con las operaciones militares, pero este tipo de pensamiento se extendió a otras actividades como la política, la economía, la empresa y la seguridad integral.

De manera similar, el pensamiento estratégico se asocia con competencias de investigación, reflexión, acción y dirección estratégica

que parten del principio de planeación. Se suman a esto las habilidades de gestión, control, disciplina de trabajo, ejecución y evaluación. Estos elementos, cuando se articulan e integran con la investigación de la seguridad de la organización, permiten disminuir a su mínima expresión los factores de riesgo y conducen a la organización a un éxito operativo a través de un derrotero seguro y previamente evaluado.

El pensamiento estratégico y la investigación se convierten en las herramientas del gerente de la seguridad para enfrentar los diferentes riesgos y amenazas que son constantes en las organizaciones. Como se ha dicho, estas no se pueden afrontar con un pensamiento tradicional, reduccionista. Este tipo de pensamiento, de acuerdo con Morin (1990), favorece el paradigma tradicional reduccionista.

Un gerente de la seguridad no puede aplicar en su trabajo un pensamiento tradicional y simple. No puede abordar la seguridad de una organización de manera fraccionada o mediante elementos que parcelen el conocimiento, borrando la relación que hay entre ellos. Los estudios de seguridad tradicionales siguen un pensamiento lineal que no permite identificar diferentes riesgos que están ocultos y que se deben descubrir.

El pensamiento tradicional, con respecto a la determinación de diferentes riesgos, tiene el inconveniente de que el mayor énfasis está puesto en lo disciplinar de la seguridad, y no en la relación de las diversas disciplinas. En procesos interdisciplinares o transdisciplinares participan distintos saberes profesionales, lo cual permite ampliar el espectro de análisis de la seguridad para la protección de los activos vitales de una organización.

Las diferentes amenazas que han surgido por la existencia del crimen organizado transnacional no se pueden enfrentar entonces mediante un pensamiento lineal, tradicional. El paradigma de la seguridad cambió, particularmente a raíz de los hechos sucedidos el

11 de septiembre del 2001. A partir de ese momento todo el sistema ancestral y tradicional de seguridad colapsó. Los conceptos de seguridad cambiaron, se empezó a dar un lugar central a la detección de las nuevas amenazas, como el crimen transnacional, terrorismo, ataques a la seguridad cibernética, tráfico de armas y drogas, lavado de activos, financiación del terrorismo y la inherente relación entre ellos. Así las cosas, es necesario fortalecer las capacidades de pensamiento estratégico y unirlas a la investigación constante y permanente para resolver problemas en todos los niveles organizacionales. Esto permite anticiparse a hechos impredecibles, como los del 11 de septiembre del 2001.

En consecuencia, el complejo sector de la seguridad organizacional solo puede ser abordado mediante un pensamiento estratégico, sistémico e integrador que le permita al gerente de la seguridad afrontar de manera holística y multidisciplinaria los diferentes riesgos y amenazas que puedan afectar las organizaciones. Lo anterior evidencia la importancia de hacer investigación en los programas de seguridad, a través del desarrollo de proyectos de investigación que articulen a las instituciones de educación superior y las empresas relacionadas con el sector de la seguridad. Se debe desarrollar una metodología investigativa que oriente los proyectos de grado a resolver problemas de la realidad mediante procesos sistemáticos. Estos proyectos deben generar procesos de intervención en situaciones reales dando relevancia e impulso al pensamiento estratégico, complejo, presente en las políticas y acciones en investigación en seguridad formativa y aplicada.

Además de identificar las situaciones de alta probabilidad e impacto, deben gestionarse pensando la seguridad como un todo, sin desestimar todas las partes. Recordemos que el todo es más que la suma de las partes, así que deben identificarse los diferentes factores internos y externos que puedan afectar la seguridad de las empresas y organizaciones de toda clase.

González et al. (2012) consideran que las competencias que privilegian la investigación son las de tipo cognitivo. Estas desarrollan un pensamiento estratégico que se caracteriza por la capacidad de entender una situación confusa descomponiendo sus partes. Por otro lado, está el pensamiento complejo, que otorga la habilidad para identificar elementos y relaciones que no aparecen a simple vista.

Asimismo, un gerente de la seguridad integral ha de estar en capacidad de pensar y concebir la seguridad de la organización en todos sus niveles. Además de los tácticos, operacionales y de campo físico, debe proteger la información y tener la capacidad de evaluar y diagnosticar los diferentes riesgos para poder elaborar planes y programas de acción. A este tenor, un gerente de la seguridad debe asociar el pensamiento estratégico con competencias en investigación, actividades orientadas a un estudio exhaustivo que lo lleven a predecir situaciones de riesgo y a la solución de problemas relacionados con la seguridad integral. Esta solución debe darse de forma casi anticipada, lo cual es posible por la predicción, una característica fundamental de toda ciencia.

Además, el pensamiento estratégico y la investigación deben orientar los procesos de dirección y gestión de la seguridad que permitan innovar e impactar las organizaciones para que sean productivas, competitivas y, en especial, para garantizar la seguridad y la protección de sus activos vitales. Las preguntas que surgen son: ¿qué es una competencia?, ¿cuáles son las competencias que debe tener un gerente de la seguridad para proteger su organización?, ¿Qué competencias en investigación debe desarrollar un gerente de la seguridad integral para reducir los múltiples riesgos que enfrenta cualquier tipo de organización, y evitar que sea impactada por los diferentes factores a que se expone en la actualidad?

En primer lugar, una competencia es el saber hacer en un contexto específico. En este caso, se hace referencia al campo de la seguridad

integral. Por ejemplo, para autores como Tobón (2013), las competencias son acciones que se reflejan en habilidades que permiten resolver problemas de un contexto especifico, que combinan conocimientos del saber conocer (el uso y manejo de conceptos y teorías), el saber hacer (la aplicación de habilidades procedimentales y técnicas) y el saber ser (actitudes y valores). Asimismo, para Gonczi y Athanasou (1996), las competencias se evidencian en el hacer a través habilidades. Estas representan el desempeño en el que se armonizan los conocimientos, actitudes, valores y destrezas en la solución de problemas.

Para Levy-Leboyer (2000), las competencias puestas en acción muestran un hacer que se hace visible a través de habilidades, destrezas, en el desempeño de un oficio o profesión. Para Ouellet (2000, p. 27), "la competencia puede apreciarse en el conjunto de actitudes, de conocimiento y de habilidades específicas que hacen a una persona capaz de llevar a cabo un trabajo o de resolver un problema particular". Del mismo modo, para Mulder, Weill y Collins (2007), las competencias a nivel profesional se hacen visibles, en el proceso formativo, cuando el estudiante es capaz de resolver problemas particulares de su disciplina de estudio.

En el caso de la seguridad, el propósito formativo por competencias es brindar al futuro gerente de la seguridad las herramientas y habilidades para hacer investigación, así como capacitarlo en el aprender haciendo y el aprender a aprender. Esto se articula con la declaración mundial de la Unesco sobre la educación superior para el siglo XXI. En este documento se señala lo siguiente:

> La educación superior ha dado sobradas pruebas de su viabilidad a lo largo de los siglos y de su capacidad para transformarse y propiciar el cambio y el progreso de la sociedad. Dado el alcance y el ritmo de las transformaciones, la sociedad cada vez tiende más a fundarse

> en el conocimiento, razón de que la educación superior y la investigación formen hoy en día parte fundamental del desarrollo cultural, socioeconómico y ecológicamente sostenible de los individuos, las comunidades y las naciones. Por consiguiente, y dado que tiene que hacer frente a imponentes desafíos, la propia educación superior ha de emprender la transformación y la renovación más radicales que jamás haya tenido por delante, de forma que la sociedad contemporánea, que en la actualidad vive una profunda crisis de valores, pueda trascender las consideraciones meramente económicas y asumir dimensiones de moralidad y espiritualidad más arraigadas (Unesco, 1998, p. 26).

Es decir, se necesita que las instituciones de educación superior que forman gerentes de la seguridad asuman, en sus procesos de formación profesional, la perspectiva de la investigación con proyección y responsabilidad social. Esta es una respuesta a la necesidad de contar con un profesional de la seguridad que aporte al desarrollo de la seguridad pública y privada del país. El gerente de la seguridad integral ha de tener entonces la capacidad, gracias al pensamiento estratégico y complejo, de enfrentar el reto de proteger a la organización de riesgos y amenazas que la puedan destruir, en un mundo lleno de la incertidumbre propia de este periodo histórico de la sociedad del conocimiento, la globalización, las organizaciones terroristas y los nuevos riesgos que hacen presencia a nivel global.

Todos estos elementos conducen a que el estudiante desarrolle competencias para la investigación. De acuerdo con Gallardo (2003), estas competencias permiten desarrollar habilidades para la indagación, la innovación, la gestión gerencial, el uso de la tecnología, así como habilidades comunicativas para la conformación de redes y divulgación de la producción intelectual aplicada a la seguridad integral. Asimismo, a través del currículo de los programas de pregrado y postgrados en seguridad se debe buscar desarrollar las competencias

investigativas para el diseño y desarrollo de proyectos orientados a la resolución de problemas. La aplicación de los conocimientos, habilidades y actitudes necesarias en la investigación son clave en ese proceso formativo.

De tal forma, deben desarrollarse actividades para familiarizar al estudiante con el proceso mismo de investigación y para formarlo como futuro investigador. Debe haber una estrategia didáctica y pedagógica en la que converjan los aportes teóricos y las prácticas, una estrategia cuyo objetivo sea consolidar los saberes propios del objeto de estudio de la seguridad. Para el caso de la formación del gerente de la seguridad integral, se deben proyectar los distintos pasos del proceso investigativo que lleven a la solución de un problema específico. Con relación a este, el educando debe poder aplicar lo aprendido teóricamente, además de confrontar las hipótesis e ideas con sus conocimientos previos y analizar conjuntamente el desarrollo del propio proceso de investigación en la solución de problemas de seguridad.

La investigación formativa, por su parte, ha sido abordada y definida por diferentes autores como el proceso que desarrolla en el estudiante competencias para resolver problemas, en un contexto determinado, utilizando los pasos del método científico. Para Lara (2006), la investigación formativa desarrolla en el estudiante un pensamiento autónomo, crítico, frente a un problema para darle solución. Así, el estudiante que se inicia en la investigación en seguridad se debe orientar a la construcción de nuevo conocimiento y ser capaz de desarrollar competencias para resolver problemas. Este proceso formativo se caracteriza porque el docente es quien acompaña y orienta el proceso de investigación. Conduce entonces al estudiante a que examine una situación dada y plantee una hipótesis, interprete, analice información, argumente y proyecte posibles soluciones.

En este punto, es pertinente resaltar la importancia de que los docentes que enseñan módulos de seguridad sean investigadores y desarrollen las clases con una metodología de aprendizaje basada en problemas. Los docentes deben motivar la indagación como metodología de enseñanza para desarrollar competencias en investigación. Esto exige, de parte de ellos, una práctica didáctica en el aula, pues son los actores vitales del desarrollo de la investigación; son los líderes académicos en el desarrollo de las competencias investigativas de los estudiantes y futuros gerentes de la seguridad integral.

Además, se debe institucionalizar la investigación en las instituciones de educación superior que cuenten con programas de seguridad integral. De acuerdo con Villaveces (2003), los currículos y la organización administrativa de las instituciones deben reflejar que ellas privilegien e impulsen las competencias en investigación y la producción de nuevos conocimientos.

Diferentes tratadistas han establecido una serie de competencias que la investigación formativa tiene que desarrollar en el estudiante. Maldonado (2010, p. 199) afirma que los estudiantes, futuros profesionales, deben poseer las siguientes competencias para desarrollar procesos de investigación.

Competencias para la investigación

- Reconocer qué fenómenos o acontecimientos pueden ser explicados en el marco de una determinada ciencia.
- Comprender lenguajes abstractos que permitan hacer representaciones conceptuales.
- Construir representaciones o modelos de explicación de fenómenos o acontecimientos empleando nociones o conceptos de las ciencias.

- Formular preguntas o plantear problemas según modos de representación de las ciencias.
- Resolver problemas empleando métodos teorías y conceptos de las ciencias.
- Capacidad de usar comprensivamente instrumentos tecnológicos y fuentes de información.
- Emplear los conocimientos para predecir los efectos de las acciones y juzgar qué tan adecuadas serían.
- Aplicar el conocimiento adquirido en nuevos contextos y situaciones reconociendo límites y condiciones.
- Emplear los conocimientos adquiridos en la apropiación de nuevos conocimientos.
- Indagar, observar y buscar explicaciones sobre problemas identificados.
- Cuestionar las interpretaciones propias y ajenas con argumentos coherentes.
- Profundizar en las preguntas reconocidas como legítimas o valiosas y realizar el esfuerzo necesario, según una disciplina, para avanzar en el campo abierto por esa pregunta.
- Reconocer la existencia y la validez de diferentes formas de aproximación a los problemas atendiendo a la naturaleza de los mismos y a los intereses de la investigación.
- Acudir a las representaciones, los métodos y las fuentes adecuadas para resolver un problema o dar razón de un fenómeno o acontecimiento.
- Compartir conocimientos y expresar clara y coherentemente los propios puntos de vista.
- Fundamentar los puntos de vista con razones, fenómenos o acontecimientos.

- Presentar y representar las ideas de distintos modos, atendiendo al contexto y representando las especificaciones del interlocutor (atender a los presupuestos de la comunicación).
- Intercambiar flexiblemente ideas, reconociendo intereses y formas de trabajo y de argumentación diferentes.
- Reconocer la validez de otros puntos de vista y tener la disposición para establecer acuerdos relacionales.
- Explorar los condicionamientos y limitaciones del propio punto de vista. Analizar críticamente el sentido de las propias acciones (autorreflexión).
- Seleccionar, jerarquizar e interpretar información y hacer inferencias sobre argumentos previos.
- Analizar críticamente las fuentes de información y contrastar distintas informaciones usando criterios racionales (Maldonado, 2010, p. 199).

Lo anterior significa que un gerente de la seguridad debe contar con competencias que se apoyen mutuamente en el pensamiento estratégico y la capacidad de investigar. Esto le permite al gerente proteger la organización de los constantes riesgos, provenientes del crimen organizado y las nuevas amenazas tecnológicas que avanzan de manera acelerada. El caso de los delitos tecnológicos, que impactan constantemente las organizaciones en el contexto actual, supone múltiples desafíos que implican conocer y analizar los diversos riesgos que amenazan la seguridad integral en las organizaciones de todo tipo (público y privado). Esto exige que el gerente de la seguridad tenga una actitud hacia la investigación asociada a un pensamiento estratégico para proteger la organización.

Al analizar los diferentes riesgos que pueden afectar una institución, se debe primero elaborar una matriz de riesgos que permita crear

un conjunto de medidas de seguridad inmersas en los procesos y estructuras organizativas existentes. Sánchez define la seguridad como "cantidad de exención de todo peligro, daño o riesgo" (Sánchez, 2008, p. 14). Del mismo modo, para Vallejo (2002), la seguridad parte de la percepción y sensación de un entorno tranquilo. Esta percepción le permite a una persona u organización actuar de manera confiada, serena, sin temor y libre de amenazas.

Conviene decir que la investigación es una competencia que debe desarrollar y utilizar constantemente un gerente de la seguridad. Además, es responsabilidad de los centros de estudios en seguridad encaminar la formación hacia procesos de investigación y el desarrollo del pensamiento crítico. Al respecto, Miyahira Arakaki (2009) muestra cómo la investigación formativa desarrolla en los estudiantes las capacidades de indagar, observar y buscar explicaciones para problemas del contexto. También, el currículo debe dinamizar las metodologías de enseñanza y los procedimientos operativos en el proceso de investigación.

Cabe indicar que gestionar la investigación en la seguridad integral permite la construcción de nuevos saberes y el desarrollo habilidades para la indagación y exploración de nuevos conocimientos; especialmente, conocimiento de tipo tecnológico y científico aplicable a la seguridad integral. Sabino define la investigación "[...] como el proceso mediante el cual un sujeto (el investigador) se encamina hacia los hechos para obtener respecto a ellos un conocimiento científico, es decir de cierta naturaleza y características" (Sabino, 1976, p. 41).

Dentro de este contexto, de acuerdo con Restrepo (2003), la investigación es un proceso de construcción de nuevo conocimiento. Este proceso se caracteriza por la creatividad, las ideas innovadoras,

que permiten abordar e interpretar algo oculto pero existente en la realidad. Ciertamente, un gerente de la seguridad ha de tener también competencias orientadas a los resultados. Además, debe promover la mejora continua de los procesos de seguridad, seleccionar, jerarquizar e interpretar la información de los diferentes riesgos y amenazas que puedan afectar a la organización. A partir de esa información, debe hacer inferencias que lleven a acciones de mejora. Por supuesto, el proceso debe basarse en argumentos previos, y debe cuestionar las interpretaciones propias y ajenas con argumentos coherentes, acudiendo a las representaciones sistémicas, los métodos de investigación y las fuentes adecuadas para resolver un problema que vulnere la seguridad de la empresa.

La gestión de la seguridad es una competencia que ofrece habilidades para dirigir y gestionar los procesos de seguridad integral, mediante los cuales se reducen a su mínima expresión los factores de riesgo que afectan la productividad y competitividad en las organizaciones. Estas, a su vez, enfrentan riesgos cada vez más complejos. Por tal motivo, deben asegurarse de que su capital humano en seguridad posea las competencias apropiadas para hacer frente a los riesgos que más probablemente los puedan afectar y pongan en riesgo sus activos vitales.

En suma, desde la perspectiva de la seguridad en la protección de activos vitales de una organización, el pensamiento estratégico y las competencias en investigación son herramientas vitales para la gestión de la seguridad integral. Son herramientas que deben estar presentes en la formación de un gerente de la seguridad para poder construir y articular modelos y planes de seguridad que permitan alcanzar los objetivos planteados por la empresa, protegiéndola de todas las amenazas y riesgos posibles.

Conclusiones

En suma, la formación de los profesionales en seguridad se debe encaminar hacia una construcción del conocimiento que sea pertinente y responda a los problemas fundamentales de la sociedad actual. Esto se logra a través de la comprensión de la complejidad y la construcción de conocimiento, pues este es un elemento esencial que favorece un adecuado desarrollo formativo. Un gerente de la seguridad integral debe desarrollar un pensamiento estratégico y competencias para la investigación. Estas le permitirán predecir y adelantarse a los diversos y constantes riesgos y amenazas que debe enfrentar la organización o empresa a la que presta sus servicios profesionales.

En el proceso de formación de un gerente de la seguridad, la aplicación del pensamiento complejo es una experiencia enriquecedora. Como una herramienta de reflexión, es ante todo un pensamiento que relaciona los elementos en contexto. Esto es útil para la creación de modelos de seguridad, según los conceptos propuestos por Edgar Morin y su aplicación.

El desarrollo de competencias en investigación le permitirá al gerente de la seguridad abordar metodologías de exploración para la solución de problemas de su cargo. Igualmente, estará en la capacidad de construir una política de prevención y enfoques ajustados a enfrentar el riesgo, la evaluación del riesgo y la gestión integral preventiva. Todo esto contribuye a reducir a su mínima expresión las diferentes amenazas que debe afrontar una organización en su actividad económica.

El pensamiento estratégico y las competencias en investigación son herramientas que le permiten al gerente de la seguridad, a partir de su racionalidad, crear modelos de seguridad para proteger a las organizaciones públicas o privadas. Estas están en constante riesgo y

enfrentan amenazas, que ponen en peligro su estabilidad y funcionamiento, provenientes del crimen organizado.

La seguridad debe ser abordada, no solo a partir del pensamiento estratégico, sino del paradigma complejo. Este permite ver las amenazas y riesgos enfrentados por cualquier organización o empresa en su actividad económica como un todo. La seguridad tiene un nombre, pero muchos apellidos (la seguridad que abarca la infraestructura crítica, ambiental, la ciberdefensa y ciberseguridad, seguridad laboral y mucha más).

Lo antes señalado significa que la seguridad de una organización no se puede parcelar. La seguridad no puede ser abordada aisladamente, o por silos, en partes sin una relación entre sí. Ese tipo de abordaje es más bien característico del pensamiento tradicional, que desarrolla el tema de la seguridad de un modo disciplinar y no a partir de la relación de las diversas disciplinas que actualmente están al servicio de la seguridad integral. La seguridad debe entonces entenderse a través de la multidisciplinariedad, interdisciplinariedad y transdisciplinariedad, características que no pueden faltar en los equipos de trabajo que abordan los estudios de seguridad.

Las competencias investigativas de un gerente de la seguridad deben proporcionarle un conjunto de herramientas teóricas y prácticas de carácter multidisciplinario para lograr habilidades y destrezas de utilidad para el análisis, diseño e implementación de sistemas integrales de seguridad. En su labor, debe emplear una planeación estratégica, métodos de evaluación, control y aplicación eficiente de procesos, a fin de diseñar soluciones efectivas para problemas críticos. Igualmente, debe tomar decisiones oportunas contrarrestando situaciones de incertidumbre o riesgo que puedan afectar los recursos vitales de una organización.

Los autores abordados coinciden en que las competencias en investigación se deben orientar a resolver problemas empleando métodos, teorías y conceptos de las diferentes ciencias. Esto genera la capacidad de usar instrumentos tecnológicos y fuentes de información comprensivamente, los cuales le permitan al futuro gerente de la seguridad integral desempeñarse como un constante investigador apoyado en fundamentos científicos para salvaguardar de riesgos y amenazas a la organización para la cual trabaje.

Referencias

Álvarez, H. y Kuratomi, I. 2005. *Pensamiento estratégico en mantenimiento.*

Castañeda, L. (2001). *Pensar, tarea esencial de líderes y gerentes.* Ediciones Poder.

Davies, W. (2000). Understanding Strategy. *Strategy and Leadership, 28*(5), 25-30. https://doi.org/10.1080/02626667

Delamer, G. R. (2005). *Estratégia: para la política, la empresa y la seguridad.* Instituto de Publicaciones Navales.

Fierro, C., Fortoul, B. & Rosas, L. (2002). *Transformando la práctica docente. Una propuesta basada en la investigación-acción.* Paidós.

Gallardo, O. (2003). Modelo de formación por competencia para investigadores. *Contexto y Educación, 18*(70), 9-25. https://doi.org/10.21527/2179-1309.2003.70.9-25

García de Mujica, D., & Daza, A. (2006). Inferencia del proceso de pensamiento estratégico basado en modelos y tendencias. *Telos, 8*(1), 34-50. https://doi.org/10.1080/02626667

Gonczi, A., & Athanasou, J. (1996). Instrumentación de la educación basada en competencias. En A. Argüelles (comp.), *Competencia laboral y educación basada en normas de competencia* (pp. 272-273). Limusa/SEP/CNCCL/CONALEP.

González, C., Tornimbeni, S., Corigliani, S., Gentes, G., Ginochio, A., & Morales, M. (2012). Evaluación de competencias requeridas para investigar.

Anuario de Investigación de la Facultad de Psicología, 1(1), 142-151. https://doi.org/10.1080/02626667

González, S. (1997). *Pensamiento Complejo.* Editorial Magisterio.

Jatar, J. (2000). *El pensamiento estratégico y el mercado laboral*. http://www.caveguias.com.ve/clasificados/trabajo/articulo38.html

Krell, H. (2009). *El pensamiento estratégico*. http://www.ilvem.com/shop/otraspaginas.asp?paginanp=348&t=EL-PENSAMIENTO-ESTRAT%C3%89GICO.htm

Lara Rodríguez, G. (2006). Investigación formativa. Una visión integral para profesiones de la salud. *Revista Ciencia y Salud*, 4. 161-176.

Levy-Leboyer, C. (2000). *Gestión de las competencias*. Ediciones Gestión S. A.

Maldonado, M. A. (2010). *Currículo con enfoque de competencias*. Ecoe Ediciones.

Miyahira Arakaki, J. M. (2009), La investigación formativa y la formación para la investigación en el pregrado. *Revista Médica Herediana, 20*(3), 119-122. https://doi.org/10.1080/02626667

Morin, E. (1990). *Introducción al Pensamiento Complejo*. Editorial Gedisa.

Morin, E. (2010). *¿Hacia el abismo?, globalización en el siglo XXI.* Paidós.

Morin, E. (2011). *La vía para el futuro de la humanidad.* Paidós.

Mulder, M., Weigel, T., & Collins, K. (2007). The Concept of Competence in the Development of Vocational Education and Training in Selected EU Member States: A Critical Analysis. *Journal of Vocational Education & Training, 59*(1), 67-88. https://doi.org/10.1080/13636820601145630

Ohmae, K. (2004). *La mente del estratega*. McGraw-Hill /Interamericana de México, S. A.

Ouellet, A. (2000). La evaluación formativa al servicio de las competencias. *Revista Escuela de Administración de Negocios, 41*, 30-42. https://journal.universidadean.edu.co/index.php/Revista

Pernía, J. (2014). *Pensamiento estratégico en directores de instituciones educativas nacionales de educación media general* [Tesis de Maestría]. Universidad del Zulia.

Porter, M. (1996). What is Strategy. *Harvard Business Review, 74*(6), 61-78. https://doi.org/10.1080/02626667

Restrepo G. (2003). Investigación formativa e investigación productiva de conocimiento en la Universidad. *Revista Nómadas 18*, 195-202. https://doi.org/10.1080/02626667

Robert, M. (2006). *El nuevo pensamiento estratégico. Puro y Simple*. Mc Graw-Hill.

Sabino, C. (1978). *El proceso de investigación*. El Cid Editor.

Sánchez, J. (2007). *Gerencia estratégica de las organizaciones del siglo XXI*. http://dspace.ucbscz.edu.bo/dspace/bitstream/123456789/13177/1/10007.pdf

Sánchez, M. (2008). *Manual para el Director de Seguridad*. Estudios Técnicos.

Tobón, S. (2013). *Formación integral y competencias: pensamiento complejo, currículo, didáctica y evaluación*. Ecoe Ediciones.

Unesco. (1998, 5 de octubre). *La educación superior en el siglo XXI Visión y Acción*. Documento final sobre conferencia de Educación Superior Mundial. Paris.

Vallejo, S. (2002). *Vademécum de la seguridad*. Talleres Graficolor.

Villaveces, J. L. (2003). *70 Años de ciencia y tecnología en Colombia* [Documento de trabajo]. Observatorio Colombiano de Ciencia y Tecnología.

Vivas, R. (2000). *Gerencia y pensamiento estratégico* [Material de trabajo]. Universidad Rafael Belloso Chacín (Urbe).

Weiberger, K. (2009). *Estrategia. Para lograr y mantener la competitividad de la empresa*. Ministerio de la Producción, Perú.

PARTE 2

Gestión en seguridad

Capítulo 4

Gestión del riesgo, reflexiones en América Latina[1]

Alejandro Ortiz Ríos*
Oscar I. Parra**

1 Capítulo de libro resultado del proyecto de investigación *Impacto de las políticas de Seguridad Integral en el desarrollo y gestión del componente de investigación del currículo* MADGSI, de la línea de investigación Seguridad Integral del grupo de investigación CIPAER, con código COL 0093003, de la Escuela de Postgrados de la Fuerza Aérea Colombiana.

* Magíster y especialista en Seguridad y Defensa Nacional de la Escuela Superior de Guerra de Colombia. Administrador Aeronáutico. Correo electrónico: alejandro.ortiz@fac.mil.co

** Estudiante de Maestría en Estudios Políticos Latinoamericanos de la Universidad Nacional de Colombia. Sociólogo e Internacionalista de la Pontificia Universidad Javeriana. Investigador. Correo electrónico: oscarparra9405@gmail.com

CÓMO CITAR

Ortiz Ríos, A., & Parra, O. (2020). Gestión del riesgo, reflexiones en América Latina. En Y. Rico, D. López Cortés, & A. Cerón R. (comps.), *Enfoques y gestión en Seguridad Integral* (pp. 105-128). Escuela de Postgrados de la Fuerza Aérea Colombiana. https://doi.org/10.8667/9789585996199.04

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

CAPÍTULO 4.
Gestión del riesgo, reflexiones en América Latina

https://doi.org/10.8667/9789585996199.04
Bogotá, Colombia
Noviembre, 2020

RESUMEN

Para comprender la constitución de los riesgos y sus elementos adjuntos, es necesario reflexionar sobre las discusiones teóricas y epistemológicas al respecto. Por ende, es oportuno un debate sobre la gobernabilidad y un estudio de las nuevas aproximaciones a la conceptualización y gestión de los riesgos. Estos nuevos análisis, como el enfoque basado en procesos, liderado por Allan Lavell, se construyen a partir de las observaciones de los procesos y los elementos locales necesarios para ampliar las percepciones del riesgo. Los esfuerzos por unificar los procesos de la gestión de riesgos son fundamentales para su mitigación. Esto es particularmente cierto en América Latina, donde hay que reconocer la complejidad de sus problemas de seguridad.

PALABRAS CLAVE

América Latina; gobernabilidad; planificación social; prevención de riesgos; sociología política.

Gestión del riesgo: ¿Concepto rígido o en construcción?

El objetivo del presente escrito es contribuir al análisis de los elementos situacionales y los actores involucrados en la identificación de vulnerabilidades y la formulación de soluciones ajustadas a las necesidades y capacidades de la región latinoamericana. Estas soluciones se pueden lograr a través de la cooperación internacional entre países y organizaciones internacionales, gubernamentales y civiles. En especial, se pretende resaltar el cambio en la conciencia general de los actores, quienes ven la necesidad de protegerse conjuntamente de los riesgos y de las amenazas emergentes, producto de la actual época tecnológica y económica. Solo a través de este tipo de ejercicios de reflexión se hace una contribución sustancial a la formulación y el moldeamiento de sistemas de gestión de riesgo.

El texto está organizado de manera que se esclarecen las formas de gestión del riesgo y las instituciones e intereses involucrados. En el primer apartado, se hace un recuento teórico-descriptivo de la gestión de los riesgos y de las amenazas a la seguridad de los Estados y las sociedades. Después de haber identificado los conceptos pertinentes, y en concordancia con ellos, se procede a caracterizar y a cuestionar la gobernabilidad y la posibilidad de un nuevo multilateralismo. En el último apartado, se busca en el enfoque basado en procesos el funcionamiento agencial y organizacional de un sistema de gestión de riesgos para América Latina.

En principio, es imperativo resaltar la necesidad de un sistema de gestión del riesgo para cualquier gobierno, sea nacional o local. Su importancia radica en la percepción constante e inevitable de que se tiene un control limitado sobre las acciones humanas y los procesos

naturales que afectan a la humanidad. Esto es lo que se denomina comúnmente como inseguridad. Las normativas y las instituciones humanas son construidas, en este sentido, para disminuir la incertidumbre sobre las consecuencias y las expectativas. En consecuencia, las instituciones encargadas de la seguridad se articulan en torno a la percepción del riesgo y a la identificación de las amenazas, en su respectivo orden de prioridad.

Para lograr sentirse seguro, se deben organizar las acciones de acuerdo con el entendimiento que se tenga de los riesgos y las posibilidades para contenerlos. Es claro que la ejecución de las estrategias no reducirá necesariamente el miedo social o el pánico moral. Pero la construcción de la gestión del riesgo necesita proveer a las sociedades de seguridad, además de afrontar las amenazas materiales. El riesgo implica un cálculo de los efectos de determinado fenómeno sobre la realidad social, que puede impedir el funcionamiento normal del sistema o interrumpir las interacciones. Niklas Luhmann afirma que el cálculo del riesgo es la contraparte secular del cálculo religioso del arrepentimiento; una relación causal vista en términos de tiempo. Sin embargo, el problema con la evaluación de las causas radica en la insuficiencia de la información que se tiene sobre el futuro y sobre las consecuencias de las acciones humanas. Por tanto, la relación entre el grado de la pérdida y su probabilidad son determinantes para las consideraciones pragmáticas-racionalistas del riesgo (Luhmann, 1993).

La diferencia que hace la teoría de Luhmann es la inclusión de la observación de segundo orden; es decir, el momento en el que el observador realiza la distinción de los límites conceptuales. Las observaciones y los significados son, entonces, transmitidos en las comunicaciones, de modo que el otro es capaz de entender la distinción hecha por el observador: "el riesgo se reconoce en la distinción de sus límites conceptuales" (Luhmann, 1993, p. 18). Sin embargo, el primer

observador reconoce el riesgo mediante el conocimiento que tiene disponible, mientras que el segundo observador observa al primero y juzga la ejecución y el criterio de observación inicial del riesgo. Para el segundo observador, el primero hace atribuciones al riesgo que direccionan su propia definición en relación con eventos, estructuras y organizaciones. No obstante, esta identificación de la atribución no es observable en plazos más largos porque se vuelve al problema de la causalidad para explicar el origen de la acción. Por tanto, se debe identificar el riesgo como una atribución que hace un observador en una situación determinada y con cierta posibilidad de materialización (Luhmann, 1993).

Es un hecho autoevidente que todo suceso o decisión conlleva riesgos. La realidad no solamente conduce a múltiples acontecimientos riesgosos o peligrosos, sino que los riesgos mismos se convierten en interpretaciones complejas porque son el resultado de un ejercicio de observación. En este sentido, la complejidad no solamente radica en la resolución del riesgo, sino en lo que significa perder para quien observa. Hay aquí un intercambio teórico entre el institucionalismo y el constructivismo entrono a la interpretación del riesgo (Beck, 2009). Ulrich Beck identifica la responsabilidad individual y social de los riesgos, porque algunos atañen a unos pocos y otros a la mayoría o a la totalidad de los sujetos. Con esta bifurcación de correspondencia del riesgo, Beck hace en su teoría un llamado moral a la "responsabilidad para *comunidades del riesgo* que no se encuentran necesariamente localizadas espacialmente" (Beck, 2009, p. 188). Para Beck, la emergencia del cosmopolitismo es la respuesta al riesgo global, una toma colectiva de responsabilidad por este. Según él, "la unificación de los riesgos es condición *sine qua non* para el cosmopolitismo" (Beck, 2009, p. 198).

En la actualidad, los riesgos no solamente han cambiado objetivamente, sino que se han diversificado en la percepción de los actores. Desde el final de la Guerra Fría, diversas disciplinas empezaron a sostener que la política cambió y que tendría una naturaleza diferente a la que tenía en la configuración anterior del mundo. Afirmaban que en el mundo actual se propendería por una multipolaridad del poder y habría una emergencia de nuevas amenazas para los Estados y para la humanidad. Ciertamente, no se puede hablar de nuevas amenazas si estas ya tenían lugar en el pasado. La diferencia es que el enemigo, al menos en la Guerra Fría para desde la perspectiva de Occidente, era el comunismo soviético. Por otra parte, desde la década de los setenta ya se había alertado a la comunidad internacional sobre los daños ecológicos causados por la actividad humana, así como sobre la expansión global del narcotráfico y la conformación de grupos extremistas islámicos dada en la década de los ochentas. La novedad del riesgo post Guerra Fría es la permanencia de las antiguas problemáticas legales, culturales y económicas en la escena internacional. Los riesgos previamente existentes eran percibidos, pero no eran priorizados por las agendas políticas de los actores porque su importancia era menor al riesgo que representaba el comunismo, incluso dentro de las sociedades occidentales.

Esto evidencia la existencia de una construcción social del riesgo. Más allá de las percepciones de los observadores, los sistemas sociales dan prioridad a unos riesgos sobre otros. El riesgo de un desastre, por ejemplo, es construido socialmente con base en las creencias, las necesidades y las prácticas sociales. El entendimiento del riesgo es constreñido por las percepciones de los eventos materiales y el desplazamiento de otras prioridades sociales.

En concordancia con Luhmann, Oliver-Smith et al. (2017) plantean que la emergencia del riesgo depende del tiempo, pues el riesgo

se expresa solamente a través de las condiciones sistémicas que lo permiten. Sin embargo, los autores reconocen que los analistas del riesgo deben realizar una interpretación metaanalítica para lograr aprehender genéricamente las condiciones materiales e idiosincráticas del riesgo. Hay que tener en cuenta que las observaciones que provienen de los grupos sociales están íntimamente relacionadas con la estructura social y su percepción de exposición al riesgo. Necesariamente, el análisis se debe hacer contemplando la desigualdad de los riesgos, que se distribuyen en diversas instancias de la sociedad. Algunos riesgos afectan a unas clases sociales más que otras, mientras otros riesgos afectan a toda la población. Los grupos sociales son motivados a producir reaccionar y responder de forma diferente, dependiendo de sus vinculaciones ideológicas.

En el panorama global del riesgo, se observa un aumento de la consciencia sobre los riesgos ambientales, que han relegado a otras problemáticas locales. Esto se debe a una creciente exposición del público a la idea de eventos extremos y a gran escala. Para entender este fenómeno, se puede recurrir a la imagen de las razones humanitarias; allí se antepone una razón ética y empática para enfrentar una situación de riesgo externa. Este es un sentido de responsabilidad que concierne a la humanidad, pero no requiere de ella un acto filantrópico, sino uno eminentemente egoísta. No hay control de los desastres naturales, sino de la exposición y la vulnerabilidad a estos (Lavell, 2012). De esta manera, el cuidado del otro se convierte en el cuidado propio.

La reflexión alrededor del origen y de la gestión del riesgo plantea variados cuestionamientos relacionados con el enfrentamiento de la vulnerabilidad de la condición humana, que se contrapone a la inevitabilidad del riesgo. Por tanto, se debe preguntar ¿La construcción del riesgo se da constantemente? Si es así, los sistemas de gestión de riesgo no pueden permanecer inmóviles, pues resultarían anacrónicos.

La gestión del riesgo, en consecuencia, debe estar aunada al desarrollo de la historia y de las relaciones sociales.

Crisis de la gobernabilidad del riesgo

El Estado como paradigma de la modernidad es fundamental para la gestión del riesgo, pues concentra el poder político y jurídico, así como la capacidad burocrática y administrativa. Con estos poderes y capacidades, el Estado ha sido el encargado de la seguridad de los ciudadanos y de la manutención del orden social, como fue establecido, según las doctrinas liberales, en un contrato social. Ahora bien, si se toma en consideración que la autoridad del Estado no alcanza a cubrir la totalidad de la población, por problemas de legalidad y de legitimidad, nos encontramos en una situación de ingobernabilidad.

Idealmente, un gobierno podrá ejercer una gobernabilidad plena en la medida en que logre tener control sobre su territorio y sobre los procesos sociales dentro de los límites de su marco legal constitutivo. Sin embargo, la práctica institucional y jurídica presentan constreñimientos y conflictos que se dan con diversos grupos sociales por razones económicas, legales, ideológicas, religiosas o étnicas. Sin duda, el gobierno soberano no logra ser absoluto debido a la dificultad de sostener relaciones armoniosas con la totalidad de la sociedad. Sin embargo, el objetivo de la gobernabilidad es, más allá de buscar y garantizar la satisfacción de todos los ciudadanos, mantener el orden social a través de la imposición y el cumplimiento de principios básicos para la estabilidad del sistema político.

En términos generales, el ejercicio del poder debe ser delegado a las instituciones y agencias del Estado, las cuales mantienen el contacto y negocian las condiciones de vida de los ciudadanos. Según visiones clásicas de la política, esta irrigación institucional en la vida social

permite mantener la legitimidad del orden instituido. Por ejemplo, si el desempleo aumenta, también aumenta el descontento, lo que puede evocar la inestabilidad del mercado laboral o de la producción económica. Por otra parte, la censura a la expresión podría llevar a formas clandestinas de organización política.

La relación que la gobernabilidad tiene con el riesgo es precisamente su gestión; es decir, la gobernabilidad busca gestionar el riesgo. Sin embargo, la transformación de las relaciones sociales y de la concepción de la política lleva a la búsqueda de nuevos objetivos estatales para su regulación. Es claro que las nociones de la seguridad han cambiado y las prioridades del Estado se han diversificado, pues la diferenciación social ha aumentado la complejidad de las demandas sociales, de los valores y las preferencias. En adición, las interacciones internacionales que se explican a través del concepto de globalización también plantean un desafío a la gobernabilidad, ya que varios sucesos que se presentan dentro del Estado tienen relación directa o indirecta con otros territorios soberanos, sean legales o ilegales; por ejemplo, migraciones irregulares o el mercado de armas o drogas.

En este sentido, la gobernabilidad debe expandirse buscando el intercambio de información con otras autoridades estatales y entablando relaciones cooperativas interagenciales. Es más, el Estado debe nutrirse de otras fuentes de poder, como el económico o el social, porque la complejidad de los riesgos implica la necesidad de respuestas compartidas y complementarias con otros sectores de la sociedad que también perciben el riesgo. En consecuencia, el Estado no es el único que acapara la definición ni la respuesta del riesgo.

Los ciudadanos también perciben como un riesgo una ineficiente administración del Estado o la cooptación de las políticas públicas por parte de capitales privados o extranjeros. Por tanto, para la manutención de la democracia, o cualquier forma de organización sociopolítica,

los ciudadanos también exigen y ejercen control sobre la organización y las acciones del Estado, esto es a lo que se refiere el término inglés *accountability*. Este se basa en la amplia validez de la idea metafísica del contrato social sobre el que se funda la sumisión de los grupos sociales a la autoridad del Estado.

En un sentido amplio, el concepto de *accountability* contribuye al fortalecimiento de la gobernabilidad, pues otras fuentes de poder estratégicas, de carácter no gubernamental, participan en el control de las decisiones de la autoridad estatal y en la delimitación de los espacios de interacción política (Canale-Mayet & Olivares, 2014, p. 13). A medida que aumente esta participación, aumentaría también la divulgación de las normas/instituciones y el consenso alrededor de estas, lo que finalmente favorecería la gobernabilidad.

En última instancia, la gobernabilidad implica un acuerdo con los actores con potencia desestabilizadora que permite el avance de la empresa política y la agenda económica Gobierno; la gobernabilidad no va a resolver los conflictos sociales. Sin embargo, como parte esencial del análisis del riesgo, se debe tener en cuenta, en cierta medida, las demandas sociales si no se quiere perder gobernabilidad debido al deceso de la legitimidad. En consecuencia, el *accountability* puede verse como un necesario retorno de la política al sistema social, una demanda de legitimidad. En principio, esta se ejerce desde la elección de gobernantes hasta la rendición de cuentas de un gobierno. Por tanto, el *accountability* enlaza la gobernabilidad a las demandas sociales, en las que están implicadas las percepciones del riesgo.

La gobernabilidad incluye la tradicional limitación de la violencia privada y la reafirmación de la soberanía del Estado. Simultáneamente, se persigue la estabilidad del sistema social, que permite a los ciudadanos sobrevivir y disfrutar de la libertad dentro de las posibilidades del mercado y de la legalidad. La gobernabilidad adquiere

entonces una relación importante con las concepciones actuales de la seguridad, como la seguridad humana (Canale-Mayet & Olivares, 2014).

Si no hay gobernabilidad, prima el conflicto social sobre la autoridad: cada grupo social o económico buscará en otras fuentes de poder las vías para gestionar los riesgos que ellos mismos perciben. La inestabilidad del gobierno no permitirá la unificación de los riesgos ni la formulación de una agenda integral para gestionar el riesgo. Por esta razón, dentro de los estudios de seguridad se propone un nuevo multilateralismo como solución a una crisis de gobernabilidad (o cuando menos una deficiencia del Estado para gestionar los riesgos por sí mismo). Este multilateralismo no solo funciona con actores locales, sino con agendas internacionales, como alianzas entre Estados que buscan objetivos similares, o alianzas con el sector privado y la sociedad civil para los siguientes temas: seguridad, economía y principios éticos (Waschuk, 2001).

El nuevo multilateralismo requeriría de una compatibilidad ideológica y una correspondencia de proyectos políticos, los cuales abren espacios para la participación de nuevos actores interesados. En la construcción de nuevas redes de grupos civiles, especialmente alrededor de las dinámicas de la globalización económica, organizadas mediante las tecnologías de comunicación globales, se forjan nuevas relaciones con los riesgos. Estas se refieren no solamente a su determinación, sino también al intercambio para fijar cursos de acción orquestados entre las diferentes localidades y grupos sociales[2].

2 "Rather than trading concessions with other states or nonstate actors, many negotiations today involve processes of mutual learning, with participants exchanging best practices and identifying comparative advantages in jointly tackling seemingly intractable multidimensional problems such as complex political emergencies" (Waschuk, 2001, p. 218).

Surge un cuestionamiento fundamental en esta dinámica inclusiva del nuevo multilateralismo. Con el aumento de la participación de los grupos civiles nacionales e internacionales a través de la presión política en medios de comunicación masiva, ¿hay un aumento real de su capacidad de negociar las agendas políticas o se trata más bien de ejercicios retóricos de la inclusión de las sociedades en la gestión del riesgo para mantener la gobernabilidad? Se puede argüir que el nuevo multilateralismo les permite a los grupos civiles de interés amplificar su voz en los procesos de negociación de las agendas políticas. Esto se hace cuestionando, o reclamando públicamente por, la decisión de alguna autoridad estatal o de un organismo multilateral. Al mismo tiempo, sin embargo, la gestión del riesgo corresponde realmente con los intereses de quienes tienen poder de influencia y desestabilización del orden.

De acuerdo con Ken Booth (2007), se ha llegado a una crisis decisional con respecto a los intereses vitales universales. Esta crisis se ilustra en seis situaciones paradójicas vigentes: 1) "hoy emerge un dilema de seguridad, como muestra de desconfianza y miedo, que tiene relación con los nuevos poderes regionales y las amenazas no tradicionales" (Booth, 2007, p. 403); 2) "se vislumbran las amenazas de la globalización, a la que subyace la economía global como proyecto, en contraposición a un *mundo más pequeño* como proceso" (Booth, 2007, p. 407); 3) "es percibido un estrés poblacional, pues la relación población-recursos provoca conflictos económicos" (Booth, 2007, p. 408); 4) "la destrucción de la naturaleza está conduciendo al colapso de los sistemas sociales, lo cual debe ser enfrentado intergeneracionalmente, a través de reformas en la producción o del cambio del sistema" (Booth, 2007, p. 409); 5) "también se encuentra una sobrecarga en la gobernanza que privilegia la prevención y el control, lo que desemboca en una nueva conciencia global y posibles contrapoderes" (Booth, 2007, p. 413), por último, 6) Booth expresa su

preocupación ante "la *temporada de la sinrazón,* una época de confusión y de contradicción ideológica entre sentimientos anticapitalistas, consumistas, radicales/violentos y apocalípticos" (Booth, 2007, pp. 416-419).

Ante este panorama complejo, la organización del multilateralismo no solo no debe obedecer a una lógica de la gobernabilidad y del control intensivo, sino que debe entender que la gestión del riesgo se basa en las interacciones locales entre la cultura y la naturaleza. Desde la postura del riesgo global, las transformaciones imperiosas responden a las formas de producir globalmente y a la distribución de la riqueza para disminuir los conflictos sociales de base y aumentar la legitimidad/participación/colaboración en la gestión de los riesgos.

La gestión del riesgo a partir de un enfoque basado en procesos para América Latina

Después de la crisis decisional y de gobernabilidad, y ante el inminente fracaso del nuevo multilateralismo, la superación del riesgo, como se ha reiterado, requiere de la inclusión real de la sociedad en la definición del riesgo, para su posterior prevención. Allan Lavell formula una definición de la gestión del riesgo bastante conveniente para el debate:

> [...] un proceso social complejo cuyo fin último es la reducción o la previsión y control permanente del riesgo de desastre en la sociedad, en consonancia con, e integrada al logro de pautas de desarrollo humano, económico, ambiental y territorial, sostenibles. Admite, en principio, distintos niveles de coordinación e intervención que van

> desde lo global, integral, lo sectorial y lo macro-territorial hasta lo local, lo comunitario y lo familiar (Lavell, 2003, p. 30).

En esta definición, Lavell incluye la necesidad de acceder a diferentes instancias de la sociedad, desde *lo macroterritorial hasta lo local.* Es más, profundiza en la importancia de evaluar las interacciones comunitarias y familiares. También es esencial recalcar, como se hizo al final del primer apartado, que la gestión del riesgo es un proceso en construcción en el que participan los grupos involucrados que perciben el riesgo y el peligro. En este sentido, Lavell plantea que la gestión como proceso debe conformar una estructura organizativa que permita la planeación incluyente y coherente. El diseño de la gestión de riesgo debe articularse con procesos sostenibles en el tiempo para su *institucionalización* y evitar caer en las acciones e intervenciones aisladas y de interés particular.

En términos generales, para Lavell, las gestiones de los riesgos se clasifican en dos tipos: la gestión correctiva y la prospectiva. La primera se refiere a un riesgo ya identificado como latente, con el cual los actores ya han tenido interacción, y se proyecta como una intervención realista en las situaciones para que las vulnerabilidades más urgentes sean reducidas y las amenazas eliminadas; siempre debe ser visible la sostenibilidad de las acciones. La segunda corresponde con un riesgo inexistente, pero que puede ser creado mediante acciones humanas. La gestión prospectiva es fundamental para el desarrollo, pues evita los errores del pasado. Evidentemente, la prospectiva corresponde a la planeación tradicional. Ella utiliza el factor riesgo para buscar proyectos más seguros; la correctiva, por su parte, procura una transformación que podría articularse con la prospectiva (Lavell, 2003).

En la figura 1 se ilustran las etapas de la gestión del riesgo según el enfoque basado en procesos: en primer lugar, es fundamental

divulgar información para la identificación de los factores de riesgo y para monitorear su progresión; en segundo lugar, se deben tomar las decisiones pertinentes para evitar riesgos en gestación; en tercer lugar, se debe corregir el riesgo ya identificado y controlar la emergencia de uno similar o sus consecuencias; en cuarto lugar, se debe formular el curso de reacción para las instituciones y la población; en quinto lugar, se debe asistir a las poblaciones involucradas en el riesgo o golpeadas por el desastre; en sexto lugar, se dirigen acciones para el restablecimiento de los sistemas y de las infraestructuras físicas afectadas (Narváez et al., 2009).

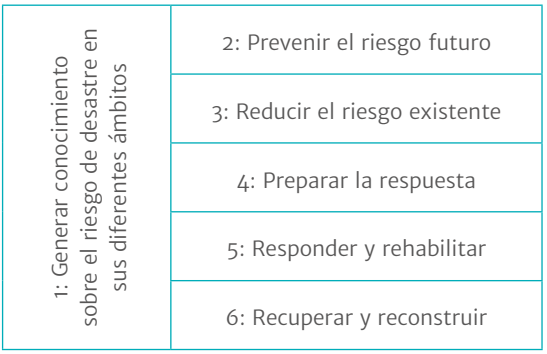


Figura 1. Procesos clave o misionales de la gestión del riesgo de desastre
Fuente: *(Narváez et al., 2009, p. 63).*

Si bien cada riesgo tiene un carácter específico, las seis etapas de la gestión del riesgo corresponden con las acciones prospectivas y correctivas. Al mismo tiempo, apuntan a una constante preparación para los posibles escenarios. Esto lleva al cuestionamiento: ¿cuál es la mejor articulación de actores para la gobernanza y para la gobernabilidad del riesgo?

Lavell encuentra que "los riesgos se expresan mejor en la localidad" (Lavell, 2003, p. 37). Esto no significa que únicamente se pueda

gestionar eficientemente el riesgo en escenarios locales. Pero se llama la atención sobre la gestión del riesgo en espacios tan homogéneos como los municipios, en los que se puede dar la cooperación interagencial entre los niveles regional, nacional e internacional. En especial, esta gestión local y descentralizada permite la ampliación del conocimiento del riesgo y de la población a partir de una perspectiva colaborativa. Además, puede concebirse como contrapeso a la globalización excluyente (Lavell, 2003).

Para identificar la necesidad de la gestión local del riesgo, se debe pensar en sus conexiones con el desarrollo, dado que las acciones emprendidas corresponden a un plan más amplio de organización económica de los potenciales productivos. Por tanto, la sociedad desempeña un rol en el desenvolvimiento de los estilos de desarrollo y los riesgos que acepta. En consecuencia, la gestión del riesgo debe apuntar a una transformación del desarrollo basada en prácticas sostenibles, y debe proveer de seguridad tanto a la población como a los recursos naturales. De hecho, entre las ventajas de la gestión local se encuentra el trabajo mancomunado de las comunidades y las autoridades locales, quienes están motivadas a cooperar por la apropiación de sus problemáticas. Lavell insiste especialmente en el trabajo conjunto con las instituciones presentes en la zona. Este trabajo implica procesos continuos y articulados a estrategias macro de desarrollo que mantienen conectadas a las comunidades con territorialidades más amplias (Lavell, 2003).

Una aproximación complementaria a la de Lavell es la teoría de los complejos regionales de seguridad de Barry Buzan y Ole Waever (2003), la cual habla de una interdependencia entre las unidades para tratar los procesos de securitización de manera conjunta (Buzan & Waever, 2003). Esta teoría comprende más que las interacciones estatales a través de la distinción de límites de la comunicación

intrarregional. Los autores observan esta aproximación teórica, no como una explicación totalizante del sistema internacional, sino como un acercamiento descriptivo, con potencial empírico, de los subsistemas regionales. Esto se debe principalmente a la cercanía geográfica que expone a sus correspondientes actores estatales y no estatales a problemas de seguridad, equiparables o compartidos, más intensos que los dilemas de seguridad globales: migraciones, contaminación de fuentes hídricas o conflicto armado. De esta forma, la interdependencia se distribuye desigualmente entre las diferentes regiones y subregiones.

Buzan y Waever afirman que las relaciones regionales pueden ser de carácter amistoso o de rivalidad. No obstante, encuentran que la capacidad de penetración de un actor en los asuntos del otro es fundamental. Cuando hay una dependencia ineludible, tienen que advocar por prácticas de seguridad comunes que los definen como complejos regionales. Los autores aclaran precisamente que su orientación teórica no acoge discursos regionalistas, sino dependencias empíricas y acciones imperativas perdurables guiadas por las condiciones materiales o por una historia compartida (Buzan & Waever, 2003). De esta manera, se concreta una relación con la gestión del riesgo de Lavell dado que la especificidad territorial del trabajo empírico, alrededor de las prácticas de seguridad, recae en última instancia sobre las percepciones y las interacciones de los actores en relación con el riesgo que comparten. El enfoque local de Lavell se complementa evidentemente con el regional de Buzan y Waever, pues ambas teorías buscan salir de los límites del Estado buscando los potenciales interactivos de los grupos sociales o del sector privado.

Buzan y Waever afirman que las principales características del complejo de seguridad suramericano son la guerra contra las drogas en Colombia y las relaciones de Mercosur en el Cono Sur. Además,

muestran como referente directo de poder externo a los Estados Unidos y se refieren una difusa separación de las interacciones entre el norte y el sur de Suramérica (Buzan & Waever, 2003). En la formación de los Estados suramericanos, la región sufrió varios conflictos internacionales que se prolongaron incluso hasta la segunda mitad del siglo XX con la guerra de las Malvinas. Sin embargo, la conflictividad intrarregional en Sudamérica sigue siendo baja en comparación con otros complejos regionales. Por una parte, durante la Guerra Fría la región se enfrentó a una alta vulnerabilidad doméstica y tuvo una baja relación interestatal, así como interregional (con excepción de las intervenciones de Estados Unidos en todos los países). Por otra parte, después de la Guerra Fría, la vulnerabilidad doméstica se mantuvo, mientras que las relaciones entre Estados aumentaron sustancialmente, tanto en la rivalidad como en la cooperación. En efecto, el crecimiento de organizaciones y pactos regionales fue determinante para el aumento del comercio en la región andina y en el Cono Sur, mientras las relaciones con otros focos de poder se alejaban de Estados Unidos. No obstante, el conflicto colombiano y la guerra contra las drogas afectan a toda la región y aumentan la presencia de Estados Unidos, financiera y militarmente (Buzan & Waever, 2003).

Casi dos décadas después del análisis del complejo regional sudamericano, se observa el crecimiento de las relaciones entre Estados en toda la región, no solamente a través del comercio bilateral, sino por medio de la apertura de organismos multilaterales de comercio y de tratados de intercambio en educación, turismo y cooperación Sur-Sur. Al mismo tiempo, se incrementan las relaciones de la región con actores globales como China y la Unión Europea a través de Tratados de Libre Comercio (TLC) y convenios de cooperación Norte-Sur. De la misma forma que se diversifican las relaciones internacionales en América Latina, también aumentan los riesgos compartidos.

En especial, riesgos con raíces en la dependencia económica y la desigualdad estructural. Estos factores tienen injerencia directa sobre la reproducción de la pobreza y del crimen organizado. En este aspecto, Colombia ya perdió protagonismo; no exclusivamente por la firma de acuerdos de paz con las Autodefensas Unidas de Colombia (AUC) y las Fuerzas Armadas Revolucionarias de Colombia (FARC), sino por la proliferación de organizaciones criminales transnacionales en toda América Latina que se encargan del narcotráfico, de la trata de personas y del comercio de armas y de fauna silvestre.

América Latina se enfrenta a una dependencia económica histórica y a la consolidación del modelo económico neoliberal, importado, después de la crisis de la deuda externa, por los Estados Unidos a través del Banco Mundial y del Fondo Monetario Internacional mediante lo que se conoció como el Consenso de Washington. Este modelo económico propuso el ajuste estructural como reforma institucional y normativa de los Estados latinoamericanos para reducir el papel del Estado en la economía y aumentar la inversión del capital privado nacional e internacional (Girón, 2008).

Con el aumento del capital privado en las economías nacionales, se termina por reforzar el régimen agroexportador y el extractivismo en la mayoría de los países; los monocultivos y la minería extensiva terminan destruyendo los ecosistemas regionales. La extensión de estas actividades económicas afecta la naturaleza más allá de las fronteras estatales. En este sentido, la exportación de *commodities* ha sido la nueva prioridad de la economía en la región, lo cual aumenta la dependencia con respecto al mercado exterior, pues es necesario encontrar demanda para las materias primas e incrementar la capacidad de importación de bienes primarios y manufacturados (Svampa, 2013).

Al final, la región no logra insertarse en el mercado internacional exitosamente, contrariamente a lo que le fue prometido con el neoliberalismo y la globalización económica. Sin duda, y en consecuencia, se debe considerar a la desigualdad como la gran fuente del riesgo en América Latina. Basta con observar los fenómenos de riesgo actual —la migración venezolana, la deforestación del Amazonas y la enorme acumulación del capital— para encontrar en los casos locales y concretos la distribución social del riesgo. El neoliberalismo afectó gravemente la distribución de la riqueza, especialmente a través de la privatización de las empresas y los recursos públicos. Con el aumento del poder económico, las políticas monetarias y fiscales tendieron a favorecer los intereses privados y la acumulación del capital. En el caso de la deforestación de la Amazonía brasileña, la tala de bosques muestra la fuerte presencia de intereses privados sobre la tierra. Las migraciones venezolanas hacia los países vecinos han generado sentimientos de xenofobia y de violación de derechos humanos, en especial con respecto a la explotación laboral y la negación del acceso a salud y a educación de los migrantes más pobres.

En consecuencia, América Latina, en especial Sudamérica como complejo regional de seguridad, es altamente vulnerable a las pulsiones y las perturbaciones de la economía mundial. En las economías latinoamericanas, debido a la terriblemente desigual distribución del ingreso, aumentan las actividades ilegales. Luis Reygadas (2008) caracteriza la desigualdad en América Latina como un fenómeno multidimensional que va "desde la concentración de los principales recursos productivos hasta los dispositivos simbólicos que marcan fronteras de inclusión y exclusión, pasando por las interacciones cotidianas" (Reygadas, 2008, p. 351). En esta caracterización, se resalta el problema de la desigualdad de los recursos económicos, yuxtapuesto con la estigmatización y

la separación social. Asimismo, mediante empleos y salarios flexibles se perpetúa la acumulación de ingresos en las clases altas y la ausencia de protección al trabajador, que se adiciona al acceso restringido a servicios públicos y al bienestar social (Reygadas, 2008).

En este análisis se puede observar cómo el riesgo se presenta de diferente forma para las economías nacionales/regionales y para las poblaciones locales. Si bien las desigualdades locales tienen efectos sobre el desenvolvimiento de la economía nacional, y sobre el desempeño de la gestión del riesgo, el ámbito regional demuestra cómo la vulnerabilidad y los efectos de la aplicación de los modelos extranjeros en la economía aumentan el riesgo para las poblaciones locales.

Conclusiones

Haciendo uso de un modelo de análisis como el de la gestión del riesgo propuesta por Lavell, se presentan concepciones de seguridad actuales que persiguen nociones más humanas y privadas de los riesgos. Este enfoque requirió de una reevaluación epistemológica y teórica del riesgo, que se conjuga con una necesidad ética de afrontar la crisis del desarrollo económico. La percepción localizada del riesgo va a necesitar considerar su gestión como un proceso orgánico llamado a apropiar el riesgo más que como una demanda de un producto generado desde el exterior.

Actualmente, los avances de las reflexiones sobre la seguridad y el riesgo van a obligar a que se dé una transición de la Reducción del Riesgo de Desastre (DRR, por sus siglas en inglés) a la Gestión del Riesgo de Desastre (DRM, por sus siglas en inglés). Esta última demanda el desarrollo de compromisos multisectoriales para la gobernanza y la integración alrededor del riesgo y resalta la necesidad de prácticas de desarrollo transformadoras a través de las redes conformadas

socialmente (Lavell & Maskrey, 2014). Este paso del DRR al DRM se hace explícito ante el reconocimiento de acciones más radicales de cambio frente a los modelos de desarrollo[3].

Ante el riesgo global que representan el cambio climático y los desastres naturales, la gestión del riesgo plantea transformaciones estructurales de la actividad humana en relación con la naturaleza, al igual que cambios en la gobernabilidad. El *accountability* va a ser un elemento fundamental para que la población cuestione y participe en la transformación de las actividades productivas y para que haya una intervención de las instituciones del Estado de forma más eficiente sobre los factores de riesgo percibidos. Para América Latina, la participación de las diversas poblaciones sobre las decisiones para favorecer la dignidad humana va a afectar positivamente la gestión de los riesgos socioeconómicos. A su vez, la búsqueda de la autonomía productiva va a permitir un desempeño más eficiente y armonioso con la naturaleza que el actual modelo de desarrollo depredador.

Referencias

Beck, U. (2009). *World at Risk.* Polity Press.

Booth, K. (2007). *Theory of World Security.* Cambridge University Press.

Buzan, B., & Waever, O. (2003). *Regions and Powers: The Structure of International Security.* Cambridge University Press.

Canale-Mayet, A., & Olivares, A. (2014). Gobernabilidad, ingobernabilidad y seguridad: algunos acercamientos teóricos. En C. Garay, L. Gil, & V. Troncoso, *Gobernabilidad y seguridad en América Latina: desafíos del sector defensa* (pp. 9-23). Universidad Santiago de Chile.

3 "The imperative of resilience and its schizophrenic goal to protect development against itself needs to be replaced with an imperative of transformative development. DRM would then characterize the transformation of development pathways and practices based on principles of equity, efficiency and sustainability" (Lavell & Maskrey, 2014, p. 278).

Girón, A. (2008). Fondo Monetario Internacional: de la estabilidad a la inestabilidad. El Consenso de Washington y reformas estructurales en América Latina. En G. Lechini (comp.), *La Globalización y el Consenso de Washington: sus influencias sobre la democracia y el desarrollo en el sur* (pp. 45-60). Clacso.

Lavell, A. (2003). *La gestión local del riesgo: nociones y precisiones entorno al concepto y a la práctica.* PNUD-Cepredenac.

Lavell, A. (2012). Reflections: Advancing Development-Based Interpretations and Interventions in Disaster Risk: Some Conceptual and Contextual Stumbling Blocks. *Environmental Hazards, 11*(3), 242-246. https://doi.org/10.1080/17477891.2012.698845

Lavell, A., & Maskrey, A. (2014). The Future of Disaster Risk Management. *Environmental Hazards, 13*(4), 267-280. https://doi.org/10.1080/17477891.2014.935282

Luhmann, N. (1993). *Risk: A Sociological Theory.* Walter de Gruyter.

Narváez, L., Lavell, A., & Pérez, G. (2009). *La gestión de riesgo de desastres: un enfoque basado en procesos.* Comunidad Andina.

Oliver-Smith, A., Alcántara-Ayala, I., Burton, I., & Lavell, A. (2017). The Social Construction of Disaster Risk: Seeking Root Causes. *International Journal of Disaster Risk Reduction, 22,* 469-474. https://doi.org/10.1016/j.ijdrr.2016.10.006

Reygadas, L. (2008). *La apropiación: destejiendo las redes de desigualdad.* Anthropos.

Svampa, M. (2013). «Consenso de los commodities» y lenguajes de valoración en América Latina. *Nueva Sociedad, 244,* 30-46.

Wascuk, R. (2001). The new multilateralism. En R. McRae, & D. Hubert (eds.), *Human Security and the New Diplomacy* (pp. 213-222). McGill-Queen's University Press.

Capítulo 5

Papel estratégico de la gestión de "nuevos" riesgos

Aristides Baldomero Contreras Fernández*

* Docente de las asignaturas de Administración, Análisis y Evaluación de Riesgos en la Escuela de Postgrados de la Fuerza Aérea Colombiana, Presidente ejecutivo e investigador en la Comunidad Internacional en Gestión de Riesgos y Seguridad (COLADCA). Correo electrónico: coladca@gmail.com

CÓMO CITAR

Contreras Fernández, A. B. (2020). Papel estratégico de la gestión de “nuevos” riesgos. En Y. Rico, D. López Cortés, & A. Cerón R. (comps.), *Enfoques y gestión en Seguridad Integral* (pp. 129-160). Escuela de Postgrados de la Fuerza Aérea Colombiana. https://doi.org/10.8667/9789585996199.05

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

CAPÍTULO 5.
Papel estratégico de la gestión de "nuevos" riesgos

https://doi.org/10.8667/9789585996199.05
Bogotá, Colombia
Noviembre, 2020

RESUMEN

Actualmente, el mundo está buscando cómo reactivar la economía y las diferentes actividades que se han visto bloqueadas por el impacto de la pandemia COVID-19. Cada actividad realizada por un ser humano o por una organización tiene multiples riesgos asociados. En este caso, uno de los riesgos ya se materializó y, por tanto, es importante insistir en la necesidad de incorporar e implementar nuevos procesos de gestión de riesgos, desde su correcto diseño en cualquier organización, como una labor vital y de gran valor, puesto que se ha evidenciado que los procesos no se están realizando correctamente.

Cada visita geoestratégica con los estudiantes del programa de Maestría en Dirección y Gestión de la Seguridad Integral en la Escuela de Postgrados de la Fuerza Aérea Colombiana, resalta aspectos, falencias; pero, sobretodo, la imperiosa necesidad de recomendaciones que nos llevan a explicar, desde el estado del arte, la palabra riesgo. De allí surge el valor actual y la suma de un actor fundamental en este capítulo, y es *el papel estratégico del proceso* de la gestión de riesgos: ¿por qué implementarlo? ¿Por qué es importante articular compromisos desde la alta dirección? ¿Por qué la gestión de riesgos es un factor diferenciador en las organizaciones? Son muchos los interrogantes que a diario se manifiestan y más cuando escuchamos a los directivos de las áreas de Seguridad o Riesgos en nuestras visitas.

A la fecha, la mayoría de las organizaciones implementa como mínimo un sistema integral de gestión, tal como el basado en aseguramiento de la calidad (bajo la Norma ISO 9001, versión 2015) y, a su vez, este ya integró en su estructura de alto nivel, la inclusión del numeral 4, Contexto de la organización, el cual lleva a que las empresas sumen un analisis de contexto que les permitirá identificar amenazas y oportunidades. Esto muestra la necesidad de planificar y realizar acciones para abordar riesgos.

PALABRAS CLAVE

Amenazas; cambio tecnológico; incertidumbre; prevención de riesgos; riesgo; sistema de gestión.

Introducción

Voltaire expresaba que "la incertidumbre es una posición incómoda, pero la certeza es una posición absurda". Este artículo se desarrolló con el objetivo de resaltar la importancia del proceso de gestión de "nuevos" riesgos en la actualidad, teniendo en cuenta que todas las personas u organizaciones toman decisiones bajo incertidumbre. Estas decisiones traen consigo elementos cambiantes o inesperados que, cuando se someten un proceso de administración de riesgos para identificar allí factores vitales, ofrecen un factor diferenciador en las organizaciones.

Estos pasos son muy importantes y, si son ejecutados de manera correcta, se identificará cómo pueden surgir muchos aspectos positivos. También surgirán aspectos por mejorar, es decir, aspectos que los profesionales, encargados o interesados en ejercer procesos de evaluación de riesgos están realizando de forma inadecuada o errónea. La indebida cuantificación en forma previa y correcta los riesgos (por desconocimiento u otra circunstancia) no permite generar alertas en forma convincente para la organización. Por tal motivo, los gerentes o CEO de las organizaciones muchas veces no entienden o no ven de forma sencilla información estratégica para la toma de decisiones, piensan que la labor no tiene importancia como proceso misional y no la ponen en consideración para la intervención que en algunos casos se requiere.

En 1921, Frank Hyneman Knight publicó su tesis, "Riesgo, Incertidumbre y Beneficio" (en inglés "Risk, Uncertainty and Profit"), en la cual esboza la diferencia entre riesgo e incertidumbre. También trata la importancia de las teorías del beneficio, cambio y riesgo en relación con el beneficio, resalta que:

> Aunque el hombre de negocios no pudiera conocer de antemano los resultados de las empresas individuales, podría operar y basar sus ofertas competitivas en un conocimiento previo exacto de la rutina, si se puede tener un conocimiento cuantitativo de la probabilidad de cada resultado posible.

La International Organization for Standardization, ISO, (2018), plantea que el riesgo es el "efecto de la incertidumbre sobre los objetivos" (p. 1), y al presentarnos la Norma Técnica ISO 31000:2018 recalca en su segunda edición que "un efecto es una desviación respecto a lo previsto". Detalla que este efecto "puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas" (ISO, 2018, p. 1). Corolario de lo anterior, en la misma norma técnica, la nota n.° 3 del punto 3.1 insiste en que, a menudo el riesgo está definido por aspectos de fuentes de riesgo, eventos potenciales, consecuencias y probabilidades.

Toma gran valor poder definir, entonces, el aspecto *cuantitativo* sobre la probabilidad en la gestión de "nuevos riesgos". En la actualidad, el mundo se mueve *a un clic*, el ciudadano está cada día más interconectado de forma proporcional a la evolución de los sectores económicos y financieros, quienes también avanzan de manera compleja a la par con la globalización. Proporcionalmente su expansión, aumentan las crisis y por ende los riesgos a afrontar en diversos ámbitos (Zorrilla, 2005).

En relación con lo anterior, Knight (2002) afirmó que "[...] todo lo que el hombre planea y ejecuta implica incertidumbre" (p. 145). Desde allí, y con las precisiones que trataremos al respecto, el rol e importancia de la gestión de "nuevos" riesgos debe ser una prioridad para implementar en las organizaciones. No es extraño que se resalte, desde los principios de la Gestión de Riesgos hasta el tratamiento de

los mismos, que el propósito de la misma "[...] es la creación y la protección del valor" (ISO, 2018, p. 2). Así las cosas, los principios y la integración que la componen son parte fundamental para fortalecer los procesos y para asistir en el establecimiento de estrategias dentro de toda organización, siendo parte de la gobernanza en todos los niveles para ayudar a identificar y disminuir la incertidumbre, alineándose con el cumplimiento de los objetivos.

En linea con los anteriores planteamientos, Mejía (2004, p. 75) señala que "desde la antigüedad el hombre ha tomado riesgos, la incertidumbre está presente aún en el corto plazo. Es causada por la imposibilidad de determinar los eventos que pueden presentarse y sus resultados; con la incertidumbre viene asociado el riesgo. En el sector de servicios bancarios se ha visto diezmada la oferta de productos y servicios, gracias a que últimamente la materialización de incidentes y delitos informáticos dan a entender que, por cada dólar que los ciberdelincuentes extraen de usuarios del sector financiero, el banco llega a perder hasta 2, 95 USD, fraude que enlista elementos adicionales, como la suma de pérdidas en costos asociados a la pérdida de intereses del dinero objeto del fraude que el banco ya no va a recibir, el costo para el cliente, gastos financieros cargo contra cargo y otros para dar respuesta a la reclamación. Cabe mencionar que esto no contempla que el cliente se vaya del banco.

De lo anterior, nace la primera conclusión de este artículo: invertir en la prevención va de la mano con los procesos de gestión de riesgos. De igual manera, se debe alertar a los evaluadores de riesgos, quienes deben ser integrales para que el aspecto más importante para los directivos de las organizaciones, o en caso de existir el C-suite[1], sea el

1 El C-suite, según *Forbes*, "[...] es considerado el grupo más importante e influyente de individuos en una empresa. Ser un miembro de este grupo viene aparejado con la

papel de la gestión de riesgos, la cual protege el capital de la empresa (Revista Forbes, 2017).

En ese sentido, Knight (1964) también dio a entender que las ganancias incluyen un tercer elemento denominado *pago por riesgo*, que ha tendido a generar una nueva confusión de ganancias e intereses. Esto nos da valor como parte fundamental y sensible para el impacto directo a las utilidades de la organización, así como también aísla totalmente al pago por riesgo y no lo iguala con gastos que se reconocerán como administrativos. Así pues, la profesión como especialistas en evaluar el riesgo adquiere un nuevo protagonismo.

Más adelante, se tratará el impacto económico de los controles en el presupuesto de la organización en dos vías, tanto desde las pérdidas que pueden surtirse como de las ganancias y el no contemplado retorno de la inversión. Se advierte que este último sí ocurre y con la metodología correcta se puede evidenciar.

Por tratar en profundidad el tema del riesgo, Knight (1964) establece el rol de la incertidumbre en las actividades empresariales diferenciando los conceptos de riesgo e incertidumbre. Establece que el primero es aquello que es mesurable y el segundo todo lo relacionado con lo incalculable. Es importante referirnos a la importancia del trabajo de establecer hechos futuros, más aún cuando hemos estado navegando en medio de cambios vertigionosos que no nos permiten identificarlos.

---

capacidad de tomar decisiones de alto riesgo, una carga de trabajo más exigente y una compensación elevada. A medida que proliferan los títulos principales, sin embargo, la inflación en el empleo puede disminuir el prestigio asociado con ser miembro del C-suite" (Revista Forbes, 2017).

Concepción de "nuevos" riesgos e incertidumbre

La gestión del riesgo es un "proceso esencial en cualquier modelo de gestión empresarial" (Ortiz & Valencia, 2017, p. 20). No hay organización que pueda estar al margen de esta premisa, independientemente de su tamaño u objeto, en la actualidad todas las empresas están sujetas a entornos o escenarios VICA[2]. El analista de riesgos debe reconocer en dónde se ubican las incertidumbres, además de establecer el alcance de los riesgos que de una u otra forma se presentan en diferentes facetas (Zorrilla, 2005).

Por otra parte, uno de los pasos más difíciles con la Junta Directiva, CEO, C-Suite, socios, administradores y gerentes en general, es llegar a un acuerdo y entendimiento en la concepción del riesgo, reconociendo la diferencia entre el apetito, la tolerancia y la capacidad del riesgo, sin dejar a un lado los riesgos residuales. Por ello se partirá de conocimientos generales hasta llegar a los específicos, lo cual nos permitirá conciliar saberes en la concepción organizacional interna.

El diccionario de la Real Academia Española define la palabra riesgo como la "contingencia o proximidad de un daño". Hemos visto cómo en la historia de la humanidad la proximidad o materialización de daños impulsaron los cambios y el establecimiento de controles en la administración actual de riesgos. Cuatro casos emblematicos fueron:

1. Naciones Unidas. Se crean el 1 de enero de 1942, sus respectivos gobiernos se comprometían a seguir luchando juntos contra las Potencias del Eje.

2 De la traducción VUCA, volátil, incierto, complejo y ambiguo.

2. Departamento de Seguridad Nacional de los Estados Unidos de América. Se crea como respuesta a los atentados del 11 de septiembre del 2001.
3. Fondo Monetario Internacional y Banco Mundial. Se crean en julio de 1944 en el marco de la conferencia de Bretton Woods, regularían el sistema monetario y el orden financiero tras la finalización de la Segunda Guerra Mundial.
4. Sistema de reserva federal de los Estados Unidos de América. Creado en el año 1913, luego del pánico de 1907 cuando la bolsa de valores de Nueva York tuviera una caida del 50% desde su maximo en el año anterior.

En ese orden de ideas, empezamos a llevar a la práctica la realidad en que la sociedad se viene desenvolviendo: riesgos e implementación de controles. ¿Dónde quedan los peligros?

De Castro (2000) plantea que los riesgos desarrollan un nivel mayor de controversias científicas que el término peligro, teniendo en cuenta las causas, probabilidades de ocurrencia y consecuencias. Así, la esencia de la definición más aceptada está relacionada con la de "el peligro que se corre". Por tanto, el concepto de riesgo se entiende como la probabilidad de ocurrencia de peligro. En ese alcance De Castro (2000) conceptualiza o incluye la probabilidad de ocurrencia de riesgo en aspectos naturales o antrópicos y la evaluación que puede realizar el hombre sobre estos y sus efectos nocivos. En esa evaluación entra el escenario de la vulnerabilidad, en el que se pueden realizar valoraciones y mediciones de pérdidas y probabilidades de ocurrencia. Por otro lado, hay mayores desaciertos cuando no existen mecanismos para calcular las probabilidades, o su tratamiento se deja a la intuición, lo que causa mayor incertidumbre.

En esa línea, de acuerdo con la literatura académica en geografía de riesgos, se evidencia que el peligro es un acontecimiento que puede causar grandes pérdidas una vez se materializa. Por tal razón el hombre debe valorar todo aquello que puede representar un daño y cada escenario que no.

No obstante, cabe aclarar que aquellos fenómenos naturales como las inundaciones, terremotos o huracanes son considerados como eventos peligrosos solo si atentan contra la vida de la gente en su lugar de habitad. Al respecto, Smith (1992) explica que "los peligros naturales resultan de los conflictos de los procesos geofísicos con la gente" (p. 9), una interpretación que le da al hombre la potestad de elegir la definición, ya que es a través de sus percepciones, acciones o localizaciones que el fenómeno natural se vuelve peligroso o no.

Más allá de las diversas definiciones sobre el concepto de peligro que se pueden encontrar, existe una tendencia que revela sus rasgos en común como:

> (a) riesgo de exposición: normalmente involuntario; (b) tiempo de advertencia: corto, excepto en el caso de peligros como la sequía, la pobreza, etc.; (c) resultados: producen daños (desastres) que justifican medidas de emergencia; y (d) pérdidas: sufridas a corto o largo plazo según los casos (De castro, 2000, párr. 14).

Estos rasgos en común del término peligro revelan que la exposición siempre presente puede producir daños. Allí la implantación de un sistema de gestión de "nuevos" riesgos es de valor.

Entre tanto, de acuerdo con los planteamientos de Izquierdo (2003), todo riesgo tiene causas y consecuencias, por lo que un gestor de riesgo al iniciar un proyecto debe evaluar los aspectos potenciales

que puedan obstaculizar el cronograma de actividades proyectado, es decir, identificar riesgos a partir de posibles causas, aspectos que son conocidos como fuentes de riesgo.

Estos se clasifican en una tipología de causas. En primer lugar, están aquellos en los cuales los requisitos del proyecto no están bien definidos; en segundo, se encuentran los aspectos relacionados con el rol del supervisor a cargo, en el que habrá afectaciones si este no posee la suficiente experiencia para ese proceso, y en tercero, los escenarios en los cuales los equipos de trabajo seleccionado no tienen el perfil especializado en el área del proyecto.

Dicho esto, ¿cómo prever y minimizar los riesgos antes de que el proyecto inicie?

Una respuesta coherente a esta pregunta es la construcción de un plan de acciones de acuerdo con: (a) revisar que estén bien definidos los requisitos para iniciar cualquier proyecto, y asegurarse que el cliente los haya aprobado; (b) si un jefe de proyecto no cuenta con la suficiente experiencia, se debe buscar uno que sí cumpla con los requisitos; y (c) si el equipo de trabajo seleccionado para la obra no está suficientemente capacitado, se deben buscar herramientas para que logre estarlo en el menor tiempo posible, y así poder cumplir con los tiempos y objetivos.

Según Sophie Gaultier-Gaillard y Jean-Paul Louisot (2019), "la clave de toda gestión es el conocimiento; para gestionar los riesgos, es preciso conocerlos, es decir, identificarlos y evaluarlos" (p. 13). Hemos mencionado antes al explicar el termino riesgo la "contingencia o proximidad de un daño" y que en medio de los procesos siempre está inmerso un grado de incertidumbre, pero ¿que causas pueden generar variabilidad cuando observamos el concepto de incertidumbre alineados con el corportamiento humano?

Ignacio Vélez Pareja (2003. p 17) menciona que existen fenómenos no atribuibles directamente al ser humano que también causan riesgo e incertidumbre. Algunas manifestaciones de ambos tipos pueden ser:

a) Inexistencia de datos históricos directamente relacionados con las alternativas que se estudian.
b) Sesgos en la estimación de datos o de eventos posibles.
c) Cambios en la economía, tanto nacional como mundial.
d) Cambios en políticas de países que en forma directa o indirecta afectan el entorno económico local.
e) Análisis e interpretaciones erróneas de la información disponible.
f) Obsolescencia.
g) Situación política.
h) Catástrofes naturales o comportamiento del clima.
i) Baja cobertura y poca confiabilidad de los datos estadísticos con que se cuenta.

Con este capitulo hemos abordado y observado que la concepción de riesgos es muy diversa y lleva en sí algo destacado: "la apreciación y papel protagonico del ser humano" en todo momento, como también la necesidad de tomar el control o proyección del futuro. Al final volvemos, sin embargo, a donde iniciamos, a los parametros de objetividad o subjetividad en marco de un proceso de administración de riesgos.

Globalización y necesidad de administración de los riesgos

Cuando se estudian los factores de riesgo, es necesario contar con un representante que tenga suficiente visibilidad y capacidad de revisar

y evidenciar, junto a la dirección, qué riesgos se pueden presentar y cómo estos evolucionarán en el tiempo, para así establecer acciones de mitigación.

Adentrados en la cuarta revolución industrial, un entorno cambiante y VICA en el que existen nuevas amenazas y oportunidades, día tras día se generan alternativas de innovación que surgen de la investigación de mercados y la disposición para el cambio. Son varios los escenarios que obligan a las organizaciones a contar con estrategias que permitan conocer los efectos tanto negativos como positivos que puede tener la incertidumbre sobre los objetivos del negocio.

Solo con revisar el "Informe de Riesgos Globales 2020" publicado por World Economic Forum (WEF), en un momento en que el mundo se sigue transformando y ha sido catalogado como "un mundo mas inestable", nuevos riesgos siguen al acecho.

Gracias a los avances de las nuevas tecnologías, globalmente la sociedad ha estado gozando de una calidad de vida en condiciones que no se habían experimentado en la historia (guardadas las proporciones y teniendo en cuenta el tema de estudio). No obstante, la velocidad con la que la sociedad está interconectada puede sobrepasar los límites de lo permitido, teniendo en cuenta a las instituciones y las comunidades.

En ese sentido, las empresas del ámbito mundial, a partir de la identificación de incertidumbres en todos los procesos mencionados, generan valor en sus servicios, lo cual les permite ser sostenibles. Así mismo, gestionar dicha incertidumbre a través de la construcción de posibles escenarios del riesgo mejoró el sistema de gestión de las diferentes compañías, creó una cultura corporativa en la cual se desarrolló la necesidad organizativa de construir estrategias, objetivos y por supuesto, una gestión de riesgos correcta (Gil, 2013).

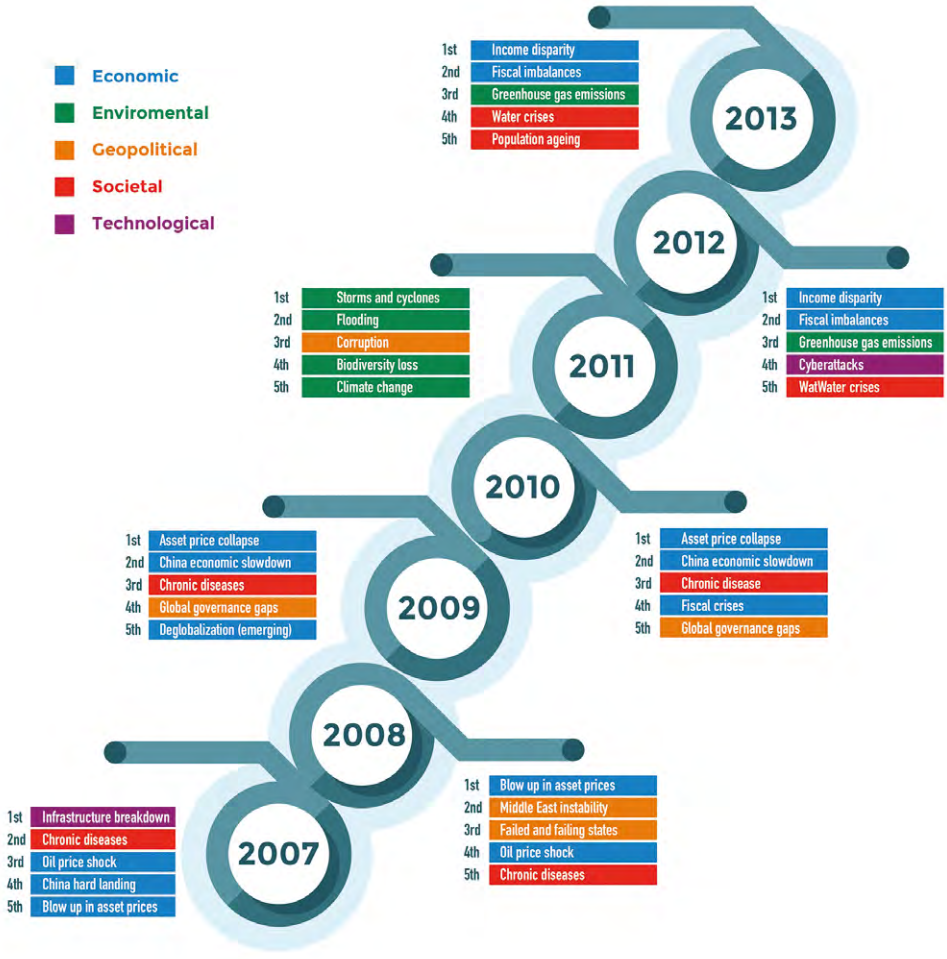
Por otro lado, autores como Bravo y Sánchez (2009) señalan que casi todas las situaciones que se consideran riesgosas son proporcionalmente inciertas, pese a que puede encontrarse que no toda incertidumbre es riesgosa.

La globalización y la facilidad con que nuevos negocios nacen y desaparecen en cuestión de segundos es una invitación a actuar de forma diferente a la tradicional. El Foro Económico Mundial ha insistido en que el desarrollo humano está en riesgo si no se hace frente a una diversidad de problemas, difíciles de reconocer a primera vista en todas las interacciones a nivel mundial, lo que implica que el número de casos siempre esté en aumento, teniendo en cuenta, además, que incluyan fracturas en diversos sistemas como el económico, tecnológico, ambiental e institucional (WEF, 2020).

Para ser más claros, concisos y ejemplares, en las siguientes figuras, adaptadas del Foro Económico Mundial en su 15ª edición, veremos los cinco riesgos que se han identificado como de mayor probabilidad, además de las incertidumbres y elementos no exhaustivos. No obstante, cabe advertir que en un mundo que por naturaleza cambia constantemente, siempre surgirán nuevos riesgos que hay que hacer el trabajo por identificarlos y tratarlos.

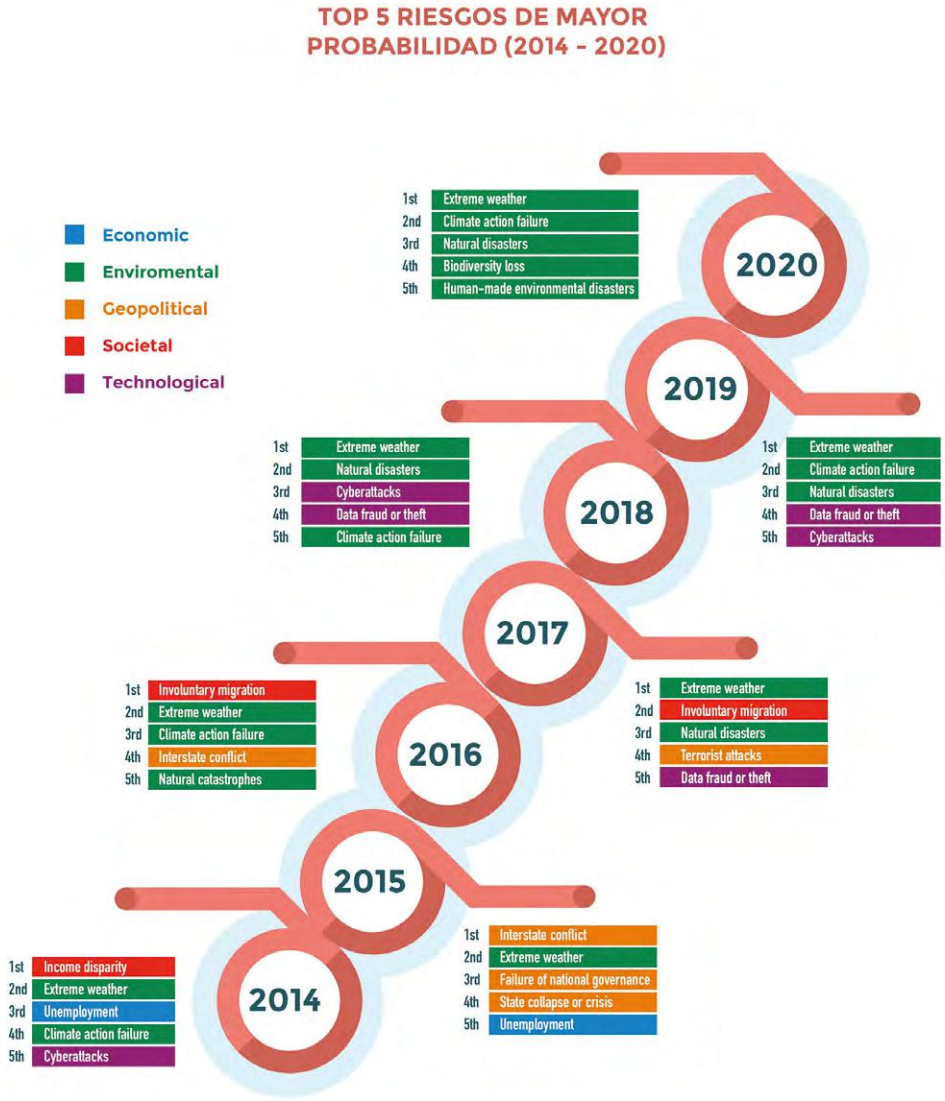
Al observar las dichas figuras, se puede llegar a las siguientes conclusiones:

1. Cualquier organización, sin distinción de su objeto o actividad económica, se enfrenta a "nuevos" riesgos que son de gran magnitud.
2. La migración a entornos digitales es una realidad, de allí el interés y persistencia por ubicarse en los primeros lugares como riesgos de mayor probabilidad de ocurrencia.
3. La evolución global, gracias a la interconexión, conecta de la misma manera nuevos riesgos a asumir.



Nota. Adaptado de The Evolving Risks Landscape, 2009 – 2019 (p. 2) por WEF (2020)
World Economic Forum 2007-2020, Global Risks Reports.

Figura 1. El panorama de riesgos en evolución, 2007–2013
Fuente: *WEF (2020).*



Nota. Adaptado de The Evolving Risks Landscape, 2009 – 2019 (p. 2) por WEF (2020) World Economic Forum 2007-2020, Global Risks Reports.

Figura 2. El panorama de riesgos en evolución, 2013-2020
Fuente: *WEF (2020).*

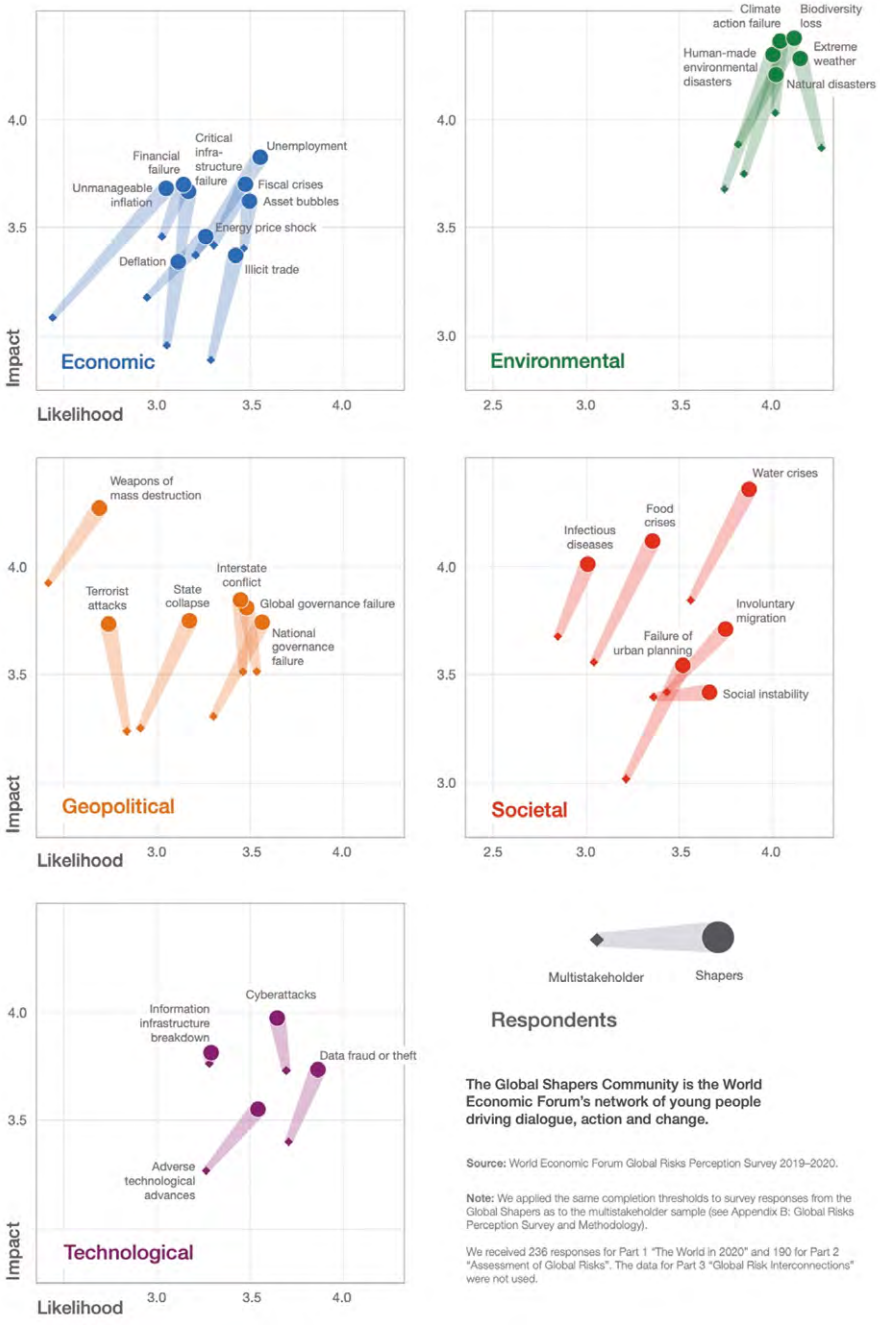


Figura 3. Panorama global de riesgos, moldeadores globales 2020
Fuente: *WEF (2020).*

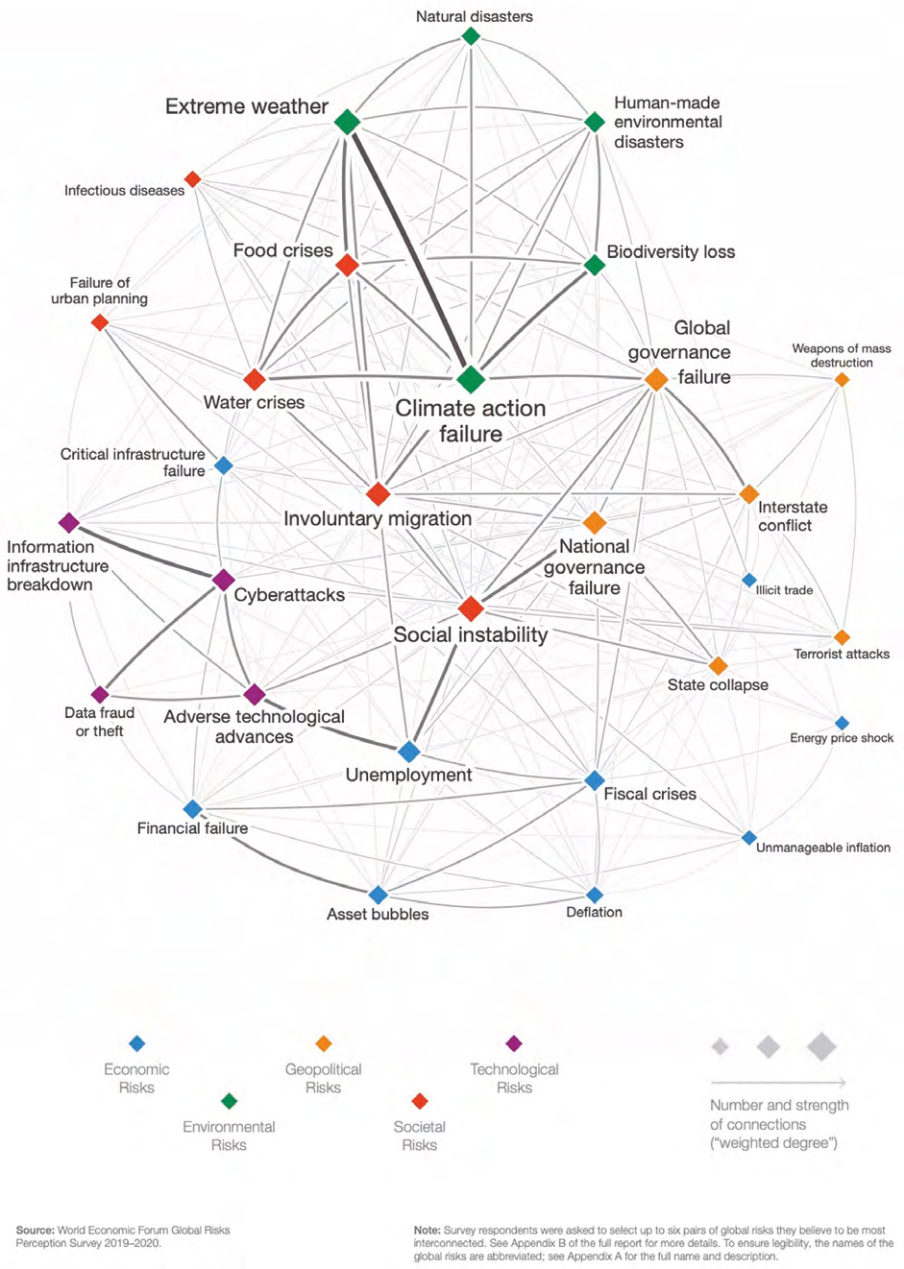


Figura 4. Mapa de interconexiones de riesgos globales 2020
Fuente: *WEF (2020).*

Ahora la pregunta es ¿cómo convencer a las directivas de la organización sobre la necesidad de invertir en la gestión y administración de "nuevos" riesgos?

Evolución, inclusión y adhesión de la gestión de riesgos en los sistemas integrales de gestión

En cualquier negocio u organización, los procesos de gestión están constituidos sobre la base de toma de decisiones y los probables riesgos que se deban asumir (Gil, 2013). En ese orden de ideas, las empresas buscan la creación de un valor como resultado del análisis de riesgos que han realizado, gracias al cual se construyen los objetivos y las estrategias de las organizaciones para que perduren en el tiempo.

En tal sentido, el riesgo es un elemento que debe considerarse desde diferentes perspectivas, desde el enfoque de un gobierno, hasta las posiciones más específicas de las empresas. Para estas últimas, el riesgo se ha constituido como uno de los aspectos que más ha causado la desaparición o limitación de las empresas, puesto que de no asumir estos desafíos en el corto plazo quedarían obsoletas.

> El riesgo, no obstante, no entra en el modelo en el que los empresarios trabajan. Pero lo hace de modo indirecto y un tanto independiente: el peligro –y todo lo nuevo es arriesgado en un sentido en el que no lo es la acción rutinaria– dificulta la obtención del capital necesario, y así, constituye uno de los obstáculos que los empresarios tienen que superar y uno de los ejemplos de resistencia del entorno que explica por qué las innovaciones no se llevan a cabo de modo uniforme y como por rutina (Schumpeter, 2002, p. 14).

En búsqueda de superar los retos corporativos y que las decisiones generen mayor valor, es importante motivar a que las empresas evaluen hasta dónde están dispuestas a asumir los riesgos, de tal forma que puedan optimizarlos y revisar su rentabilidad. En ese orden de ideas, en la cultura empresarial, la gestión del riesgo se debe asumir y difundir como parte fundamental de la empresa, debe ser parte de la gobernanza, interactuando con todas las partes interesadas.

Las organizaciones que dan valor a la implementación de sistemas integrales de gestión venían trabajando bajo una estructura común de los sistemas de gestión, que para Colombia se contempla en la norma más certificada a nivel mundial, a saber la ISO 9001, por la que se adopta un sistema de gestión de la calidad, y que acorde con la nueva actualización editada, punto n.° 6 de la norma, se detalla así:

6. Planificación
   6.1. Acciones para abordar riesgos y oportunidades.
      6.1.1. Al planificar el sistema de gestión de la calidad, la organización debe considerar las cuestiones referidas en el apartado 4.1 [Comprensión de la organización] y los requisitos referidos en el apartado 4.2 [Comprensión de las necesidades y expectativas de las partes interesadas], determinar los riesgos y oportunidades necesarias de abordar con el fin de:
         (a) asegurar que el sistema de gestión de la calidad pueda lograr sus resultados previstos;
         (b) aumentar los efectos deseables;
         (c) prevenir o reducir efectos no deseados;
         (d) lograr la mejora.
      6.1.2. La organización debe planificar:
         (a) las acciones para abordar estos riesgos y oportunidades;
         (b) la manera de:

1) integrar e implementar las acciones en sus procesos del sistema de gestión de la calidad (véase 4.4. [Sistema de gestión de la calidad y sus procesos]);
2) evaluar la eficacia de estas acciones.

Cabe resaltar que las acciones tomadas para abordar los riesgos y oportunidades deben ser proporcionales al impacto potencial en la conformidad de los productos y los servicios. Para lo cual no están por fuera de la familia las normas 14001, 18001, 27001, 28000 o 45001, y que, gracias a la adopción del "Anexo SL", brindan una estructura de alto nivel que surgió durante la búsqueda de la organización internacional para que los sistemas de gestión tuvieran la misma conformación y que esto permita facilitar la integración entre las difentes normas de la ISO en las organizaciones.

Para las personas que laboran en el gremio, e insisten en la inclusión y adhesión de la gestión de riesgos en los procesos, ha sido un gran logro que la norma ISO 9001:2015, en su introducción, estipulara el concepto de "pensamiento basado en riesgos", ya que pensar y proyectar el riesgo es importante para lograr un sistema de gestión con altos estándares de calidad y eficiencia. De esa forma, el pensamiento construido a partir del riesgo siempre ha estado presente en todas las ediciones de la norma internacional mencionada. Además, se han incluido protocolos sobre procesos preventivos para erradicar no conformidades, analizarlas y seleccionar acciones apropiadas para prevenir sus efectos.

Según David MacNamee, la administración de riesgos significa vigilar activamente para asegurar la sensibilidad de la organización, que le permita detectar los riesgos, contar con sistemas ágiles que aseguren flexibilidad para responder al riesgo y desarrollar aprendizaje

adaptativo que asegure la capacidad de los recursos de la organización para mitigar el riesgo (MacNamee, 2002, p. 18).

Así las cosas, para estar alineados con los requisitos de la normatividad internacional, las organizaciones necesitan planear y ejecutar acciones para enfrentar los riesgos y aprovechar las oportunidades. Y así, analizar los riesgos como una forma de oportunidad, desarrollar un componente base para potenciar la eficacia de la calidad de los sistemas de gestión y lograr los resultados esperados, incluyendo mitigar las posibles afectaciones.

Dichas oportunidades surgen de las situaciones favorables que se presenten para conseguir los resultados esperados, un ejemplo de ello son aquellas circunstancias que le permiten a una organización ser atractiva para los clientes y, así, elaborar productos o servicios para disminuir los retos y potenciar la productividad.

Por otro lado, los planes para aprovechar dichas oportunidades también deben considerar los riesgos a los cuales pueden estar asociados. Si bien de estos surgen oportunidades, no todos los riesgos las generan, y cuando lo hacen, no todos se presentan de la misma manera. Dicho lo anterior, el panorama de las organizaciones llegó a una etapa de transición fundamentalmente basada en riesgos.

En ese sentido, es importante adentrarnos en la Norma Internacional sobre las directrices de la Gestión de riesgos - ISO 31000, norma técnica que no es certificable como un sistema de gestión, pues es solo una guía.

Sumado a lo mencionado en el capitulo anterior, al adoptar un sistema de gestión de la calidad con nuevas prebendas y cambios introducidos en gestión de riesgos como una decisión estratégica y no como un requisito de cumplimiento para la organización, de inmediato se reconocerán beneficios potenciales, entre los cuales se encuentran:

a. **Abordar los "nuevos" riesgos y oportunidades:** se relaciona con el contexto y los objetivos planteados. En ese sentido, las organizaciones por esencia tendrán que realizar un proceso de implementación y mejoramiento de su sistema de gestión de calidad e incluir los proceso necesarios teniendo en cuenta su contexto interno y externo, sus interacciones y partes interesadas.
b. **Enfoque al cliente:** establece que la gerencia tiene que mostrar una imagen de liderazgo y compromiso frente a su clientela, con la que debe asegurarse de aquellas oportunidades y riesgos que pueden ocurrir y perjudicar el producto o servicio que se brinda. De esta manera la satisfacción del cliente será una variable primordial y que siempre se tendrá presente.
c. **Análisis y evaluación:** toda organización debe tener un sistema de análisis y evaluación de acuerdo con una estrategia de seguimiento. De esta forma, sus resultados cuentan con un historial de seguimiento y le permitirá la mejor información disponible, con ella se pueden discutir e identificar las acciones que se requieren para el abordaje de los riesgos y, por ende, las oportunidades que permiten.
d. **Entradas de la revisión por la dirección:** la revisión que se quiere realizar por parte de la dirección principal estará constituida por un planeamiento riguroso, haciendo énfasis en aquellas consideraciones eficaces que se tuvieron en cuenta para analizar los riesgos y oportunidades. En medio de la "nueva" realidad que vivimos, organizaciones como The Institute of Internal Auditors han resaltado que: "La responsabilidad de la dirección de alcanzar los objetivos organizativos comprende tanto los roles de primera como las de segunda línea". (IIA, 2020)
e. **No conformidad y acción correctiva:** cuando llegasen a ocurrir escenarios en los que se presente alguna no conformidad, así

provenga de alguna queja, la organización debe tener en cuenta un proceso de actualización de riesgos y oportunidades mientras se construye una nueva planificación.

Y por último, detallando en el Anexo A de la Norma de Gestión de Riesgos ISO 31000, respecto a la aplicabilidad, se deberia tener en cuenta lo siguiente:

Aplicabilidad (a5) (Nivel de complejidad)

Dicha normatividad no señala una lista de las posibles "exclusiones" que una organización podrá o no aplicar en el establecimiento de sus requisitos al momento de organizar el sistema de gestión de calidad. No obstante, la aplicación de dichos requisitos puede constituirse teniendo en cuenta el nivel de complejidad de la organización, incluyendo los rangos establecidos de acuerdo con las actividades y los modelos de gestión que se haya decidido adoptar, además de los riesgos y oportunidades que se puedan encontrar.

ISO 31000:2018 y el modelo de las tres líneas del IIA 2020

Gestionar "nuevos" riesgos requiere una nueva visión y una integración del panorama de la gestión de riesgos con una mirada holística y desde diferentes visiones (Contreras, 2020).

La norma ISO 31000 "está dirigida a las personas que crean y protegen el valor en las organizaciones gestionando riesgos, tomando decisiones, estableciendo y logrando objetivos y mejorando el desempeño" (ISO, 2018, p. i).

Así las cosas, si se quiere establecer la existencia de algún riesgo, es necesario considerar tres aspectos importantes: (a) las posibilidades de ocurrencia de los eventos; (b) los eventos deben caracterizarse por la incertidumbre, y (c) se debe esperar un resultado a partir de una inversión (Zorrilla, 2005).

En esa línea, la norma aborda los tres elementos anteriores, proporciona un enfoque común para gestionar cualquier tipo de riesgo y no es específica de una industria o un sector, de modo que la ISO 31000 se podrá utilizar en el tiempo de existencia de la organización. A su vez, podrá ser utilizada en diversas actividades en las que se incluye la planificación para toma de decisiones, sin importar el nivel.

Ahora bien, cabe recordar a Martínez y Casares (2011) quienes afirman que "la gerencia de riesgos en un entorno global se está perfilando como una estrategia financiera y empresarial que proporciona una importante ventaja competitiva a las empresas que disponen de ella" (p. 13), lo cual nos invita a retomar el factor diferenciador y la iteratividad para ayudar a las organizaciones a establecer su estrategia, lograr sus objetivos y tomar decisiones informadas.

Según las ideas de Ismodes (2019), y siguiendo la versión 2018 de la norma, algunos errores comunes que se pueden presentar en estos momentos y basados en la identificación de riesgos son:

a) Asumir que riesgo es solo un tema financiero u operacional.

b) Enfocarse en los datos históricos y no proyectar el futuro con escenarios.

c) Tratar de delimitar la cobertura de la gestión de riesgo.

d) Eliminar muy pronto riesgos de baja probabilidad y alto impacto.

e) Eliminar o no tomar en cuenta los riesgos no medibles.

f) Minimizar riesgos no tradicionales.

Figura 5. Principios, marco de referencia y proceso
Fuente: *Norma ISO 31000 (2018).*

Referencias normativas: la responsabilidad que recae en materia de abordar riesgos y oportunidades basados en la norma técnica publicada motivó a que ISO 31000 se actualizara a nivel mundial en la ISO 31000:2018, con el fin de resolver cómo y cuáles acciones se deben tomar para abordar los riesgos y oportunidades en las organizaciones, temas solucionados de forma concreta y detallada en los documentos rectores de la gestión de riesgos, a saber:

- **Norma técnica ISO 31000:2018** e **ISO IEC 31010**, la cual presenta treinta y un (31) técnicas para evaluación de riesgos.
- **La guía 73:2009**, que define la terminología y conceptos, entre ellos:
  - *Evaluación del riesgo:* "El proceso de comparación de los resultados del análisis del riesgo (3.6.1) con los criterios de riesgo (3.3.1.3) para determinar si el riesgo (1.1) y/o su magnitud son aceptables o tolerables".
  - *Actitud ante el riesgo:* "Enfoque de la organización para apreciar un riesgo (1.1) y eventualmente buscarlo, retenerlo, tomarlo o rechazarlo".

Explica el Instituto de Auditores Internos en su reciente publicación, actualizando las tres lineas de defensa, que

> "las organizaciones son empresas humanas que operan en un mundo cada vez más incierto, complejo, interconectado y volátil. A menudo tienen múltiples partes interesadas con intereses diversos, cambiables y en ocasiones, competitivos. Las partes interesadas confían la supervisión organizativa a un órgano de gobierno, que a su vez delega recursos y autoridad a la dirección para que tome las medidas apropiadas, incluyendo la gestión del riesgo."

Basados en la concepción del Instituto y los nuevos cambios que introdujo al actualizar el modelo, podemos ver cómo identificar las

estructuras y los procesos que hacen parte del proceso de administración de riesgos nos ayuda a cumplir los objetivos.

Resalta también el IIA que el modelo presentado se optimiza al "centrarse en la contribución de la gestión de riesgos a la obtención de objetivos y la creación de valor, así como en cuestiones de 'defensa' y protección del valor". De lo cual podemos evidenciar que ambas organizaciones, tanto ISO como el IIA, están alineadas en el valor que permite obtener a las organizaciones un proceso de administración de riesgos.

Toma de decisiones basadas en riesgos y recursos necesarios

El principio n.º 1 de las tres lineas de defensa resalta que la toma de decisiones basadas en el riesgo es un proceso considerado que incluye análisis, planificación, acción, monitoreo y revisión, y toma en cuenta los impactos potenciales de la incertidumbre sobre los objetivos.

Al mencionar aspectos de articulación con la gestión de riesgos, la ISO 31000 que el compromiso debería incluir: "La disponibilidad de los recursos necesarios" (p. 8). Hemos estado insistiendo en varios apartes del documento en la responsabilidad que le atañe a los líderes de la administración de riesgos.

Ambos documentos nos invitan a hablar de peligros e identificar la localización de estos, a "entender bien el riesgo, lo cual es entender bien el '*business model*' de la empresa y sus puntos de creación de valor" (Bapst, 2004). Entender si la implementación de algunos controles está en la misma via de los objetivos de la organización en que laboramos es muy importante, por ello reconocer mis capacidades, como las de mi adversario, las amenazas, los riesgos y el retorno de la inversión es vital.

Conclusiones

Al hablar de gestión de riesgos moderna, se trata un tema transversal a todos los gremios o sectores en cualquier país. En el gobierno corporativo, es necesario realizar un reconocimiento riguroso para identificar posibles riesgos.

El mayor descuido en procesos de administración de riesgos estaría en cabeza de la alta dirección: su apoyo, concentración y compromiso son vitales en varios sentidos y en cada estapa.

Cada día seguirán naciendo "nuevos" riesgos y esto impulsará la labor de administración de riesgos como papel estrategico dentro de las organizaciones. Para nadie es extraño que la estructura, roles y responsabilidades en las mismas se está moldeando a entornos flexibles e integrales, en donde la integración y comunicación es vital en tiempo real.

La introducción de la toma de decisiones basada en incertidumbre cambiará los modelos de gestión desde un punto de vista que antes se basaba en certidumbres. Por ende, desde ya podemos mencionar que estarán incluidas entre las habilidades y competencias que serán evaluadas y apetecidas por las organizaciones.

El valor de la información fiable y disponible cada día será mayor; la principal función del administrador de riesgos será realizar una excelente cartografia de los mismos. Esta deberá contemplar el cálculo del valor del impacto económico frente a las medidas de reducción de los posibles riesgos y estudiar en forma clara los costos en materia de implementación de medidas para controlarle, permitiendo un legible retorno de la inversión.

Cualquier empresa podrá hacerle frente a los diversos riesgos sin importar los ámbitos en los que actúe, inclusive escenarios habituales o de operaciones, aunque esto pueda generar algunos riesgos con

respecto a la toma de decisiones, pues "la esencia de 'hacer negocios' es, precisamente, correr riesgos. En otras palabras, el riesgo es una elección propia, más que una imposición o un obstáculo indeseable" (Deloitte et al., 2003).

Ahora bien, la ISO 31000 es una herramienta de gestión de riesgos que ha conseguido un reconocimiento internacional, es la base de todos los sistemas de gestión al momento de realizarse la adopción y entrada de los riesgos y oportunidades como parte fundamental del sistema de gestión, un instrumento que fomenta la adopción de ventajas competitivas para cualquier organización que implementa sus postulados. De otro lado, la implementación de la gestión de riesgos en diferentes sistemas de gestión tiene su origen en una necesidad particular, como la homologación de términos y conceptos que suelen ser utilizados en la gestión del riesgo. De esta forma, evita que estos sean interpretados por separado y mitiga los riesgos o posibles incidentes que puedan ocurrir.

Por último, las organizaciones que implementan la gestión de sus riesgos obtienen grandes beneficios, entre ellos:

1. Desarrollar enfoques estructurados hacia la gestión del riesgo que pueden contribuir a resultados positivos, que a su vez son coherentes y también pueden ser comparables.
2. Adaptación de las metas y proyecciones de las organizaciones a contextos de carácter interno y externo.
3. Promocionar una mayor consciencia y elección de gestión del riesgo, a partir de la participación de las partes que están interesadas de forma oportuna.
4. Anticipar, detectar o reconocer los riegos ante cualquier incertidumbre o limitación que identifiquen las organizaciones apropiadamente.

5. Mejorar continuamente el sistema de gestión del riesgo, a través de las experiencias y los aprendizajes.

Referencias

Bapst, P.A. (2004). El mapa de riesgos, punto de partida para una buena gerencia global de riesgos. *Gerencia de Riesgos y Seguros*, *21*(85), 31-39. https://dialnet.unirioja.es/ejemplar/87747

Bravo, O., & Sánchez, M. (2009). *Gestión integral de riesgos.* Bravo & Sánchez.

Contreras, A. (2020). Delgado hilo de conexión del delito cibernético y el crimen organizado [Diapositiva de PowerPoint]. Repositorio Biblioteca Q1 COLADCA Universidad UNAULA. https://bit.ly/2FWObd4

De Castro, S. (2000). Riesgos y peligros: una visión desde la geografía. *Scripta Nova. Revista Electrónica de Geografía y Ciencias Sociales*, *60*. http://www.ub.edu/geocrit/sn-60.htm

Deloitte & Touche, e Instituto Mexicano de Ejecutivos de Finanzas IMEF. (2003). *Administración integral de riesgos de negocio: cómo lograr una mayor efectividad en su evaluación y manejo: procesos y herramientas para minimizar su impacto: situación actual de las empresas de México*. Instituto Mexicano de Ejecutivos de Finanzas.

Gaultier-Gaillard & Louisot (2017). *Gerenciar los Riesgos en la empresa.* 3R Editores

Gil, T. (coord.), Comellas, D., Galdeano, I., Hernández, L., Jiménez, A., Jiménez, J., Lafita-Fernández, J., Llorente, C., Martin, V., Muñoz, C., & Werner C. (2013). *Definición e implantación de Apetito de Riesgo*. Instituto de Auditores internos de España y MAPFRE

Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC. (2015). *Norma Técnica Colombiana NTC-ISO 9001: Sistemas de Gestion de Calidad.* ICONTEC.

International Organization for Standardization, ISO. (2018). ISO 31000:2018, Traducción oficial, Gestión del riesgo — Directrices, Risk Management – Guidelines (Vol. 2). Suiza: ISO.

Ismodes, J. (2019). *GRC: Gobierno Corporativo, Riesgo y Cumplimiento Regulatorio*. Javier Ísmodes Cascón.

Izquierdo, J. (2003). Riesgo e incertidumbre en la gestión de proyectos informáticos. *Partida Doble*, *150*, 86-95.

Knight, F. (1964). Theories of Profit; Change and Risk in Relation to Profit. En F. Knight, *Risk, Uncertainty and Profit*. NY New century Press.

Knight, F. A. (2002). La ética de la competencia. *Revista de economía institucional*, *4*(7), 133-164. https://www.redalyc.org/pdf/419/41900708.pdf

Martínez, M., & Casares, I. (2011). El proceso de gestión de riesgos como componente integral de la gestión empresarial. *Boletín de Estudios Económicos*, *66*(202), 73-93.

McNamee, D. (2002). La Gerencia de riesgos hoy y mañana. Experiencias en administraciones públicas. *Gerencia de riesgos y seguros*, *19*(77), 17-30

Mejía, R. (2004). La administración de riesgos empresariales. *AD-MINISTER Universidad EAFIT*, 5, 74-85

Ortiz, L., & Valencia, F. (2017). Gestión de riesgos en eTOM. Un análisis comparativo con los estándares de riesgo corporativo. *Revista Logos Ciencia & Tecnología*, *9*(1), 85-99.

Real Academia Española RAE. (2019). Riesgo. *En el diccionario de la Real Academia de la Lengua Españo*la. http://dle.rae.es/?id=WT8tAMI

Revista Forbes. (2017, 4 de mayo). ¿Eres un C-suite? https://forbes.es/lifestyle/10872/eres-un-csuite/

Schumpeter, J. (2002). *Ciclos económicos: análisis teórico, histórico y estadístico del proceso capitalista*. Universidad de Zaragoza.

Smith, K. (1992). *Environmental hazards: assessing risk and reducing disaster*. Routledge.

The Institute of Internal Auditors, Inc. (2020). *El modelo de las tres líneas del IIA 2020, una actualización de las tres líneas de defensa*. Lake Mary, Estados Unidos. https://global.theiia.org/translations/PublicDocuments/Three-Lines-Model-Updated-Spanish.pdf

Universia. (2018, 30 de julio). ¿Trabajas en un entorno VICA y aún no lo sabes? https://noticias.universia.es/practicas-empleo/noticia/2018/07/30/1160918/trabajas-entorno-vica-aun-sabes.html

Velez, I. (2003). *Decisiones Empresariales Bajo Riesgo e Incertidumbre.* Grupo editorial Norma.

World Economic Forum. (2020). *The Global Risks Report 2020*.

Zorrilla, J. (2005). Globalización, incertidumbre y riesgo. *Intangible Capital*, *1*(9), 1-17.

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.

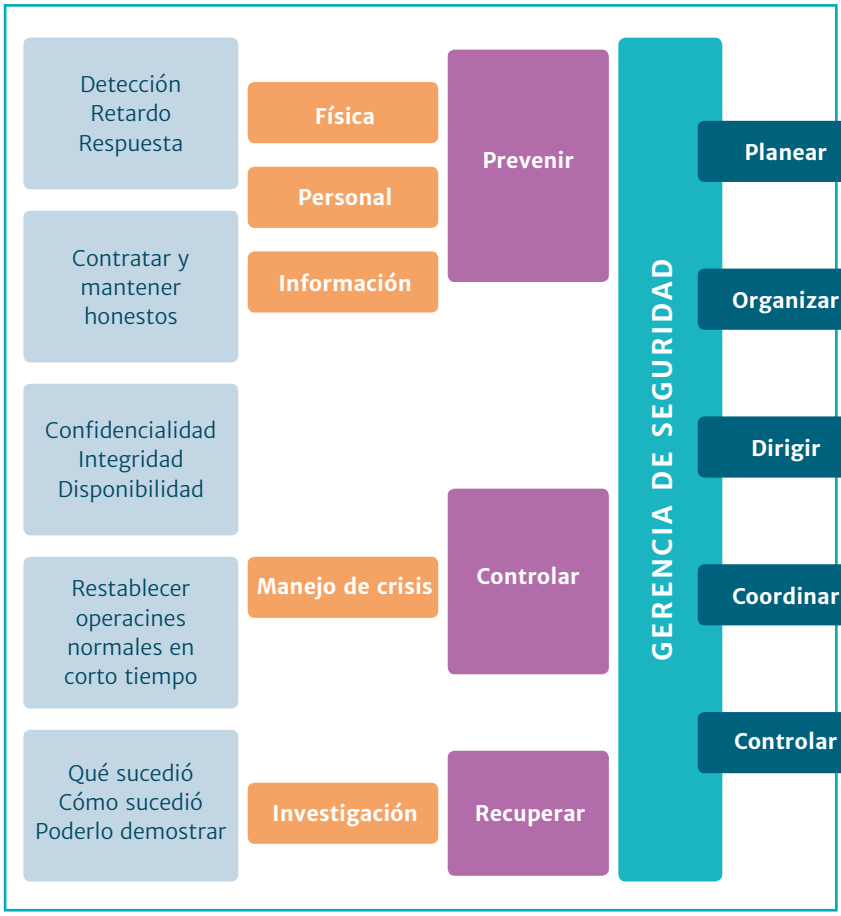


Figura 1. Relación habilidades técnicas vs. habilidades gerenciales
Fuente: *elaboración propia.*

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.

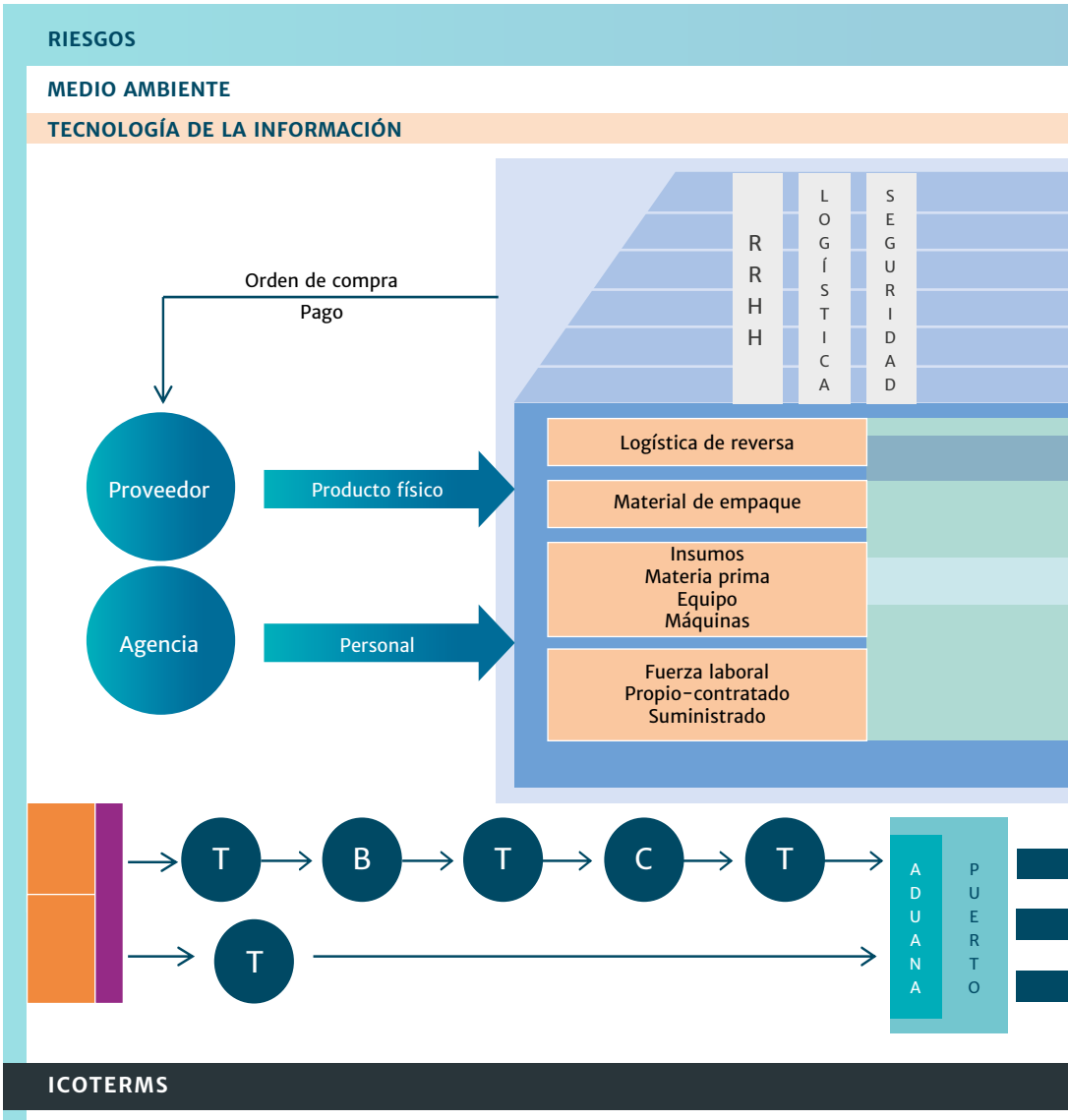
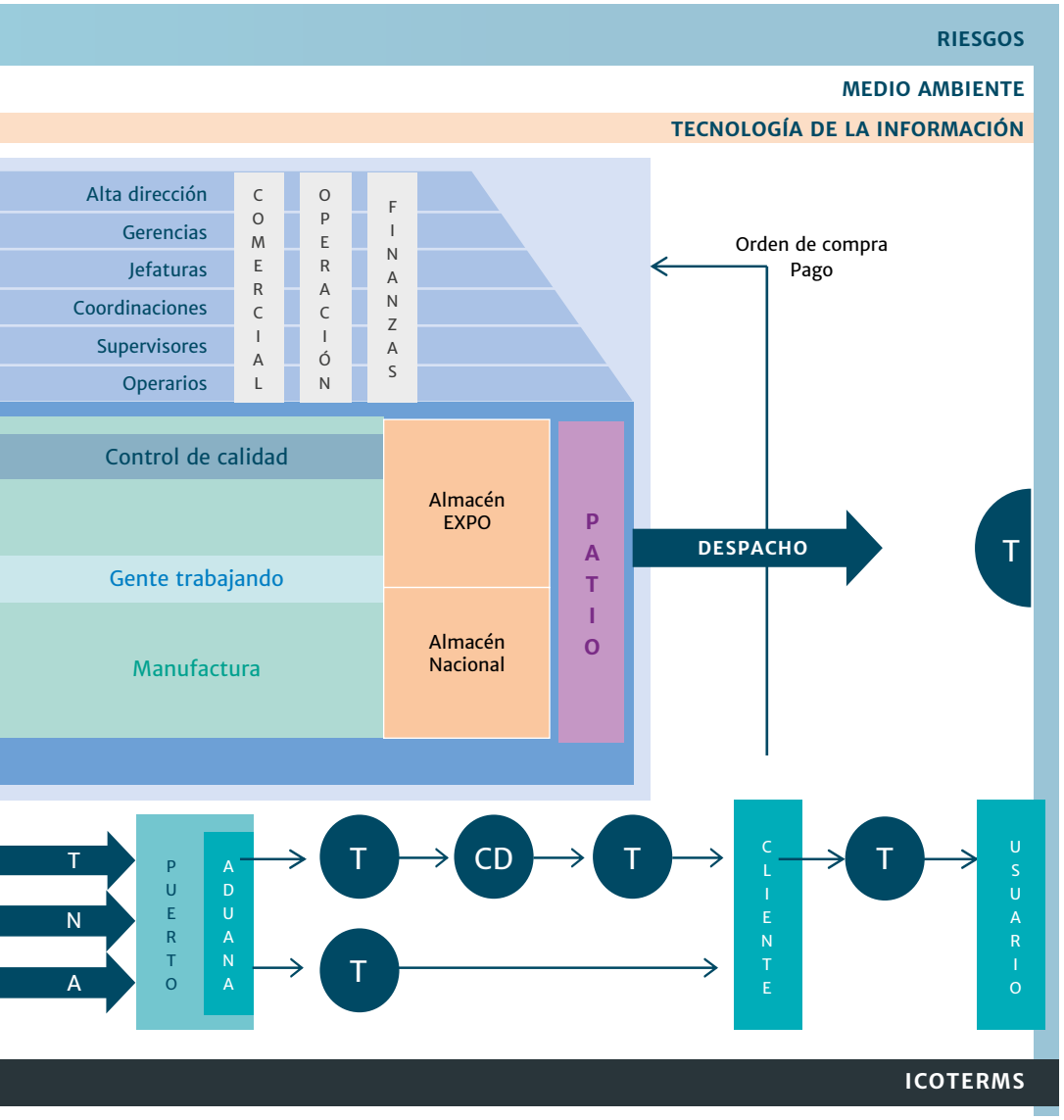


Figura 3. Cadena de Suministro
Fuente: *elaboración propia.*


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

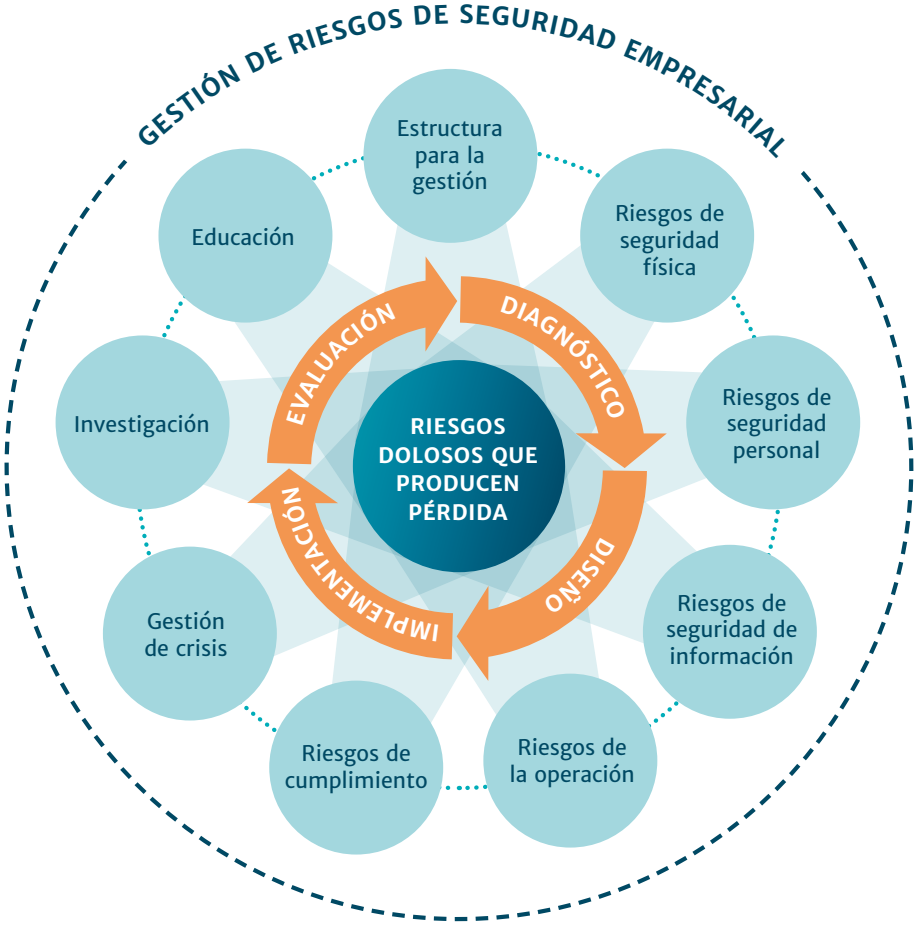


Figura 4. Integración de gestión de riesgos empresariales
Fuente: *elaboración propia*

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.

Capítulo 7

La gestión de seguridad en la cadena de suministro

Álvaro F. Moncada N.*

* Doctor en empresa en la economía internacionalizada. Magister en Administración de empresas y liderazgo estratégico. Investigador del programa de Maestría en Logística Aeronáutica de la Escuela de Postgrados de la Fuerza Aérea Colombiana. Correo electrónico: alvaro.moncada@hotmail.com.

CÓMO CITAR

Moncada, A. F. (2020). La gestión de seguridad en la cadena de suministro. En Y. Rico, D. López Cortés, & A. Cerón R. (comps.), *Enfoques y gestión en Seguridad Integral* (pp. 187-207). Escuela de Postgrados de la Fuerza Aérea Colombiana. https://doi.org/10.8667/9789585996199.07

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

CAPÍTULO 7.
La gestión de la seguridad en la cadena de suministro

https://doi.org/10.8667/9789585996199.07
Bogotá, Colombia
Noviembre, 2020

RESUMEN

Con el fin de mantenerse competitivas en entornos dinámicos, las empresas han requerido rediseñar sus cadenas de suministro para hacerlas cada vez más complejas y extensas, producir en países de bajo costo, con mayor número de eslabones y actores globales, lo cual en conjunto genera nuevas amenazas y riesgos que tienen su origen fuera de la empresa. Las interrupciones en la cadena de suministro y la turbulencia del entorno, muestran que las capacidades logísticas disponibles en las organizaciones (basadas en tiempo, costos, eficiencia y calidad) no son suficientes para identificar y mitigar las nuevas amenazas y riesgos existentes producto de diversos fenómenos como la globalización, las crisis económicas y la masificación de la tecnología, las cuales hacen cada vez más vulnerables dichos procesos a eventos internos y externos, especialmente los relacionados con el comercio exterior y el transporte multimodal. Esta nueva perspectiva demanda la incorporación de un nuevo elemento, la seguridad vista como un componente esencial para su adecuado funcionamiento y continuidad, ampliando su orientación de eficiencia en los procesos y riesgos operativos, hacia un enfoque global que incorpora la seguridad en cada uno de sus eslabones y actores.

El presente artículo incorpora la gestión de seguridad en la cadena de suministro, y presenta una propuesta para su análisis, usando como fundamento el estándar de mayor aplicación a nivel global, ISO 28000. Con la anterior, se brinda a la dirección de la empresa y a sus directivos, los elementos adecuados para la incorporación de la gestión de seguridad en su cadena de suministro (GSCS), fortaleciendo sus capacidades logísticas de gestión de la demanda, gestión del suministro y gestión e intercambio de información.

PALABRAS CLAVE

Control de calidad; gestión de recursos; operación administrativa; prevención de riesgos; seguridad.

Introducción

En el panorama económico actual, la gestión de la cadena de suministro es un elemento fundamental en el desarrollo económico de las naciones (Porter, 1987). Para mantenerse competitivas en mercados globalizados, las empresas se han visto obligadas a rediseñar sus cadenas de suministro, creando unas cada vez más complejas y extensas, basadas en la producción en países de bajo costo y con mayor número de proveedores distribuidos por el mundo (Stajniak, 2010). Esto se traduce en nuevas amenazas y riesgos, que no necesariamente tienen su origen en el interior de la organización o sus propios procesos.

Resultado de estos fenómenos externos, la cadena de suministro es cada vez más susceptible a las perturbaciones y vulnerable a eventos políticos, sociales y económicos, convirtiendo su seguridad en un reto complejo que demanda nuevos paradigmas para su identificación, análisis, valoración y mitigación (Chopra & Meindl, 2016).

En la cadena de suministro se pueden identificar espacios críticos en relación con la seguridad, por lo cual este factor se ha convertido en prioritario frente a los procesos de comercio global en las épocas recientes. En ese sentido, su adecuada gestión es un elemento fundamental del proceso logístico que amplía su alcance y la convierte en un requisito esencial para entregar los productos en el lugar correcto, el momento adecuado, con la cantidad y calidad requerida (Stajniak, 2010).

La dinámica del entorno muestra que las capacidades logísticas disponibles de la organización (basadas en tiempo, costos, eficiencia y calidad) no son suficientes para identificar y mitigar las nuevas amenazas y riesgos existentes, producto de diversos fenómenos como la

globalización, las crisis financieras, los desequilibrios económicos y la masificación de la tecnología. Estos fenómenos hacen cada vez más vulnerables las dinámicas de la cadena de suministro a sus eventos internos y externos, en especial los relacionados con el comercio exterior y el transporte multimodal.

Dicho esto, el riesgo en este escenario se define como "la probabilidad y el impacto de eventos o condiciones imprevistas de nivel macro o micro que influyen adversamente en cualquier parte de una cadena de suministro, conduciendo a fallas o irregularidades de nivel operacional, táctico o estratégico" (Ho et al., 2015, p. 5035). A su vez, Tablado (2016) lo define como los posibles sucesos que afectan de manera negativa el flujo de productos o servicios, cuyo resultado puede ser expresado en términos de perjuicio de orden cuantitativo o cualitativo, o en sus palabras, "la gestión del riesgo en la cadena de suministros trata de valorar, identificar y cuantificar las potenciales disrupciones para reducir el impacto en la misma" (Tablado, 2016, p. 2).

Esta nueva perspectiva demanda la incorporación del elemento seguridad, como componente esencial para el adecuado funcionamiento de la cadena de suministro, al ampliar su orientación de eficiencia en los procesos y riesgos operativos hacia un enfoque más global que incorpora la seguridad en cada uno de sus eslabones y actores. De ese modo, se busca responder a dicha necesidad mediante el análisis de la visibilidad, la capacidad de respuesta y la agilidad, como elementos fundamentales para garantizar que las cadenas de suministro del futuro conserven su ventaja competitiva.

Partiendo de un marco teórico sustentado en la seguridad de la cadena de suministro, este trabajo analiza los tipos y factores de riesgo que inciden en ella, desde la perspectiva de la cadena de valor,

clasificando el riesgo de la demanda, riesgo en la manufactura, riesgo en el suministro y riesgo en el flujo, para en conjunto evaluar su impacto y probabilidad de ocurrencia. Como resultado, se establece un marco de referencia para la gestión del riesgo en la cadena de suministro a partir de la identificación de riesgos y amenazas, el análisis de riesgos, la valoración y priorización de los riesgos, la implementación de las medidas que mitigan los riesgos y el monitoreo y seguimiento de la implementación, que, alineados con las normas de las ISO 28000, permiten un mejoramiento continuo de la seguridad en la cadena de suministro y conducen a la generación de ventaja comercial y competitiva.

Marco teórico

La seguridad en los procesos habituales de la cadena de suministro puede definirse como el "esfuerzo colaborativo interorganizacional que utiliza metodologías cuantitativas y cualitativas de gestión de riesgos para 'identificar, evaluar, mitigar' y monitorear sucesos o situaciones inesperadas de nivel macro y micro, que podrían afectar adversamente cualquier parte de una cadena de suministro" (Ho et al., 2015, p. 5036).

La seguridad en la cadena de suministro

Los diversos incidentes que ocurren en los países (terrorismo, narcotráfico, piratería, entre otros) y dentro de ellos (robos, huelgas, crisis

políticas y económicas), así como desastres naturales y ambientales, han obligado a las empresas a aumentar los controles y el seguimiento en el comercio internacional y local para garantizar la seguridad de las operaciones comerciales, mediante la implantación de mecanismos de actuación, que requieran algún tipo de estandarización y homologación entre los actores, a fin de que resulten efectivos para las partes y no incrementen significativamente los costos de las transacciones asociados a la logística de los productos y servicios. Es así como surgen los sistemas de gestión de seguridad en la cadena de suministro, tales como ISO 28000, Business Anti-Smuggling Coalition o Coalición Empresarial Anticontrabando (BASC) e innumerables iniciativas de los países para el movimiento y control de mercancía, entre las que se encuentran Customs-Trade Partnership Against Terrorism o Asociación de Aduanas y Comercio contra el Terrorismo (C-PAT), World Customs Organization u Organización Mundial de Aduanas (WCO), Operador Económico Autorizado (OEA) y Nuevo Esquema de Empresas Certificadas (NEEC)[1].

Dentro del alcance de dichas iniciativas se propone el establecimiento de lineamientos para el tratamiento adecuado de la seguridad, la implantación de un sistema de análisis y gestión de riesgos, la evaluación y gestión del componente de seguridad a todos los actores de la cadena, así como la comprensión y difusión sobre la idea de construir una cultura de la seguridad que coordine todas las actividades y

1 En específico, aduanas de los EE. UU. e Iniciativa de Protección de Fronteras (Border Protection Initiative), el Modelo de Normas de la Organización Mundial de Aduanas para la seguridad de la cadena de suministro (WCO) y el Reglamento de la Comunidad Europea para la Mejoría de la Seguridad de la Cadena de Suministro del Operador Económico Autorizado (OEA).

esté acorde a los desafíos del contexto. Cada estándar se compone de la identificación y evaluación de amenazas, la gestión y tratamiento del riesgo, la aplicación de normas que buscan contener las amenazas y riesgos, la preparación para atender incidentes de seguridad y emergencias, la gestión adecuada de los fallos e incidentes relacionados con la seguridad de la cadena de suministro y la gestión de la documentación (Intedya, 2016).

Según Peláez (2009), un sistema de gestión de la seguridad para la cadena de suministro es el componente de la gestión que comprende "la estructura organizativa, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos para determinar y llevar a cabo la política de gestión de la seguridad en la cadena de suministro" (2009, p. 28).

Por su parte, Monroy & Monroy (2014) afirman que normalmente un sistema de gestión "ayuda a las compañías a reducir costos en sus procesos, mejorar la efectividad de las operaciones, incentivar la innovación, potencializar la empresa en su mercado, eliminar barreras administrativas y comerciales, aumentar la satisfacción de clientes y sobre todo, a proteger todos y cada uno de sus procesos" (p. 20). Para su desarrollo se requieren cuatro etapas que describen el paso a paso del proceso, el cual, en la medida que se vuelve un ciclo recurrente, obtiene mejorías.

Según la ISO, un sistema de gestión se compone de cuatro etapas:

1. Etapa de generación del sistema de gestión propuesto.
2. Etapa de planeación en la que se definen las estrategias y estructuras requeridas para la implementación del sistema.

3. Etapa de implementación en la cual se ejecutan las acciones establecidas para poner en funcionamiento el sistema en la organización.
4. Etapa de control en la que se establecen los indicadores de desempeño del proceso que miden el cumplimiento de los objetivos fijados y se determinan las acciones preventivas y correctivas que puede requerir el sistema.

Tipos y factores de riesgo en la cadena de suministro

Según Trkman y McCormack (2009) y Olson y Wu (2010), los riesgos en la cadena de suministro se clasifican en internos y externos, dependiendo de la fuente que los origina, los internos son propios de la empresa y externos son los del entorno. En esa línea, Lin & Zhou (2011) proponen tres categorías de riesgos: (i) riesgo organizativo o interno, (ii) riesgo de la cadena de suministro o relacionado con la red y (iii) riesgo ambiental o externo.

Por otra parte, Ho et al. (2015) proponen un marco conceptual para la clasificación del riesgo de la cadena de suministro con diversos grados de impacto (riesgos macro y micro), tanto en la cadena de suministro externa como interna (riesgos de demanda, fabricación y suministro) y diferentes tipos de flujo (información, transporte y riesgos financieros).

En la siguiente tabla se presenta un resumen de los factores de riesgo y sus principales eventos:

Tabla 1. Identificación de riesgos según factores y tipo

Factor de riesgo	Eventos	
Riesgos en la demanda	· Pronósticos imprecisos de la demanda. · Variabilidad de la demanda. · Incertidumbre de la demanda. · Efecto látigo. · Exigentes niveles de servicio.	· Poder del cliente. · Deficiente relacionamiento con el cliente. · Cambios en la competencia. · Ciclo de vida de los productos. · Cambios en el mercado.
Riesgos en la manufactura	· Huelgas. · Ambiente deficiente de trabajo. · Insatisfacción de los trabajadores. · Ausencia de planes de entrenamiento. · Obsolescencia de productos. · Costos de inventario.	· Flexibilidad de la producción. · Capacidad de producción. · Calidad y seguridad de productos. · Mantenimiento insuficiente. · Proceso de fabricación inestable. · Cambios de diseño. · Cambios tecnológicos.
Riesgos en el suministro	· Imposibilidad para manejar cambios en la demanda. · Fallas en los requerimientos de entrega. · Imposibilidad de precios competitivos. · Retrasos tecnológicos. · Incapacidad para atender requerimientos de calidad. · Bancarrota de proveedores.	· Dependencia de proveedores. · Tercerización. · Número de proveedores. · Falta de integración con proveedores. · Gestión de proveedores. · Fortaleza de los proveedores. · Contrato.
Riesgos en los flujos	· Comercio electrónico. · Demoras en la información. · Falta de transparencia de la información entre logística y comercialización. · Seguridad de Internet. · Falta de compatibilidad en las plataformas de IT. · Fragmentación de proveedores de transporte. · Entrega a tiempo, dentro del presupuesto. · Daños en el transporte. · Accidentes en el transporte.	· Fluctuaciones en las divisas. · Fortaleza financiera del cliente · Variaciones de costo. · Fluctuaciones de precio. · Bajos márgenes de rentabilidad. · Crecimiento del mercado. · Tamaño del mercado. · Tiempo de procesamiento interno. · Gestión de cartera de clientes. · Periodos de crédito.

Fuente: *elaboración propia a partir de Trkman & McCormack (2009), Olson & Wu (2010), Lin & Zhou (2011), Bowersox et al. (2012), Gligor & Holcomb (2012), Ho et al. (2015) y Manners-Bell (2017).*

Impactos del riesgo en la cadena de suministro

Según el tipo de daño (posible o potencial), se diferencian cuatro impactos de los riesgos en la cadena de suministro, categorizados de acuerdo con las posibles consecuencias en la organización:

a. **Catastróficos**: son sucesos que arriesgan la supervivencia de las organizaciones, los más comunes son los asociados a desastres naturales.
b. **Críticos:** son aquellos eventos que tienen una consecuencia grave en el desarrollo de las operaciones de la cadena de suministro, pero sus alcances negativos no son una amenaza para el desarrollo normal de la compañía.
c. **Marginales:** se estipulan como riesgos que se controlan sin ninguna dificultad y su alcance es leve para la empresa.
d. **Despreciables:** sus efectos no se perciben a simple vista por la empresa. Además de ello, son elementos que hacen parte del día a día de las operaciones de la organización (García, 2009; Cerem Comunicación, 2017).

Matriz de riesgo e impacto

Tabla 2. Matriz de riesgos en la cadena de suministro

		Impacto				
		Despreciable	Menor	Moderado	Crítico	Catastrófico
PROBABILIDAD	Muy alta	B	B	A	A	A
	Alta	B	B	B	A	A
	Media	C	B	B	A	A
	Baja	C	C	B	A	A
	Muy baja	C	C	C	B	A

Fuente: *elaboración propia.*

Según lo establecido en los numerales anteriores, para cada riesgo se debe: (i) medir la probabilidad de ocurrencia del riesgo en la clasificación de raro, poco probable, posible, probable y muy probable, y (ii) medir el impacto o consecuencia de la ocurrencia del evento de riesgo en la clasificación de insignificante, menor, moderado, elevado o crítico y extremo o catastrófico.

El procedimiento consiste en (i) la ubicación de cada riesgo según su probabilidad e impacto en la matriz de riesgos y (ii) la clasificación de los riesgos en las categorías de: importancia alta (A), media (B) y baja (C).

El riesgo puede ser medido en forma económica, cuando se dispone de la información sobre el costo de la ocurrencia del riesgo, incluida su recuperación de la situación de contingencia. Este se conoce como el valor monetario esperado (EMV) y es calculado así:

$$\text{EMV} = \text{Probabilidad} \times \text{Impacto} * \text{Costo}$$

Gestión del riesgo en la cadena de suministro

Los riesgos se identifican con situaciones que impactan el desarrollo consecutivo de actividades. Para gestionarlos se usa el marco de referencia presentado a continuación:

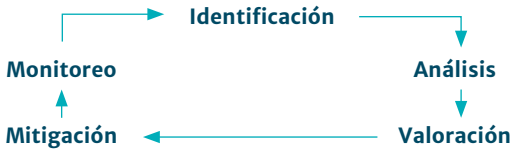


Figura 1. Marco de referencia para la gestión del riesgo en la cadena de suministro
Fuente: *elaboración propia.*

Identificación de riesgos y amenazas

Es necesario precisar que la amenaza es "todo aquello que tenga una posibilidad o probabilidad de ocurrir como causante de daño, mientras que el riesgo es el producto de la ocurrencia de la amenaza y su consecuencia" (García, 2009, p. 17). En esta actividad, se examina la incertidumbre que puede presentarse en la diversidad existente de los procesos de la cadena de suministro y se alistan sus consecuencias o riesgos significativos. Es decir, debe analizarse qué puede pasar, cómo puede pasar y por qué puede pasar.

Cabe señalar que el procedimiento se compone de la caracterización del proceso de suministro, se fracciona según las características y luego se define el riesgo en cada operación (Centro Latinoamericano de Innovación Logística, 2010). Dicho esto, basados en el trabajo de Ho et al. (2015), se propone la siguiente matriz para la identificación de los riesgos en la cadena de suministro:

Tabla 2. Identificación de riesgos según factores y tipo

Matriz tipo/factor riesgo		Tipo de riesgo			
		Micro		Macro	
		Interno	Externo	Interno	Externo
Factor riesgo	Demanda				
	Manufactura				
	Abastecimiento				
	Flujo				

Fuente: *elaboración propia.*

Análisis de riesgos

En esta actividad se obtiene una lista de cada uno de los riesgos identificados en la cadena de suministro, en la cual se establecen y analizan las probabilidades de ocurrencia y sus efectos. Para cada uno de ellos, se determina la probabilidad de ocurrencia del riesgo o materialización de la amenaza y se establece el impacto potencial o las consecuencias que se podrían generar en la cadena de suministro, usando generalmente la lista de impacto. Como señala Cañizares (2010) uno de los aspectos más complejos en la conceptualización y ejecución de un sistema de gestión de seguridad en la cadena de suministro es el análisis de los escenarios de riesgo, lo cual permite "obtener la información necesaria para establecer objetivos y metas para la gestión de la seguridad" (p. 9) en la cadena de suministro. Según Cañizares (2010), se precisa que dicho análisis de riesgos relacione cuáles son los objetivos propuestos por la organización en relación con su seguridad; cuáles son los rasgos más distintivos en términos generales del sistema, así como sus funciones y procesos principales; identificar cuáles son los activos críticos y cuáles no lo son en la organización; cuáles son los escenarios de amenazas y sus posibles resultados, cómo evaluar los planes y medidas implementados para gestionar el riesgo, entre otros aspectos relevantes.

Valoración y priorización de los riesgos

En esta actividad se hace una lista priorizada de riesgos basados en la matriz de probabilidad e impacto. Se clasifican en categorías y se seleccionan los de mayor impacto para trabajar en ellos de forma inmediata. Como resultado de esta actividad, se obtiene una matriz

priorizada de los riesgos de acuerdo con su importancia y necesidad de control.

Implementación de las medidas que mitigan los riesgos

Esta actividad busca mitigar la vulnerabilidad de la cadena de suministro. "Es el grado de exposición de la cadena de suministro a las interrupciones ocasionadas por los riesgos originados en las operaciones propias de cada organización, en las interacciones dentro de la cadena y en la interacción de esta con su entorno" (Centro Latinoamericano de Innovación Logística, 2010, p. 34).

Monitoreo y seguimiento

Con esta actividad se buscar medir si todos los procedimientos implementados están cumpliendo con su propósito. La comunicación es un factor clave para las personas y organizaciones que hacen parte de la cadena de suministro y la participación del personal es fundamental en cuanto a la consciencia que posean sobre sus compromisos con la seguridad y el conocimiento de normatividades y prácticas habituales de cualquier organización, en específico, sobre políticas, procedimientos y prácticas de la organización relativas al tema de seguridad.

El factor humano tiene mayor incidencia en la seguridad que el factor tecnológico y generalmente constituye en el eslabón más débil de la seguridad en la cadena de suministro. Su falta de involucramiento y compromiso puede conducir a la pérdida de la eficacia en las acciones y controles implementados.

La norma ISO 28000 y la gestión de seguridad en la cadena de suministro

El enfoque de la norma toma los pilares básicos de los criterios evaluativos del riesgo. La aplicación de la norma evidencia que las organizaciones que la implementan en sus procesos tienden a controlar el riesgo en la medida en que se incrementa un proceso sistemático de identificación, análisis y valoración de riesgos junto con sus respectivas acciones de mejora y monitoreo, lo cual contribuye a elevar los niveles de desempeño de la organización.

Farfán (2013) expone que la norma tiene cinco elementos esenciales: el sistema de gestión de seguridad que permite "desarrollar, mantener, documentar y mejorar el sistema"; la política de seguridad que orienta la identificación de factores críticos y la implementación de planes para su gestión; la evaluación, identificación y planificación del riesgo; la comunicación efectiva, y, por último, la etapa de verificación, mediante la cual se determina cómo funciona el sistema y cómo se realiza la medición que permite revisar el desempeño en forma objetiva.

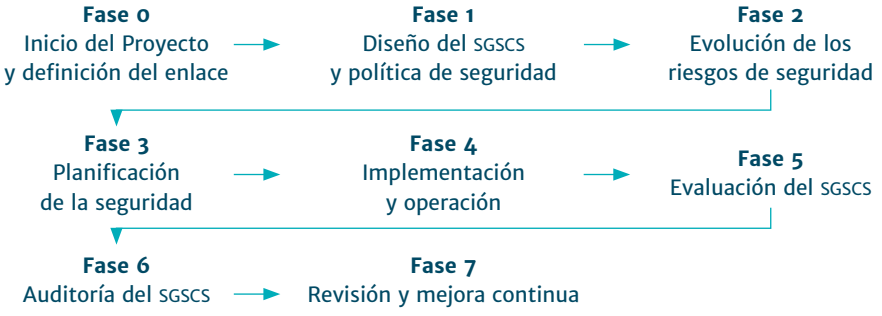


Figura 2. Fases en la implementación de SGSCS basado en la NTC-ISO 28000
Fuente: *elaboración propia.*

Por último, la familia ISO 28000 tiene cuatro desarrollos, cuyo propósito se resume a continuación:

- ISO 28001:2007. Calidad en aquellas prácticas para determinadas evaluaciones y planeamientos para la seguridad de las cadenas de suministro. Normalmente se complementa con iniciativas de seguridad de diferentes países u organizaciones.
- ISO 28002:2011. Desarrollo de directrices en la cadena de suministro.
- ISO 28003:2007. Lineamientos para organizaciones cuyo objetivo es prestar servicios en temas como las auditorías o certificaciones en el tema en cuestión.
- ISO 28004:2007. Directrices utilizadas en la aplicación e implementación de la normatividad ISO 2008, además del mantenimiento y mejoras.

Directrices para la aplicación de la norma ISO 2008, incluyendo la implementación, mantenimiento y mejora del sistema de gestión de la seguridad.

Conclusiones

Las condiciones del entorno y la dinámica global de los negocios exigen la incorporación de la seguridad como componente esencial para el adecuado funcionamiento y continuidad de la cadena de suministro, ampliando la orientación en la eficiencia de los procesos y control de los riesgos operativos hacia un enfoque global que incorpora la seguridad en cada uno de sus eslabones y actores. En tal sentido, se busca identificar las amenazas al evaluar y controlar los riesgos para así mitigar sus consecuencias, lo cual será alcanzado con la implementación del sistema de gestión de la seguridad en la cadena de suministro,

con un enfoque centrado en el negocio y en la toma de decisiones con base en la realización de evaluaciones de riesgos y amenazas, contribuyendo a la continuidad del negocio y la resiliencia empresarial.

El sistema de gestión de la seguridad en la cadena de suministro debe fundamentarse en la mejora continua, ya que la seguridad en la cadena de suministro debe ser un proceso iterativo que conduzca a mejoras en el desempeño general de la seguridad en todos los procesos y actores en los que se encuentra inmersa la organización. Esta orientación hacia la mejora continua permite la identificación de oportunidades y ajustes de prácticas ineficientes en la cadena de suministro, conduce a una gestión efectiva de recursos y capacidades de la organización, alinea los riegos con los objetivos empresariales y así contribuye a la generación de ventaja competitiva.

De esta forma, el objetivo principal del proceso de la gestión de riesgos en la cadena de suministro es establecer cuáles pueden ser las fuentes que perturban la cadena de suministro, así como medir cada factor de riesgo posible, además de evaluarlo (en impacto y probabilidad), tomar decisiones sobre qué políticas de riesgos se deberían aplicar en los casos que se presenten y poner en práctica las medidas preventivas correspondientes.

Específicamente, la norma ISO 28000 es uno de los sistemas de gestión de mayor aplicación en las organizaciones, ya que pretende establecer la seguridad en la cadena de suministro a partir de algunos criterios de los análisis de riesgo, identificar los aspectos relevantes para la continuidad del negocio y establecer las acciones para los posibles riesgos y amenazas, en un ambiente de mejora continua.

La implantación del sistema de gestión de seguridad en la cadena de suministro contribuye a una reducción de costos de forma global, puesto que permite aumentar el margen de efectividad de las

operaciones, construye espacios para el cambio y la implementación de opciones transformadoras, proyectando la competitividad de la empresa en su entorno natural de mercado, ya que los factores de innovación le permiten tener menos barreras de acceso en sus ventas y generar la fidelización de sus clientes.

Referencias

Bowersox, D., Closs, D., & Cooper, B. (2012). *Supply Chain Logistics Management.* McGraw-Hill Education.

Cañizares, R. (2010, 17 de enero). *La seguridad de la cadena de suministro.* Grupo Euler. https://es.slideshare.net/cprti/seguridad-en-la-cadena-de-suministro

Centro Latinoamericano de Innovación Logística. (2010, 26 de mayo). *Riesgo en cadena de abastecimiento.* LOGYCA. https://www.icesi.edu.co/blogs/bitacorariesgointegral1010/files/2010/11/gestion-de-riesgos-en-la-sch.pdf

Cerem Comunicación. (2017, 18 de octubre). *Reforzando la seguridad en la cadena de suministro.* Cerem International Business School. https://www.cerembs.co/blog/reforzando-la-seguridad-en-la-cadena-de-suministro

Chopra, S., & Meindl, P. (2016). *Supply Chain Management: Strategy, Planning and Operation* (6th ed.). Pearson.

Farfán, C. (2013). Sistema de gestión de la seguridad para la cadena de suministro. La ISO 28000. *Concepto Logístico,* 4, 6- 16.

García, R. (2009). Riesgos de la Cadena de Suministro. En D. Lloret, P. Peláez y R. García (Coord.), *ISO 28000:2007 - La seguridad en la Cadena de Suministro* (pp. 16-20). Centro Español de Logística. http://coslada.es/semsys/tesauro/visorImagenes.do?operacion=pintarImagen&codigoTermino=24213&codigoAtributo=213467&nombreFichero=guia-iso280002007.pdf

Gligor, D., & Holcomb, M. (2012). Understanding the Role of Logistics Capabilities in Achieving Supply Chain Agility: A Systematic Literature Review. *Supply Chain Management: an international Journal, 17*(4), 438-453.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply Chain Risk Management: a Literature Review. *International Journal of Production Research, 56*(16), 5031-5069.

Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC. (2008). *Norma Técnica Colombiana NTC-ISO 28000.*

Instituto Colombiano de Normas Técnicas y Certificación ICONTEC. (2016). *Certificación ISO 28000*. http://www.icontec.org/Ser/EvCon/Paginas/PCS/ci28000.aspx

Intedya International Dynamic Advisors. (2016). *Estándares nacionales para la gestión de la seguridad de la cadena de suministro*. Intedya International Dynamic Advisors. http://www.intedya.com/internacional/166/consultoria-estandares-nacionales-para-la-gestion-de-la-seguridad-de-la-cadena-de-suministro.html#submenuhome

Lin, Y., & Zhou, L. (2011). The Impacts of Product Design Changes on Supply Chain Risk: A Case Study. *International Journal of Physical Distribution & Logistics Management, 41*, 162-186.

Manners-Bell, J. (2017). *Supply Chain Risk Management: Understanding Emerging Threats to Global Supply Chains*. Kogan Page Publishers.

Monroy, N., & Monroy, M. (2014). *Desarrollo del sistema de gestión de la cadena de suministro en Carlon S.A. basado en la norma ISO 28000:2007* [Tesis de pregrado, Universidad Libre]. Repositorio de la Universidad Libre. https://repository.unilibre.edu.co/handle/10901/7849

Olson, D., & Wu, D. (2010). A Review of Enterprise Risk Management in Supply Chain. *Kybernetes, 39*, 694-706.

Peláez, P. (2009). Pasos para la implantación de la norma ISO 28000:2007. En D. Lloret, P. Peláez y R. García (Coord.), *ISO 28000:2007 - La seguridad en la Cadena de Suministro* (pp. 16-20). Centro Español de Logística. http://coslada.es/semsys/tesauro/visorImagenes.do?operacion=pintarImagen&codigoTermino=24213&codigoAtributo=213467&nombreFichero=guia-iso280002007.pdf

Porter, M. (1987). *Ventaja competitiva*. Editorial Continental.

Stajniak, M. (2010). Supply Chain Management-Safety Aspects. *Logforum*, *6*(4), 1-9.

Tablado, F. (2016). Gestión del riesgo. *Meetlogistics.* https://meetlogistics.com/wp-content/uploads/2016/10/La-gestión-del-riesgo-en-la-Cadena-de-Suministro.pdf

Trkman, P., & McCormack, K. (2009). Supply Chain Risk in Turbulent Environments – A Conceptual Model for Managing Supply Chain Network Risk. *International Journal of Production Economics*, *119*(2), 247-258.

Capítulo 8

La cuarta revolución y la era de la inteligencia artificial: implicaciones en la seguridad y el trabajo[1]

Carlos Enrique Álvarez Calderón*
Yesid Eduardo Ramírez Pedraza**

1 Este artículo hace parte del proyecto de investigación de la Maestría en Seguridad y Defensa Nacionales, titulado "Desafíos y nuevos escenarios de la seguridad multidimensional en el contexto nacional, regional y hemisférico en el decenio 2015-2025", el cual hace parte del grupo de investigación Centro de Gravedad de la Escuela Superior de Guerra General Rafael Reyes Prieto, reconocido y categorizado en (A1) por MINCIENCIAS, con el código COL0104976.

* Politólogo y magíster en Relaciones Internacionales de la Pontifica Universidad Javeriana. Coaching Ontológico Empresarial de la Universidad San Sebastián de Santiago de Chile. Coordinador de investigación en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra de Colombia. Correo electrónico: carlos.alvarez@esdegue.edu.co

** Coronel en retiro del Ejército Nacional de Colombia, magíster en Seguridad y Defensa del Colegio Interamericano de Seguridad y Defensa. Director de la Maestría en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra de Colombia. Correo electrónico: yesid.ramirez@esdegue.edu.co

CÓMO CITAR

Álvarez Calderón, C. E., & Ramírez Pedraza, Y. E. (2020). La cuarta revolución y la era de la inteligencia artificial: implicaciones en la seguridad y el trabajo. En Y. Rico, D. López, & A. Cerón R. (comps.), *Enfoques y gestión en Seguridad Integral* (pp. 209-237). Escuela de Postgrados de la Fuerza Aérea Colombiana. https://doi.org/10.8667/9789585996199.08

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

CAPÍTULO 8.
La cuarta revolución y la era de la inteligencia artificial: implicaciones en la seguridad y el trabajo

https://doi.org/10.8667/9789585996199.08
Bogotá, Colombia
Noviembre, 2020

RESUMEN

Las tecnologías de la información, potencializadas por la cuarta revolución industrial y su amplia adopción en el mundo, vienen dando lugar a una serie de nuevos y revolucionarios modelos comerciales, así como al surgimiento de nuevos desafíos en términos de seguridad. Por ejemplo, en un ambiente económico y productivo cada vez más dependiente del ciberespacio y la automatización, la seguridad de la información debería considerarse como un componente crítico de la seguridad integral de las organizaciones, ya que su función debe ser establecer la confianza entre organizaciones e individuos y permitir que el intercambio de información a través de Internet sea seguro y proporcione a las personas la tranquilidad necesaria para realizar sus actividades productivas. Por lo tanto, este documento de reflexión busca dar cuenta de cómo los recientes cambios tecnológicos están transformando en el presente los aspectos sociales, políticos y económicos de la vida humana, pero, además, la gestión de la seguridad en todos sus niveles.

PALABRAS CLAVE

Industrialización; inteligencia artificial; revolución tecnológica; seguridad laboral; sociedad de la información.

Introducción

Diversos estudios académicos (Jensen & Wiest, 2001; Søgaard et al., 2009; Headrick, 2009; Teng, 2014; Álvarez et. al., 2017; Álvarez & Zambrano, 2017), han dado cuenta de la importancia que el cambio tecnológico ha tenido a través de la historia en las creencias políticas y sociales, así como en la expansión del poder político y la riqueza material de las sociedades, un fenómeno que indudablemente antecede la reciente era digital.

Tradicionalmente, la tecnología se ha definido como la forma en que el conocimiento científico evoluciona en la producción de bienes, servicios y en el cumplimiento de objetivos, utilizando herramientas y técnicas para lograr ciertos resultados. El término "tecnología" se originó del uso que en el siglo XVI se le dio a la palabra griega *tekne* (τεχνη), que significa "arte, técnica u oficio", y *logos* (λογος), que significa "conjunto de saberes".

La historia de la relación entre la humanidad y la tecnología es extensa; se remonta millones de años atrás al primer uso humano de las piedras como herramientas y a su configuración en dispositivos más eficientes hacia el paleolítico temprano. Los pueblos primitivos descubrieron el uso del fuego como una tecnología de supervivencia e idearon sistemas cada vez más complejos de gestión del agua para el riego y posteriormente para la energía hidroeléctrica. Así mismo, a medida que las tecnologías de las comunicaciones se desarrollaban gracias a la difusión de la imprenta, el telégrafo o Internet, la gente pudo saber más sobre otros países, haciéndose más cosmopolita y conocedora de su entorno.

El periodo del renacimiento tardío en Europa occidental vio un gran progreso en las artes y las ciencias, así como la agitación social que unía a la Edad Media con la historia moderna. La tecnología cambió

los conjuntos de habilidades humanas al implementar métodos y procesos para el manejo de los recursos naturales y de esta manera obtener ventajas en la competencia y adquisición de servicios. A su vez, la tecnología en las ciencias de la salud y la agricultura mejoró la esperanza de vida, en especial en la Edad Moderna; y aunque dichas tecnologías parecían tener una función exclusivamente personal, pues hacían la vida más placentera y eficiente, los líderes de antaño y de tiempos más recientes han recurrido a la tecnología como una ayuda para construir los Estados y conquistar a otros pueblos. En efecto, acueductos que se extienden por cientos de kilómetros y la construcción de barcos para la guerra y el comercio fueron algunas de las tecnologías que les permitieron a estos líderes mantener y expandir su poder en el sistema internacional. El armamento comparativamente simple de la gente en la Edad de Piedra dio paso a una maquinaria más compleja para la conquista y la destrucción, armamento que ha tenido un uso cada vez más devastador (Álvarez et. al., 2017).

Las limitaciones de la fuerza mecánica humana y los descubrimientos del fuego, metales e iluminación, propiciaron el desarrollo de herramientas que ayudarían o sustituirían el esfuerzo humano (Zafirovski, 2011). Por esta razón, las máquinas se construyeron con el fin de proporcionar un medio para que los humanos pudiesen operar y lograr ciertas tareas, o para reemplazar el esfuerzo humano en su totalidad. La maquinaria consumida y la energía convertida proporcionaron, por medios mecánicos, químicos, térmicos, eléctricos u otros, plusvalías económicas que transformaron a la sociedad, la economía y, por supuesto, a la seguridad.

Dicho lo anterior, este documento de reflexión busca dar cuenta del impacto de los recientes cambios tecnológicos que van más allá de la computación tradicional y que el Foro Económico Mundial ha denominado la cuarta revolución industrial, la cual estaría transformando,

en el presente, los aspectos sociales, políticos y económicos de la vida humana, pero, además, la gestión de la seguridad en todos sus niveles.

Las primeras tres revoluciones

La palabra "revolución" denota un cambio abrupto y radical. De acuerdo con Shwab (2016), las revoluciones se han producido a lo largo de la historia cuando nuevas tecnologías y formas novedosas de percibir el mundo desencadenan un cambio profundo en los sistemas económicos y las estructuras sociales. En este orden de ideas, el primer cambio estructural en la forma de vida de los seres humanos pudo haber llegado a presentarse con la sedentarización de las sociedades y la domesticación de animales, en el proceso de transición hacia la agricultura, hace unos 10.000 años. Antes de la mecanización, el esfuerzo humano fue impulsado por la existencia de animales y la mano de obra humana para construir, trabajar la tierra y viajar; en este contexto, la revolución agraria combinó el esfuerzo animal con el de los seres humanos para la producción, el transporte y las comunicaciones. Luego, con la acción mecánica del agua, el viento y el fuego, la productividad agrícola se incrementó exponencialmente, estimulando el crecimiento de la población y permitiendo asentamientos humanos más grandes, dando paso, hace aproximadamente 5.000 años, a la urbanización y al surgimiento de los primeros estados primitivos (Álvarez, 2017).

A partir de la segunda mitad del siglo XVIII, la revolución agraria sería seguida por una serie de revoluciones industriales, las cuales "marcaron la transición de la potencia muscular a la potencia mecánica, evolucionando hacia la actual cuarta revolución industrial, en donde el poder cognitivo mejorado está aumentando la producción

humana" (Schwab, 2016, p. 11). En términos generales, se aceptó que el término "revolución industrial"[2] se pudiese referir, en principio, al periodo comprendido entre 1770 y 1870, en el cual el cambio tecnológico permitió aprovechar las fuerzas mecánicas y eléctricas para las transformaciones de los métodos de fabricación y producción que, aunados a nuevos modos de transporte y modernos tipos de infraestructura, abandonaron la lógica feudal de una economía dependiente de la actividad agrícola. Si bien su génesis se produciría en Occidente, particularmente en Gran Bretaña (transformando el Imperio Británico en el "taller del mundo"), en un siglo ya se había extendido al continente americano y a la cuenca del Asia y el Pacífico.

La primera revolución industrial, desencadenada por la construcción de ferrocarriles y la invención de la máquina de vapor, marcaría el comienzo de la producción mecánica. La primera máquina de vapor fue construida por Tomas Savery en 1698, y se utilizó para bombear agua acumulada de las minas de carbón; a pesar de la maravilla tecnológica que representaba para la época, tenía una aplicación limitada, ya que utilizaba presión atmosférica y trabajaba en contra del vacío del vapor condensado para extraer agua[3]. Sin embargo, el salto de la presión de vacío, pasando por la energía cinética mecánica, hasta el movimiento continuo de rotación, no se produciría sino hasta 1781 con el advenimiento del diseño revolucionario de James Watt para su máquina de vapor.

Su motor permitió alimentar una amplia gama de fabricación, maquinaria agrícola y de producción. El invento marcó el comienzo de lo

2 El término "revolución industrial" ingresó por primera vez en el léxico del pensamiento en 1799 (Cipolla, 2003).

3 Posteriormente, en 1712, Tomas Newcomen desarrollaría la primera máquina de vapor comercial basada en un diseño de pistón.

que se describiría como la primera revolución industrial y el inicio de la mecanización al permitir la producción de energía mecánica a partir de la energía térmica generada por la combustión de productos químicos y el oxígeno. Su revolución fue la capacidad de aprovechar la energía mecánica sin el uso de intervención humana o animal y facilitar a los seres humanos trabajar más eficazmente usando energía mecánica (desde bombas estacionarias fijas, elevadores de grúas y molinos, hasta la locomoción en forma de trenes y carruajes sin caballos). En consecuencia, y hacia 1886, las máquinas de vapor ya serían capaces de desarrollar 10.000 caballos de fuerza, utilizándose a gran escala en barcos de vapor interoceánicos y locomotoras industriales de largo alcance (Jörg, 2016).

La segunda revolución industrial, de finales del siglo XIX y principios del siglo XX, hizo posible la producción en masa, fomentada por el advenimiento de la cadena de montaje, los motores eléctricos y la electrificación a escala industrial. Adicionalmente, el motor de combustión petroquímico y el prototipo inicial del moderno motor de gasolina habilitaron la construcción del primer automóvil en 1885 por parte de Gottlieb Daimler.

La tercera revolución industrial se daría a partir de 1960. Suele denominarse revolución "informática" o "digital", ya que se caracterizó por el desarrollo de los semiconductores (década de 1960), la informática personal (años 70 y 80), e Internet (década de 1990). Sus inicios se establecieron con los desarrollos en la microelectrónica y los semiconductores de mediados de la década de 1950 hasta principios de los años setenta, cuando los primeros procesos de integración a gran escala crearon circuitos integrados, combinando miles de transistores en un solo chip (Cooper & Kaplinsky, 1989).

El circuito integrado aceleró el paso desde la tecnología mecánica y analógica a la electrónica digital, transformando la digitalización

de la información y los procesos informáticos, que, como resultado, alentaron el surgimiento de la informática empresarial, liderada por compañías como IBM, Hewlett Packard, Microsoft, Sun Microsystems y una plétora de diferentes empresas. Eventualmente, el desarrollo de las telecomunicaciones y su infraestructura condujeron al inicio de Internet en la década de 1990, que hacia finales de esta ya había creado los cimientos de los centros de datos mundiales, los dispositivos móviles y la aparición de los motores de búsqueda (como Google), los mercados en línea (como Amazon o Apple Store), las redes sociales (como Facebook y Twitter), entre muchas otras plataformas, extendiendo la revolución digital a todos los rincones del mundo y conectando a personas e industrias en una escala sin precedentes.

La cuarta revolución industrial: implicaciones en el trabajo

El nacimiento de la World Wide Web trajo consigo una nueva sintaxis y protocolos que permitieron a las maquinas "hablar" entre ellas y con los humanos; a su vez, los acelerados avances en la inversión de espectro y ancho de banda proporcionaron enlaces a empresas comerciales y ciudades, a las infraestructuras de redes de transporte, energía y servicios públicos. No obstante, desde comienzos del siglo XXI, nuevos avances tecnológicos en inteligencia artificial, impresión 3D, robótica, computación cuántica, nanotecnología y bioingeniería, entre otras, estarían cambiando radicalmente la manera de fabricar, intercambiar y consumir materiales, dinero, productos y servicios.

Este conjunto de tecnologías dio cuenta de una cuarta revolución industrial. Si bien parten de la revolución digital, es la fusión de estas tecnologías y su interacción a través de los dominios físicos, digitales

y biológicos lo que hace que la cuarta revolución industrial sea fundamentalmente diferente de las revoluciones anteriores (Shwab, 2016).

> En esta cuarta revolución, las tecnologías emergentes y la innovación de amplia base se difunden mucho más rápido y más ampliamente que en las anteriores, que continúan desarrollándose en algunas partes del mundo. La segunda revolución industrial aún no se ha experimentado por completo en el 17 % del mundo, ya que casi 1.300 millones de personas aún carecen de acceso a la electricidad. Esto también es cierto para la tercera revolución industrial, con más de la mitad de la población mundial (4.000 millones de personas), la mayoría de las cuales vive en el mundo en desarrollo, sin acceso a Internet. Sin embargo, mientras el huso (el sello distintivo de la primera revolución industrial), tardó casi 120 años en extenderse fuera de Europa, por el contrario, el Internet permeó en todo el mundo en menos de una década (Shwab, 2016, pp.12-13).

Los avances técnicos en las ciencias de materiales, nuevas técnicas de fabricación, inteligencia artificial, investigación biológica, el internet de las cosas, las ciudades inteligentes, los automóviles sin conductor, la telemedicina, entre otros, han permitido desarrollos dentro de la cuarta revolución que tendrían el potencial de cambiar industrias enteras y la experiencia humana. Pero la cuarta revolución industrial también destaca la paradoja de estas tecnologías disruptivas y las nuevas habilidades que cambiarían la productividad a través de la automatización, planteando uno de los mayores desafíos al empleo humano.

Durante siglos, la llegada de nuevas tecnologías al lugar de trabajo ha provocado temores entre los trabajadores y, a veces, reacciones violentas. Ya en 1589 la reina Isabel I de Inglaterra se negó a otorgarle una patente a un bastidor inventado por William Lee porque supuestamente estaba preocupada por el efecto que este tendría en el gremio de los tejedores a mano. A principios del siglo XIX, los trabajadores

textiles de Gran Bretaña y Francia rompieron telares automáticos en sus fábricas y los impresores manuales protestaron la llegada de las prensas a vapor.

Desde la Primera Revolución Industrial en el siglo XVIII, las economías de Europa, Estados Unidos y otros países sufrieron dos oleadas de cambios estructurales. Durante la primera oleada, la mecanización permitió una revolución en la agricultura y en la industria, lo que provocaría una migración de los trabajadores del campo a las ciudades; la segunda se produjo en los últimos 60 años, ya que la participación del empleo en el sector manufacturero ha disminuido en algunos países, incluso cuando el crecimiento en los sectores de servicios se aceleró (Herrendorf et al., 2014). Los cambios de los empleos que han venido acompañando este proceso de transformación estructural han sido relevantes; por ejemplo, en los Estados Unidos la participación de la agricultura en el empleo disminuiría del 58 % del empleo total en 1850, al 2,5 % del empleo en la actualidad. En solo 40 años, entre 1880 y 1920, la participación del empleo agrícola disminuyó un 25 %; durante las mismas décadas, otros sectores también se transformaron por la mecanización y la electrificación, como, por ejemplo, la disminución en la proporción de mineros y trabajadores domésticos.

Desde 1960, cuando comenzó la segunda ola de transformación estructural, la fabricación cayó del 27 % al 9 % del empleo total en los Estados Unidos, a medida que la automatización y el comercio mundial transformaron la fabricación y la demanda de servicios. En general, los patrones son similares en otros países; el empleo agrícola en China cayó como porcentaje del empleo total el 32 % en solo 25 años, del 60 % en 1990, al 28 % en el 2015. En México, la participación de la agricultura en el empleo disminuyó del 52 % en 1960 al 13 % en el 2015. En Japón, el empleo agrícola disminuyó de una proporción del 31 % del empleo total en 1960 al 3,5 % en el 2015 (Manyika et al., 2017).

Desde David Ricardo hasta Karl Marx y John Maynard Keynes, expresaron en su momento las preocupaciones por el efecto del cambio tecnológico en el empleo, como sucede en el presente con los rápidos avances en robótica e inteligencia artificial. El economista político David Ricardo estaba preocupado a principios del siglo XIX porque las máquinas harían que el trabajo fuera redundante (Ricardo, 2004), mientras que Karl Marx preveía, en 1850, una era en la que los medios de trabajo serían transformados por "un sistema automático de maquinaria" (Marx, 1973). En 1930, John Maynard Keynes acuñó el término "desempleo tecnológico" para describir una situación en la que la innovación que economizaba en el uso del trabajo desarticulaba el ritmo al que podían crearse nuevos empleos, en una "fase temporal de inadaptación" (Keynes, 1963). En consonancia, varios académicos y tecnólogos destacados como Brynjolfsson y McAfee (2014) sostienen que la última ola de tecnologías podría ser particularmente perturbadora para el mercado laboral a nivel mundial en los próximos años.

Figura 1. Evolución de las Revoluciones Industriales
Fuente: *Adaptado de Skilton & Hovsepian (2018).*

Hoy por hoy, algoritmos dictan la negociación automatizada de billones de dólares en activos de los mercados financieros, mientras los *chatbots* artificialmente inteligentes estarían desplazando a los humanos en los centros de atención telefónica o *call center*. Muy pronto los aviones y los automóviles podrían funcionar de manera autónoma, poniendo en peligro los medios de subsistencia de aquellos que conducen profesionalmente. A pesar de que los robots han venido realizando ciertos trabajos repetitivos en diversas fábricas durante décadas (como es el caso de las plantas ensambladoras de automóviles), ahora podrán "voltear" la carne de hamburguesas en la parrilla, descartar tomates verdes en una máquina clasificadora de alta velocidad usando reconocimiento de imágenes, o incluso colocar ladrillos en obras de construcción; inclusive, impresoras gigantes 3D en la actualidad podrían hacer casas de hormigón en una fracción del tiempo de lo que le tomaría a un equipo de obreros experimentados.

La Federación Internacional de Robótica afirmaba que en los procesos de fabricación, en el 2018, existía un promedio de 99 unidades de robots industriales por cada 10.000 empleados, en comparación con 74 unidades en el 2016. En el 2018, la instalación global de robots industriales aumentó un 6 % con relación al 2017, alcanzando las 422.271 unidades y una cifra de US$16,5 billones; el principal motor del crecimiento sería, al igual que en el pasado, la industria eléctrica y de electrónica (un incremento del 41 %). No obstante, la industria automotriz sigue constituyéndose como el principal cliente de robots industriales, participa del 30 % del total de instalaciones, seguido por la industria eléctrica y electrónica con el 25 %, la industria metalmecánica con el 10 %, la industria de plásticos y químicos con el 5 %, y la industria de comidas y bebidas con el 3 % (el 19 % restante se distribuye en una diversidad de sectores industriales y agroindustriales) (Wittmann, 2019).

Los 5 principales mercados de robots industriales están en China, Japón, Estados Unidos, Corea del Sur y Alemania, y concentran el 74 % de las instalaciones globales de robots industriales. Según Wittmann (2019), China es el principal mercado desde el 2013, representando el 36 % del total de las instalaciones en el 2017 y el 2018; tan solo en el 2018, se instalaron en China 154.032 unidades de robots industriales, una cantidad que excede el número combinado de robots industriales instalados en el continente americano y europeo (130.772 unidades). Los siguientes mercados de importancia en la instalación de robots industriales son Japón, con 55.240 unidades y los Estados Unidos, con 40.373 unidades instaladas en el 2018.

Por su parte, el número total de robots de servicios profesionales vendidos en el 2018 aumentó en un 61 %, a 271.000 unidades, de los 168.000 en el 2017, alcanzando la cifra de US$9,2 billones. Los vehículos autónomos, particularmente los vehículos aéreos no tripulados, representan la fracción más grande en el mercado de robots de servicio profesional (41 % de todas las unidades vendidas). La segunda categoría más grande son los robots de inspección y mantenimiento, participan del 39 % de todas las unidades vendidas. Por su parte, los robots de servicio para aplicaciones de defensa representaron el 5 % del número total de robots de servicio vendidos en el 2018 (Haegele, 2019). Con relación a las ventas de exoesqueletos humanos motorizados, estas aumentaron de 6.700 unidades en el 2017 a 7.300 unidades en el 2018 y su creciente demanda se debe a que los exoesqueletos respaldan el trabajo ergonómico al reducir las cargas en el trabajador.

A pesar de que se encuentran entre los robots de servicio más caros del mercado, se ha presentado una importante dinámica en las ventas de robots médicos, pasando de 3.400 unidades en el 2017 a 5.100 unidades vendidas en el 2018 (un aumento del 50 %). Las aplicaciones

médicas más importantes de robots de servicios son la cirugía asistida por robot o los sistemas de terapia y rehabilitación (Haegele, 2019). Los robots también han jugado un papel importante en la lucha contra el COVID-19 en todo el mundo; por ejemplo, el robot de desinfección UVD ha tenido una gran demanda desde el brote de la pandemia de COVID-19 en el 2020, hasta el punto de que se ordenaron más de 2.000 robots UVD para destruir el virus en los hospitales de China, y particularmente en la ciudad de Wuhan, el epicentro de la pandemia. Con relación a lo anterior, los robots de servicio para uso personal y doméstico se encuentran principalmente en las áreas de robots domésticos (aspiración, limpieza de pisos, corte de césped, limpieza de piscinas) y robots de entretenimiento (juguetes, sistemas de pasatiempos, educación e investigación). El número total de robots de servicio para uso personal y doméstico aumentó en un 59 % en el 2018 con relación al 2017; tan solo en el 2018, se vendieron más de 11,6 millones de robots aspiradores y limpiadores de pisos (Haegele, 2019).

En suma, la automatización del software informada por el aprendizaje automático y la inteligencia artificial (IA) tendría un profundo efecto en el mercado laboral. Los *chatbots* inteligentes parecerían reemplazar a la mayoría del personal de los *call center* en unos 10 años, hasta el punto de que, para el 2020, el 85 % de las preguntas podrían llegar a ser respondidas por asistentes virtuales; cuando se tiene en cuenta que una gran compañía de telecomunicaciones como AT&T emplea alrededor de 100.000 operadores de *call center* para atender a sus 120 millones de clientes, se evidencia que serían muchos los trabajos que podrían desaparecer rápidamente como consecuencia de la cuarta revolución industrial. En Colombia, el impacto también sería notorio, tomando en cuenta que esta industria que factura $2,9 billones de pesos, empleaba en el 2014 unas 180.000 personas.

Manyika et al. (2017) concluyen que casi dos tercios de todos los puestos de trabajo podrían tener una parte significativa de sus actividades automatizadas para el 2030 (al menos un 30 %), afectando 800 millones de puestos de trabajo. La automatización podría acelerar la productividad de la economía mundial entre 0,8 y 1,4 % del Producto Interno Bruto (PIB) global al año, suponiendo que la mano de obra humana reemplazada por la automatización vuelva a unirse a la fuerza de trabajo y sea tan productiva como lo fue en el 2014. La automatización por sí sola no sería suficiente para lograr aspiraciones de crecimiento económico a largo plazo en todo el mundo; para eso, se necesitarían medidas adicionales que aumenten la productividad, incluida la reelaboración de procesos comerciales o el desarrollo de nuevos productos y servicios. No obstante, el crecimiento de la productividad que permite la automatización puede garantizar la prosperidad continua en las naciones envejecidas y proporcionar un impulso adicional a las de rápido crecimiento. Para las empresas, la implementación de la automatización podría brindar beneficios en el ahorro de costos laborales, pero también en una miríada de otras formas de mejorar el rendimiento. Puede facilitarles a las empresas acercarse a los clientes y predecir las necesidades de mantenimiento, reduciendo drásticamente el costo de las operaciones en algunas actividades y ampliando la vida útil de los activos de capital existentes.

La inteligencia artificial: implicaciones en la seguridad

La inteligencia artificial (IA) podría ser definida como "cualquier sistema artificial que realice tareas en circunstancias variables e impredecibles, sin supervisión humana significativa, o que pueda aprender

de su experiencia y mejorar su rendimiento [...], pudiendo resolver tareas que requieren percepción, cognición, planificación, aprendizaje, comunicación, o acción física" (Ayoub & Payne, 2016, p. 812).

Si bien el campo de la investigación en IA comenzó en 1956[4], su interés se vería potencializado en el 2010 gracias a la convergencia de tres desarrollos habilitantes: la disponibilidad de fuentes de *Big Data*[5], mejoras en los enfoques de aprendizaje automático y el aumento en el poder de procesamiento de la computadora. Este crecimiento ha avanzado el estado de la IA "modular", que se refiere a algoritmos que abordan conjuntos de problemas específicos, como juegos, reconocimiento de imágenes y vehículos autónomos (todos los sistemas actuales de IA caen dentro de la categoría de la IA modular). El enfoque más prevalente para la IA modular es el aprendizaje automático, que implica algoritmos estadísticos que replican las tareas cognitivas humanas derivando sus propios procedimientos a través del análisis de grandes conjuntos de datos de entrenamiento. Durante el proceso de capacitación, el sistema informático crea su propio modelo estadístico para realizar la tarea especificada en situaciones que no ha encontrado anteriormente.

Las IA modulares tienen una experiencia limitada en un dominio particular y pueden aprender a través de la práctica para mejorar su rendimiento. Una IA general, por el contrario, puede utilizar su

---

4 En 1956, John McCarthy propuso organizar un taller de dos meses sobre la idea de la recién creada inteligencia artificial. La reunión estimuló la investigación que condujo primero a sistemas automáticos y luego a sistemas expertos en los años 70 y 80, respectivamente. El primero implicaba la automatización simple de máquinas de preguntas matemáticas y estadísticas, incluida la resolución de pruebas lógicas.

5 Los *Big Data* o Metadatos son aquellos conjuntos de datos o combinaciones de conjuntos de datos cuyo tamaño (volumen), complejidad (variabilidad) y velocidad de crecimiento (velocidad) dificultan su captura, gestión, procesamiento o análisis mediante tecnologías y herramientas convencionales, tales como bases de datos relacionales y estadísticas convencionales. La mayoría de los analistas y profesionales actualmente se refieren a los *Big Data* como los conjuntos de datos que van desde 30-50 Terabytes a varios Petabytes.

conocimiento de forma mucho más flexible para abordar una gama mucho más amplia de problemas más abstractos y sin límites, incluidos los que requieren una comprensión de los significados y valores. Tanto la IA modular como la general son capaces de aprender acerca de la tarea en la que participan y de mejorar su desempeño a lo largo del tiempo. Una IA modular que trabaja para mejorar el rendimiento de su dominio es similar a un golfista que perfecciona su *swing*, o a un guitarrista virtuoso que trabaja en su solo; la máquina aprende y se adapta, pero su arquitectura subyacente (*hardware* y *software* por igual) permanece sin cambios.

Los expertos generalmente coinciden en que pasarán muchas décadas antes de que se pueda avanzar a un estado de IA general, o a sistemas capaces de inteligencia a nivel humano en una amplia gama de tareas. Sin embargo, el creciente poder de los algoritmos de IA modulares ha provocado una ola de interés comercial. La inversión en IA está creciendo rápidamente, dominada por gigantes digitales como Google y Baidu; por su parte, Manyika et al. (2017) estimaron que a nivel mundial los gigantes tecnológicos gastaron entre US$20 mil millones a US$30 mil millones en IA en el 2016, con un 90 % de este gasto en Investigación y Desarrollo (I+D) y un 10 % en adquisiciones de IA.

En el marco de las guerras de quinta generación (Álvarez et. al., 2017), la IA tendría una serie de características únicas que podría ser importante a considerar a medida que estas tecnologías ingresaran al campo de la seguridad nacional. Primero, la IA es una tecnología de uso múltiple, ya que tiene el potencial de integrarse en prácticamente todo lo que se estime; Kelley (2014) declaraba que la IA "animará a los objetos inertes, como lo hizo la electricidad hace más de un siglo. Todo lo que antes electrificamos ahora lo cognitizaremos" (p. 23). En segundo lugar, muchas aplicaciones de IA serían de doble uso, es decir, que tienen aplicaciones militares y civiles. Por ejemplo,

"los algoritmos de reconocimiento de imágenes pueden entrenarse para reconocer gatos en videos de YouTube y actividades terroristas en videos en movimiento (FMV) capturados por aviones piloteados remotamente (RPA) en Siria o Afganistán" (Allen & Chan, 2017, p. 47). En tercer lugar, la IA es relativamente transparente, lo que significa que su integración en un producto no sería inmediatamente reconocible.

A nivel táctico, las ventajas de la IA modular le otorgarían ventajas a un actor de ganar las batallas donde pueda desplegarse efectivamente. Una IA modular que puede optimizar alguna actividad táctica (por ejemplo, el asalto a una posición enemiga, la coordinación rápida de ataques y la maniobra a través de plataformas automatizadas en red), superaría con creces a un comandante de batallón experimentado. El poder marítimo y aéreo serían los dominios más susceptibles a la IA debido a la falta comparativa de la compleja intervención humana relativa, por ejemplo, a la guerra urbana irregular (Álvarez, 2017). No obstante, existe un riesgo a que la IA no esté libre de errores; en 1988, el sistema de puntería de un destructor estadounidense equipado con Aegis derribó por error a un avión civil iraní, identificándolo como un caza F-14 (Singer, 2004). En este sentido, una capacidad táctica tuvo un impacto estratégico. En el futuro, las decisiones similares sobre la identidad de los posibles adversarios serán cada vez más automatizadas, sobre todo porque los sistemas opuestos de otra manera serán tecnológicamente capaces de frustrar a los operadores humanos. Un ataque de enjambres de ágiles y autónomos actores solo podría defenderse con sistemas que operen rápidamente, con autonomía e inteligencia.

En el nivel de toma de decisiones estratégicas, la IA modular podría mejorar la calidad de la toma de decisiones humanas a niveles estratégicos, utilizando sus capacidades para modelar a través de micromundos, evaluando riesgos. La máquina podría dominar grandes

cantidades de datos, reconocer patrones que de otro modo podrían pasarse por alto y desafiar las suposiciones aceptadas. Podría responder a situaciones dinámicas más rápidamente y con menos deficiencias cognitivas que un estratega humano. La IA podrá evitar algunos de los defectos humanos de la estrategia, como la susceptibilidad a invertir en costos irrecuperables o el razonamiento afectivo, incluido el juicio de riesgo sesgado. Puede mitigar los efectos de la fatiga y el estrés, así como la carga de sobrecarga de información (Ayoub & Payne, 2016). Una IA modular que actúa como consejero estratégico puede conferir una ventaja distintiva anticipando e identificando riesgos con opciones estratégicas, incluidas aquellas que los humanos no han previsto; y podría aprender de sus errores y mejorar sus algoritmos a medida que avanza el conflicto, mientras que los humanos permanecen enraizados en su heurística cognitiva y arraigado pensamiento grupal.

Un actor protagónico en el conflicto ideológico que caracterizarían las guerras de redes (*Net War*), en el marco de guerras de quinta generación, serían las redes sociales (Álvarez et. al., 2017). Las redes sociales se describen como el software que permite a las personas interactuar, conectarse, jugar o colaborar mediante el uso de una red informática. Esta definición abarca los sitios populares de redes sociales, incluidos *blogs*, *wikis*, *podcasts*, etiquetas y, más recientemente, los motores de búsqueda. Incluso hace relativamente poco, el uso de comunidades en línea para establecer y construir conexiones entre aquellos con intereses compartidos también se ha convertido en parte del mundo corporativo. A medida que las redes sociales profesionales como LinkedIn y Blue Chip Expert continúan creciendo, y los grupos profesionales ganan popularidad en sitios que alguna vez fueron personales como Facebook y MySpace, los profesionales de la seguridad integral y la gestión de riesgos deberán enfrentar la realidad de que

estos sitios están surgiendo como fuente de divulgación no autorizada de información corporativa confidencial.

Si bien existen numerosos beneficios para las soluciones de redes sociales, el profesional en seguridad integral debería centrarse en los riesgos de las redes sociales. Al igual que con todas las tecnologías emergentes, las redes sociales avanzan rápidamente y los profesionales de la seguridad deben ser conscientes de los riesgos asociados. Hay una generación que ingresa a la fuerza de trabajo que supone que esta tecnología no solo estará disponible para su uso, sino que también sería esencial para la forma en que se comunican con colegas y socios comerciales. Aunque la utilización de las redes sociales conlleva ventajas internas y externas, la política y la arquitectura para defenderse de los riesgos deben abordarse de manera proactiva y no tomarse a la ligera.

En las transacciones comerciales, la integridad y la confidencialidad son ingredientes clave en la construcción de la confianza mutua. Del mismo modo, para realizar negocios a través de Internet, las empresas deben tener la seguridad de que cualquier información transmitida a través de Internet no será manipulada o robada. Dichos incidentes tendrían un efecto devastador en la credibilidad de todas las transacciones comerciales futuras y, en última instancia, podrían socavar las relaciones comerciales. Por ello, es críticamente importante que las empresas estén equipadas con mecanismos que aseguren la integridad de su información y comunicaciones digitales; este es un requisito absolutamente vital para la promoción y preservación de la confianza dentro de una empresa, así como también entre la compañía, sus clientes y socios comerciales.

Como resultado, el advenimiento de Internet fue rápidamente seguido por un gran interés y preocupación con respecto a la seguridad de la información. El éxito de la seguridad se basaría en la combinación

correcta de personas, procesos, políticas y tecnología de un sistema de gestión de red con la capacidad de razonamiento intelectual, toma de decisiones dinámicas en tiempo real y auto-adaptación y mejoras basadas en la experiencia. Por ende, el diseño de un marco de gestión de redes sociales eficiente, dinámico y automatizado requeriría el apoyo del campo de la IA. Lidiar con la incertidumbre y la inconsistencia ha sido parte de la IA desde sus orígenes; en efecto, las tecnologías para gestionar la incertidumbre y la inconsistencia ya se han utilizado en áreas como los algoritmos de clasificación utilizados en los motores de búsqueda web. La expectativa es que las tecnologías de IA puedan desempeñar un papel igualmente importante en el contexto de las evaluaciones de seguridad.

El campo de la IA involucra el diseño e implementación de sistemas que exhiben capacidades de la mente humana, tales como el razonamiento, el conocimiento, la percepción, la planificación, el aprendizaje y la comunicación. La IA abarca varias subdisciplinas que incluyen aprendizaje automático, satisfacción de restricciones, sistemas de búsqueda y agentes múltiples, razonamiento e ingeniería y procesamiento del lenguaje natural. Las técnicas basadas en los principios de IA como red neuronal, algoritmo genético, sistemas expertos e inferencia difusa, proporcionan habilidades sofisticadas de toma de decisiones inteligente, mejora basada en la experiencia y resolución creativa de problemas. Por consiguiente, su aplicación en aspectos de las métricas de seguridad podría ser beneficiosa, particularmente como un medio para reducir la subjetividad y la participación humana en la realización de evaluaciones de seguridad (Sattikar & Kulkarni, 2012).

La técnica de inteligencia artificial más nueva, como los Procesadores de Lenguaje Natural (PLN), se parece mucho a la forma en que aprenden los cerebros humanos. Además de las operaciones comunes

del procesador de textos que tratan el texto como una mera secuencia de símbolos, los PLN consideran la estructura jerárquica del lenguaje: varias palabras forman una frase, varias frases hacen una oración y, en última instancia, las oraciones transmiten ideas. Al analizar el significado de la lengua, los sistemas de PLN llevan mucho tiempo desempeñando funciones útiles, como corregir la gramática, convertir la voz en texto y traducir automáticamente entre idiomas. Del mismo modo, los PLN que en realidad son una matriz de algoritmos complejos, se pueden usar para detectar correos no deseados, para escanear mensajes de correo electrónico, descubrir el contenido de los mensajes en el cual el correo electrónico sospechoso se envía a un área de cuarentena donde un administrador puede ver el contenido para determinar si lo descarta o lo pasa (Sattikar & Kulkarni, 2012).

Del mismo modo, las técnicas de IA también pueden ayudar a identificar el comportamiento intrusivo, utilizando técnicas de detección de anomalías y de detección de uso indebido. Las redes sociales son excelentes plataformas para aplicar las técnicas de IA. A medida que las redes sociales se hacen cada vez más grandes y las personas las utilizan para compartir más información, las técnicas de IA podrían ser realmente útiles para organizar la información y llevar las piezas más relevantes a los usuarios de una manera completamente personalizada, ayudando además a delinear las categorías básicas de las inquietudes en torno a la privacidad de la información, así como a su protección.

Conclusiones

La historia no necesariamente se repite, pero sí proporciona un valioso contexto y lecciones aprendidas para el futuro de la demanda laboral en un momento de automatización. Entre esas lecciones, la innovación

tecnológica en el pasado ha permitido la creación de nuevos empleos, más de los que ha destruido, aumentando la productividad, estimulando los aumentos sostenidos en los niveles de vida y provocando un cambio en el equilibrio entre el trabajo y el ocio. Sin embargo, la transición no siempre ha sido fluida, por ejemplo, los salarios reales se estancaron durante casi 50 años en la Inglaterra del siglo XIX durante la Revolución Industrial, y solo volvieron a aumentar en un momento de reformas sustanciales de la política social.

Las nuevas tecnologías han aumentado el crecimiento de la productividad, lo que ha permitido a las empresas bajar los precios para los consumidores, pagar salarios más altos o distribuir beneficios entre los accionistas. Esto estimula la demanda en toda la economía, impulsando la creación del empleo. Sin embargo, la revolución industrial de finales del siglo XVII vio la mecanización arrasar a muchas industrias. La agricultura en particular, que representaba alrededor del 50 % de los puestos de trabajo en toda Europa, observó ese porcentaje disminuir a menos del 5 % en la actualidad. Tal trastorno fue indudablemente doloroso para aquellos que no pudieron adaptarse a los nuevos avances, aunque eventualmente surgieron nuevos tipos de empleo.

Más recientemente, hubo cambios sísmicos en la economía global; en los últimos 30 años se ha venido experimentando una transformación digital con el surgimiento de Internet y los avances significativos en la globalización (Álvarez & Zambrano, 2017). Los datos del Banco Mundial muestran que el desempleo global como porcentaje del total de la fuerza de trabajo cayó del 6,1 % en 1991 al 5,8 % en el 2017, a pesar de que la población aumentó de 5,4 mil millones a 7,6 mil millones en el mismo periodo. Por lo tanto, las tecnologías de la cuarta revolución industrial, incluidas la inteligencia artificial y la robótica,

generaron beneficios significativos para los usuarios, las empresas y las economías, elevaron la productividad y el crecimiento económico de los Estados.

La Automatización Robótica de Procesos (ARP) eliminaría la necesidad de que el personal realice actividades aburridas, repetitivas y basadas en reglas, como ingresar datos o manejar la nómina, por lo que la ARP no tendría que conducir a un sacrificio del personal, ya que podría empoderarlos y darle rienda suelta a su creatividad, librándolos de hacer cosas improductivas. En este orden de ideas, las reuniones versarían sobre las ideas, y no tanto sobre mecánica o procesos. Pero incluso los optimistas admiten que a medida que desaparecen los trabajos poco calificados, la gente tendría que aprender nuevas habilidades para compensar. No obstante, el grado en que estas tecnologías desplacen a los trabajadores dependería del ritmo de su desarrollo y adopción, así como del crecimiento económico y del crecimiento de la demanda laboral. Aun cuando la cuarta revolución industrial afectaría algunas ocupaciones, también crearía nuevas ocupaciones que no existen hoy en día, al igual que lo hicieron las tecnologías del pasado. Sin embargo, para el 2030, entre 75 a 375 millones de trabajadores (del 3 % al 14 % de la fuerza laboral mundial) necesitarían cambiar de categoría ocupacional.

Además, todos los trabajadores deberán adaptarse a medida que sus ocupaciones evolucionen junto con máquinas cada vez más capaces; parte de esa adaptación requeriría un mayor logro educativo, o pasar más tiempo en actividades que requieren habilidades sociales y emocionales, creatividad, capacidades cognitivas de alto nivel y otras habilidades relativamente difíciles de automatizar. En consecuencia, para lograr buenos resultados durante la cuarta revolución industrial, los responsables de las políticas públicas y los líderes empresariales

deberán abrazar los beneficios de la automatización y, al mismo tiempo, abordar las transiciones de los trabajadores generadas por estas tecnologías.

Estos cambios desafiarán los modelos actuales de capacitación de la fuerza de trabajo, así como los enfoques comerciales para el desarrollo de habilidades. Otra prioridad sería repensar y fortalecer la transición y el apoyo a los ingresos para los trabajadores atrapados en las corrientes opuestas de la automatización. En total, se exigiría la necesidad de un nuevo tipo de pensamiento y liderazgo que reconozca el desafío de gestionar los nuevos tipos de automatización y su seguridad, así como reconciliar las paradojas y otros fenómenos que han surgido como consecuencia de la cuarta revolución industrial.

Las tecnologías de la información, potencializadas por la cuarta revolución industrial y su amplia adopción en todo el mundo, vienen dando lugar a una serie de nuevos y revolucionarios modelos comerciales para la era moderna. De hecho, las tecnologías de la información están transformando las formas tradicionales de llevar a cabo negocios, reemplazándolos con soluciones que promueven el intercambio eficiente de información entre las partes involucradas y aseguran la satisfacción del cliente. En este orden de ideas, la seguridad de la información debería considerarse como un componente crítico de la seguridad integral de las organizaciones, ya que su función sería establecer la confianza entre organizaciones e individuos, permitiendo que el intercambio de información a través de Internet sea seguro y proporcione a las personas la tranquilidad necesaria para realizar negocios en línea. En este sentido, la seguridad de la información debería verse como un habilitador más que como un inhibidor, tanto para las empresas como para las personas. Es en este contexto que la IA modular podría llegar a jugar un papel fundamental, gracias a su capacidad en el manejo de metadatos y el aprendizaje continuo.

Por último, los Estados Unidos disfrutaron ventajas sustanciales en innovación y fuerza económica en la segunda mitad del siglo pasado. Muchas de las innovaciones en la IA ocurrieron en los Estados Unidos y los beneficios que asisten a estas innovaciones se acumularon primero en ese país. No obstante, estas innovaciones se están difundiendo con rapidez, especialmente con el fuerte impulso académico y comercial para democratizar la IA. El aumento de expertos en IA e innovadores en otras naciones (por ejemplo, China) es probablemente la señal más indicativa que apunta a la pérdida de la ventaja de los Estados Unidos como primer jugador en el terreno de la IA, lo cual tendría, en el mediano y largo plazo, efectos geopolíticos y geoeconómicos considerables.

Referencias

Allen, G., & Chan, T. (2017). *Artificial Intelligence and National Security*. Belfer Center for Science and International Affairs.

Álvarez, C. (2017). Geopolítica vertical y el fenómeno de urbanización de la guerra en el Siglo XXI. *Ensayos en Defensa y Seguridad*, *11*, 8-38.

Álvarez, C., Santafé, J. & Urbano, O. (2017). *Metamorphosis Bellum*: ¿Mutando a guerras de quinta generación? En C. Álvarez (Ed.), *Escenarios y Desafíos de la Seguridad Multidimensional en Colombia* (pp. 145-248).

Álvarez, C., & Zambrano, J. (2017). Globalización desviada: plataforma de convergencia criminal. En C. Álvarez (Ed.), *Escenarios y Desafíos de la Seguridad Multidimensional en Colombia* (pp. 249-307).

Ayoub, K., & Payne, K. (2016). Strategy in the Age of Artificial Intelligence. *Journal of Strategic Studies*, *39*(5-6), 793-819.

Brynjolfsson, E., & McAfee, A. (2014). *The Second Machine Age: Work, Progress, and Prosperity in a time of Brilliant Technologies*. W.W. Norton.

Cipolla, C. (2003). *Before the Industrial Revolution: European Society and Economy from 1000–1700*. W.W. Norton.

Cooper, C., & Kaplinsky, R. (1989). *Technology and Development in the Third Industrial Revolution*. Routledge.

Haegele, M. (2019). *World Robotics 2017 Service Robots.* International Federation of Robotics.

Headrick, D. (2009). *Technology: A World History*. Oxford University Press.

Herrendorf, B., Rogerson, R., & Valentinyi, A. (2014). Growth and Structural Transformation. En P. Aghion & S. Durlauf (Eds.), *Handbook of Economic Growth*, 2, 855-941.

Jensen, G., & Wiest, A. (2001). *War in the Age of Technology: Myriad Faces of Modern Armed Conflict*. New York University Press.

Jörg, B. (2016). *A History of the Global Economy: From 1500 to the Present.* Cambridge University Press.

Kelley, K. (2014, 27 de octubre). *The Three Breakthroughs That Have Finally Unleashed AI on the World*. Wired Magazine. https://www.wired.com/2014/10/future-of-artificial-intelligence.

Keynes, J. (1963). *Essays in Persuasion*. W.W. Norton.

Manyika, J., Lund, S., Chui, M., Bughin, J., Woetzel, J., Batra, P., Ko, P., & Sanghvi, S. (2017). *Jobs Lost, Jobs Gained: Workforce Transitions in a Time of Automation*. McKinsey Global Institute.

Marx, K. (1973). *Grundrisse: Foundations of the Critique of Political Economy*. Vintage Books.

Ricardo, D. (2004). *On the Principles of Political Economy and Taxation*. Dover Publications.

Sattikar, A., & Kulkarni, D. (2012). A Role of Artificial Intelligence Techniques in Security and Privacy Issues of Social Networking. *International Journal of Computer Science Engineering & Technology*, 2(1), 792-795.

Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum.

Søgaard, M., Jørgensen, U. & Clausen, C. (2009). The Social Shaping Approach to Technology Foresight. *Futures, 41*, 80–86.

Singer, P. (2004). *Wired for War: The Robotics Revolution and Conflict in the 21st Century*. Penguin.

Skilton, M., & Hovsepian, F. (2017). *The 4th Industrial Revolution: Responding to the Impact of Artificial Intelligence on Business*. Palgrave Macmillan.

Teng, J. (2014). *Musket, Map and Money: How Military Technology Shaped Geopolitics and Economics*. Versita.

Wittmann, M. (2019). *World Robotics 2019 Industrial Robots*, Frankfurt: International Federation of Robotics.

Zafirovski, M. (2011). *The Enlightenment and Its Efects on Modern Society*. Springer.

Conclusiones

Abordar la discusión sobre una posible interpretación de la seguridad integral implicó la búsqueda de fundamentos teóricos relacionados con el corazón de los problemas del conocimiento de distintas ciencias sociales tales como la ciencia política, la sociología, las relaciones internacionales, la administración y la antropología. Se encontró que, en muchos de los interrogantes y aproximaciones a la noción de seguridad, es posible establecer relaciones concomitantes y algunas de las veces yuxtapuestas entre los distintos ámbitos de estudio. Esta primera conclusión del proceso justifica el enfoque seleccionado por los autores que asumieron el método interpretativo del constructivismo y la hermenéutica como marco de acción en relación con la elaboración de un debate sobre la noción de seguridad.

De la aplicación de estos enfoques y miradas interdisciplinares a la seguridad integral, también resultó posible que esta, como objeto de estudio, fuera relacionada con el contexto contemporáneo que la caracteriza como cambiante y volátil; esto varía la identidad de actores participantes en el fenómeno. Este es un hecho poco reconocido en las interpretaciones clásicas de la seguridad.

A partir de esta visión, fue posible aproximarse a la discusión de situaciones complejas que exigen una interpretación holística frente a los dilemas de la seguridad, y que incluyen realidades como los temas ambientales, la inestabilidad de los nuevos mercados y la relación de la seguridad con la implementación de las innovaciones tecnológicas.

De igual forma, a través de los capítulos fue posible ofrecer propuestas de acción social en torno a los nuevos desafíos de la seguridad que, desde una perspectiva del conocimiento, plantean preguntas y nuevos horizontes para la investigación y avance del estado del arte relacionado.

Siguiendo estos lineamientos, el libro logró explorar el terreno de la seguridad integral desde el ámbito de la gestión en distintos terrenos de estudio, partiendo de una visión regional con la contextualización de los desafíos que se presentan para América Latina, en unos escenarios puntuales que se relacionan con las prácticas empresariales y la toma de decisiones en los nuevos espacios laborales. Resultado de estos artículos, se reconocen desarrollos y prácticas de innovación en gestión del riesgo, así como la reflexión sobre los requerimientos y estándares de implementación de procesos de gestión en seguridad integral que incluyan la dimensión tecnológica y el ámbito humano de las interacciones, para terminar por delimitar las implicaciones que dichos aspectos han tenido sobre el mundo del trabajo.

Por último, el texto se presenta como un esfuerzo de consolidación de distintas visiones que tienen en común la necesidad de construir ámbitos de reflexión conjuntos, así como herramientas de investigación fundadas en el reconocimiento a la diversidad y complejidad de las realidades contemporáneas.

Yuber Rico Venegas
Alejandra Cerón Rincón

Para mayores informes:

Dirección postal | Mailing Address | Endereço postal

Cra. 11 n.º 102-50 Edificio ESDEGUE, Escuadrón de Investigación
Oficina 411. A.A.110111. Bogotá D.C., Colombia
(057-1) 620 6518. Ext. 1700, 1715,1722, 1730
Correo electrónico: cienciaypoderaereo@epfac.edu.co

Biblioteca Escuela de Postgrados
de la Fuerza Aérea Colombiana

Correo electrónico: biblioteca@epfac.edu.co

https://libros.publicacionesfac.com

Enfoques y gestión en Seguridad Integral
fue compuesto en caracteres ConduitITC y Merriweather.
Se terminó de imprimir en Bogotá D. C.,
en noviembre del 2020.

Este libro es el resultado de un proyecto de investigación de la Maestría en Dirección y Gestión de la Seguridad Integral (MADGSI), denominado *Impacto de las políticas de seguridad integral en el desarrollo y gestión del componente de investigación del currículo* MADGSI. Para desplegar las capacidades de profundización y alcance de un proyecto de estas características era necesaria la construcción de un estado del arte consistente e interdisciplinar. La revisión bibliográfica sobre las teorías, las metodologías y las epistemologías presentes en los debates clásicos y contemporáneos sobre la seguridad hizo evidente la necesidad de elaboración conceptual para la exploración de la seguridad integral.

Los capítulos que pertenecen a la primera parte de este escrito recorren discusiones epistemológicas y ontológicas de la seguridad integral a través de la revisión de textos pertenecientes a la sociología, a las relaciones internacionales y a la historia. A través de estas disciplinas, y desde distintos enfoques interpretativos, se hace una evaluación intuitiva de la realidad global actual. La segunda parte contiene estudios de caso de la gestión del riesgo y los procesos de la seguridad empresarial, de la cadena de suministros y de la seguridad del trabajo. Estos trabajos tienen un carácter descriptivo y analítico que abarca los procedimientos de la seguridad y sus vulnerabilidades.

Las reflexiones presentadas en esta investigación son necesarias para la evolución conceptual de la seguridad integral, la cual se postula como una posición viable para concebir los desafíos contemporáneos de la seguridad. El impacto inmediato buscado mediante esta revisión del estado del arte y de algunas gestiones específicas de seguridad no tradicional, es la reflexión sobre los conceptos y teorías enseñadas en los cursos y procesos de posgrados como los de la MADGSI.

COLECCIÓN C&PA

ISBN 978-958-59961-8-2