Revista Científica General José María Córdova, Bogotá, Colombia, enero-junio, 2017
Tecnociencia - Vol. 15, Núm. 19, pp. 269-289
issn 1900-6586

Cómo citar este artículo: González, J. Myer, R. & Pachón, W. (2017, enero-junio). La evaluación de los riesgos antrópicos en la seguridad corporativa: del Análisis Modal de Fallos y Efectos (AMFE) a un modelo de evaluación integral del riesgo. *Rev. Cient. Gen. José María Córdova* 15(19), 269-289. DOI: http://dx.doi.org/10.21830/19006586.81

10

La evaluación de los riesgos antrópicos en la seguridad corporativa: del Análisis Modal de Fallos y Efectos (AMFE) a un modelo de evaluación integral del riesgo*

DOI: http://dx.doi.org/10.21830/19006586.81
Recibido: 24 de agosto de 2016 • Aceptado: 2 de noviembre de 2016

Anthropic Risks Assessment in Corporate Security: From the Failure Mode and Effects Analysis (FMEA) to a Comprehensive Model of Security Risk Assessment

Évaluation des risques anthropiques en matière de sécurité d'entreprise: de l'analyse des effets et des modes de défaillance (FMEA) à un modèle complet d'évaluation des risques pour la sécurité

Avaliação dos Riscos Antrópico em Segurança Corporativa: O Análise dos Modo de Falha e de Efeitos (AMFE) para um Modelo Integral de Avaliação de Risco

Julio César González [a]
Rick Alan Myer [b]
William Pachón Muñoz [c]

* Este artículo científico de reflexión surge de investigaciones adelantadas por el grupo de investigación Sociedad, estrategia y seguridad, en el marco de los proyectos: INV-EES-1558: "Educación superior y post-conflicto en Colombia: proceso de reconstrucción de tejido social basado en el post-conflicto" e INV-EES-2345 "Caracterización de riesgos en los primeros 9 meses de implementación de los acuerdos de paz entre gobierno y la guerrilla de las FARC-EP", financiados por la Universidad Militar Nueva Granada (UMNG), Bogotá, Colombia. Así como también, de las discusiones en gestión del riesgo y seguridad corporativa lideradas por la dirección de posgrados de la Facultad de Relaciones Internacionales, Estrategia y Seguridad de la Universidad Militar Nueva Granada, durante el periodo 2014-2017.

[a] Magíster en Ciencias de la Seguridad y Criminología, Universidad Católica de Murcia. Director de posgrados de la Facultad de Relaciones Internacionales, Estrategia y Seguridad. Docente e investigador de la Universidad Militar Nueva Granada. <julio.gonzalezr@unimilitar.edu.co>

[b] Doctor en Asesoramiento Psicológico de la Universidad de Memphis, Tennessee. Docente de la Universidad de Texas El Paso (UTEP), jefe del Departamento de Psicología Educacional y Servicios Especiales de la Universidad de El Paso, Texas. <ramyer@utep.edu>

[c] Magíster en Análisis de Problemas Políticos, Económicos e Internacionales Contemporáneos, Universidad Externado de Colombia e Instituto de Altos Estudios para el Desarrollo (IAED). Docente e investigador de la Universidad Militar Nueva Granada. <william.pachon@unimilitar.edu.co>

Resumen. El presente artículo plantea la discusión en torno a la aplicación de la metodología Análisis Modal de Fallos y Efectos (AMFE) para la evaluación de los riesgos antrópicos en seguridad corporativa, partiendo de un análisis comparativo entre el riesgo y el delito, desde la perspectiva del *iter criminis*. La hipótesis es que las metodologías actuales para la evaluación del riesgo antrópico son insuficientes, toda vez que no analizan las fases o etapas del riesgo; poniendo en entredicho la efectividad de los resultados. De esta manera, las investigaciones adelantadas en seguridad física corporativa sugieren una necesidad de adaptación del método AMFE a los riesgos antrópicos, proponiendo una nueva herramienta inmersa dentro de los fundamentos de la norma técnica para la gestión del riesgo, publicada por la Organización Internacional para la Estandarización, permitiendo una evaluación integral a las fases del riesgo, con una escala de valores lógica y útil para los gerentes en seguridad corporativa.
Palabras clave: Análisis Modal de Fallos y Efectos; evaluación de riesgos y seguridad corporativa; riesgos antrópicos.

Abstract. This article raises the discussion about the application of the "Failure Mode and Effects Analysis" (FMEA) methodology, in risk assessment for corporate security, based on a comparative analysis between risk and crime from the "Iter Criminis" perspective. The hypothesis to hold is that the risk assessment methodologies, used for the anthropic risk, are not enough; since they don't analyse the stages at which the risk occurs. The results of these methodologies could be questioned about the effectiveness in the risk assessment. Thus, the investigations conducted into corporate physical security, suggests a need for adaptation of FMEA method to anthropic risks, proposing a new tool embedded within the grounds of the technical standard for risk management techniques based on the International Organization for Standardization, allows a comprehensive assessment to the risk phases, with a logical scale value and useful for corporate security managers.
Keywords: Failure Mode and Effects Analysis; risk assessment and corporate security; anthropic risk.

Résumé. Cet article soulève la discussion sur l'application de la méthodologie analyses des modes de défaillance de leurs effets (AMDEC) pour l'évaluation des risques anthropiques dans la sécurité des entreprises, sur la base d'une analyse comparative entre le risque et la criminalité dans la perspective de «iter criminis». L'hypothèse de tenir est que les méthodes actuelles d'évaluation des risques anthropiques sont insuffisants, car ils n'analysent les phases ou étapes du risque; remettre en cause l'efficacité des résultats. Ainsi, les enquêtes menées sur la sécurité physique des entreprises, suggèrent un besoin d'adaptation de la méthode AMDEC risques anthropiques, proposant un nouvel outil intégré dans l'enceinte de la norme technique pour la gestion des risques, publié par l'Organisation internationale pour les normalisations, ce qui permet une approche globale des phases d'évaluation du risque, avec une échelle de logique et utile pour les gestionnaires dans les paramètres de sécurité d'entreprise.
Mots-clés: Analyse des Modes et des Effets de Défaillance; évaluation des risques et sécurité des entreprises; risques anthropiques.

Resumo. Este artigo levanta a discussão sobre a aplicação da metodologia de Análise Modal Falhos e Efeitos (AMFE) para a avaliação de riscos antrópicos em segurança corporativa, com base em uma análise comparativa entre o risco e crime da perspectiva de iter criminis. A hipótese de realizar é que as metodologias atuais para antrópica avaliação de risco são insuficientes, uma vez que não analisar as fases ou etapas de risco; pôr em causa a eficácia dos resultados. Assim, os inquéritos efetuados em segurança física das empresas, sugerem a necessidade de adaptação do método AMFE riscos antrópicos, propondo uma nova ferramenta incorporado dentro do recinto da norma técnica para a gestão de risco, publicado pela Organização Internacional para normalização, permitindo umas fases de avaliação global do risco, com uma escala de lógica e útil para os gestores nas configurações de segurança corporativos.
Palavras chave: Análise Modal Falhos e Efeitos; avaliação de riscos e segurança corporativa; riscos antrópicos.

Introducción

La evaluación de los riesgos antrópicos es un proceso vital para los organismos y departamentos de seguridad estatales y privados, que busca dinamizarse, día a día, con herramientas que permitan anticipar los posibles eventos que amenacen el adecuado funcionamiento o la continuidad de las organizaciones. A esta necesidad, la ISO 31010:2009 (Gestión del riesgo- Técnicas de apreciación del riesgo), propone dentro de su estructura el Análisis Modal de Fallos y Efectos (AMFE) como una de las 31 herramientas de posible uso para la evaluación de los riesgos. Desde esta perspectiva normativa y metodológica, se hace necesario entender la dinámica propia del riesgo antrópico en el contexto de seguridad, a fin de plantear una nueva aplicación del AMFE y poder determinar sus fortalezas respecto a otros tipos de metodologías.

De manera inicial, se realiza una breve revisión de la evaluación de los riesgos antrópicos, haciendo un planteamiento de análisis desde la perspectiva del *iter criminis*, dada la similitud entre la dinámica propia del delito y del riesgo antrópico. Así, se proponen las fases del riesgo antrópico, que permiten un mejor análisis de cada riesgo dentro de su contexto particular.

De esta forma, se analizan de manera comparativa las etapas del riesgo antrópico y las metodologías consecuencia-probabilidad; esta última, una de las más usadas en el sector de la seguridad y la salud ocupacional e incluida también en la norma técnica para la Evaluación del Riesgo (ISO, 2009). A partir de este análisis, se identifica una etapa del riesgo no contemplada en su valoración, de acuerdo con la metodología consecuencia–probabilidad, la cual facilitará posteriores análisis para tratar el riesgo de una forma consecuente a su manifestación, pero de manera anticipada a la generación del daño.

Posteriormente, se realiza una revisión detallada de la metodología del AMFE que permite plantear su posible utilización en un espectro que cubre el riesgo antrópico a un nivel más completo que la metodología consecuencia–probabilidad.

Finalmente, se plantea metodológicamente una alternativa de utilización del AMFE en la evaluación de los riesgos antrópicos, generando un enfoque tridimensional del riesgo antrópico, la cual permite realizar un análisis y tratamiento del riesgo antrópico en cada una de sus etapas de manera integral y promover mejores mecanismos de control.

Generalidades de la evaluación de riesgos antrópicos

La gestión de los riesgos se ha constituido en un proceso fundamental para las diferentes actividades que se desarrollan o ejecutan en los sistemas de seguridad corporativa (Hopkin, 2014), según sea el caso, previniendo la ocurrencia de eventos indeseados. La necesidad de protección, en especial dentro del campo de los riesgos antrópicos, ha promovido el uso cada vez más asiduo y técnico de las diferentes metodologías para la evaluación cuantitativa de los riesgos.

En el campo de la seguridad se tienen una amplia variedad de metodologías para la evaluación de los riesgos antrópicos que en muchos casos son igualmente usadas en otros escenarios de seguridad diferentes a la seguridad física.

Dentro de las metodologías más usadas para la evaluación de los riesgos antrópicos de seguridad, se tienen tres formas de valoración: cualitativa, semicuantitativa y cuantitativa (Bravo & Sánchez, 2012).

La publicación de la norma ISO 31000:2009, definida como Gestión del riesgo– principios y directrices, ha propiciado un marco de referencia importante para el avance en la estandarización en lo relacionado con la gestión del riesgo, aspecto que hasta la fecha presentaba diversos conceptos y metodologías de evaluación, a nivel mundial, dado los diferentes conocimientos científicos y desarrollos de nuevas herramientas técnicas según el campo de aplicación y tipos de riesgos.

De la misma manera, en la ISO 31010:2009 se ilustran varias metodologías para la evaluación del riesgo y se les asigna una valoración según la aplicabilidad. Así, con la norma ISO 31010:2009 se abre un nuevo espectro para los profesionales de la seguridad, quienes buscan implementar herramientas metodológicas que les permitan desarrollar análisis cada vez más integrales en la actividad de la evaluación del riesgo antrópico en la seguridad corporativa; toda vez que, hasta el momento, se han utilizado de forma generalizada en Colombia metodologías como consecuencia-probabilidad y amenazas-vulnerabilidad.

Para proceder al análisis del riesgo, este ha sido dividido en tres categorías (Hopkin, 2014):

1. Los riesgos asociados a las amenazas o riesgos puros.
2. Los riesgos de control o asociados a la incertidumbre.
3. Los riesgos de oportunidad o especulativos.

Así, los riesgos que en el contexto industrial generan mayor interés son, entre otros: catástrofes nucleares, desastre industrial, desorden civil, criminalidad (robo, hurto, fraude, espionaje industrial y secuestro), conflicto de interés (sobornos, divulgación de información privilegiada y prácticas de negocio no éticas) y riesgos misceláneos (Broder & Tucker, 2012). A pesar de la gran cantidad de literatura en riesgos de control y riesgos puros, la profundidad del análisis que ameritan los riesgos de origen antrópico se ha limitado a tratar, de manera general, la evaluación de estos sin profundizar adecuadamente en la dinámica con la cual se manifiestan ni proponer mecanismos propios de valoración adecuados para estos.

Dentro del derecho penal y por la similitud de enfoque, se ofrece una excelente alternativa para entender la infracción penal como una acción humana y de fenómeno social (Lozano, 1979), la cual es la misma génesis para la ocurrencia de un riesgo de origen antrópico. Esta óptica permite generar un claro paralelo entre la acción dañina que conlleva el riesgo antrópico y la acción antijurídica desde la perspectiva del delito.

En virtud de la similitud entre muchos de los riesgos de origen antrópico y el delito,[1] desde la perspectiva del modo como se ejecuta, a pesar de ser conceptos con enfoques diferentes, el significado de delito lleva implícito un agente generador, un agente afectado y una conducta que produjo una lesividad o daño, para lo cual se debe aplicar una pena. En consecuencia, el riesgo antrópico abarca todas las fases anteriores, excepto la parte penal, lo cual se puede apreciar mediante un comparativo de elementos comunes entre delito y riesgo. En la tabla 1 se exponen los elementos frecuentes entre delito y riesgo.

1 "Según Dohna, el delito es la transgresión culpable de las normas" (Jiménez, 2010).

Tabla 1. Comparativo de elementos comunes entre delito y riesgo

Delito	Riesgo
Delincuente (sujeto activo)	Agente generador
Bien material o jurídico	Sistema o agente afectado
Antijuridicidad material (acción lesiva o daño)	Pérdida potencial o real

Fuente: Diseño propio

Con base en los elementos anteriores, se aprecia la similitud entre los componentes del delito y riesgo, de tal manera que es procedente entender la dinámica delictiva como un proceso criminal o *iter criminis*, con el fin de aplicarlo de forma paralela a las fases del riesgo. El *iter criminis*, como proceso o desarrollo de un hecho punible, tiene cuatro fases: ideación, preparación, ejecución y consumación (Bernate, 2008).

Dentro de la dinámica del riesgo, las fases se pueden relacionar así: ideativa, que se puede equiparar con la fase de motivación (o manifestación del pensamiento) del agente generador del riesgo; la segunda fase del *iter criminis*, o fase preparativa, es equiparable con la fase de validación de las vulnerabilidades para ejecutar la acción dañina; la tercera fase, o ejecución del delito, se puede equiparar con la manifestación del riesgo, y la etapa de consumación es equiparable con la manifestación del daño.

El paralelo que se plantea entre el *iter criminis*, cuyo enfoque es la determinación de una conducta punible y el riesgo como situación de posible ocurrencia con situaciones adversas (O'Byrne, 2008, pp. 30-39), permite definir, analógicamente, las acciones que se llevan a cabo en las fases de manifestación del riesgo (tabla 2).

Tabla 2. Propuesta para definir las fases o etapas del riesgo

Fase *iter criminis*	Fase del riesgo
Ideación: surge la idea criminal en la mente del delincuente (Córdoba, 1993).	Fase de motivación y capacidad del agente generador: en esta fase el agente desarrolla la motivación para ejecutar la acción dañina.
Actos preparatorios: conductas materializadas o no para poner en peligro el bien jurídico protegido (Castro, 2009, pp. 97-132).	Fase de identificación de vulnerabilidades: el agente potencial, generador del riesgo, identifica las condiciones que le permitirán o le dificultarán ejecutar la acción dañina y racionaliza los recursos y actividades para tal fin.
Ejecución: el agente emplea los medios elegidos para realizar el plan (Zambrano, 2012)	Manifestación del riesgo: se lleva a cabo la acción que puede llevar a que el daño se materialice.
Consumación: se realiza el verbo rector del tipo penal, poniendo en peligro el bien jurídico protegido (Salas, 2007).	Manifestación del daño: Luego de manifestarse, el riesgo genera un daño con tal impacto negativo, que su mitigación representa una gran dificultad.

Fuente: Diseño propio

En el enfoque anterior, se evidencia cómo dos conceptos se relacionan estrechamente y permiten darle al riesgo antrópico una perspectiva de proceso, para analizar la aplicación de las diferentes metodologías de la evaluación del riesgo.

Generalidades de las herramientas metodológicas en la evaluación de los riesgos

Las diferentes metodologías y herramientas para la evaluación del riesgo, si son aplicadas sistemática y apropiadamente, pueden advertir las distintas vulnerabilidades de un sistema (Ostrom & Wilhelmsen, 2012). No obstante, para los riesgos antrópicos se han utilizado algunas metodologías para la evaluación del riesgo, unas incluidas en la norma estandarizada para la valoración del riesgo (ISO, 2009); otras por fuera de dicho estándar. Muchos de los modelos o metodologías existentes para el análisis y evaluación de los riesgos han alcanzado extraordinaria complejidad y rigor mediante el empleo de la ciencia matemática, mientras que otros son de extraordinaria sencillez y aplicabilidad en el mundo de la seguridad (Valero & Cruz, 2002).

Por esto último es procedente la descripción de un evento de manifestación del riesgo en dos formas: en términos del daño que genera cuando sucede y en términos de probabilidad de ocurrencia (Broder & Tucker, 2012).

La metodología de la ASIS International (por sus siglas en inglés; American Society for Industrial Security), denominada General Security Risk Assessment Guideline, define claramente que esta es aplicable en ambientes donde los bienes y personas estén en riesgo por incidentes asociados con la seguridad (ASIS International, 2003). Esta guía de ASIS contempla dos variables para la evaluación cuantitativa del riesgo, como son: la frecuencia o probabilidad y la criticidad del evento de pérdida.

De manera muy similar a la guía de ASIS, el estándar australiano para la gestión del riesgo AS NZS 4360:2004 (previo a la ISO 31000:2009) planteaba en su numeral 3.4.3 la utilización de la consecuencia y la probabilidad para analizar los riesgos (Australian/New Zealand Standard [AS/NZS], 2004).

Asimismo, y no menos importante en el uso específico para riesgos antrópicos antisociales, se tiene la metodología de Mossler, cuya finalidad es identificar, analizar y evaluar las amenazas y los factores que tienen influencia en su manifestación a partir de la valoración de sus variables: función, sustitución, profundidad, extensión, agresión y vulnerabilidad (Valero & Cruz, 2002).

De las anteriores metodologías, es importante asociar las normas para la evaluación del riesgo, tanto de la General Security Risk Assessment Guideline (2003), como de la ASIS y el estándar AS/NZS 4360 (2004), las cuales cumplen con los requisitos metodológicos utilizados en la matriz consecuencia-probabilidad, expuesta en la norma ISO 31010:2009.

Esta metodología permite conocer el valor del riesgo a partir del producto de las dos variables (probabilidad por consecuencia), de manera que es prioritario establecer o valorar la consecuencia y posteriormente la probabilidad (IEC 60812, 2006).

A pesar de que la metodología ISO 31010:2009 presenta una alta aplicabilidad en el análisis y evaluación de los riesgos asociados a conductas antrópicas antisociales, se hace necesario pro-

fundizar el análisis del riesgo hacia las fases de: motivación-capacidad, identificación de vulnerabilidades, manifestación del riesgo y manifestación del daño.

En este sentido, la variable probabilidad se asocia directamente con las fases de motivación-capacidad e identificación de vulnerabilidades, entendiendo que para que exista el riesgo antrópico deben estar de forma manifiesta el agente generador de la amenaza y la vulnerabilidad. Por su parte, la evaluación de la variable consecuencia está asociada con la fase de manifestación del daño, es decir, cuando el sistema afectable ha sufrido la pérdida (figura 1).

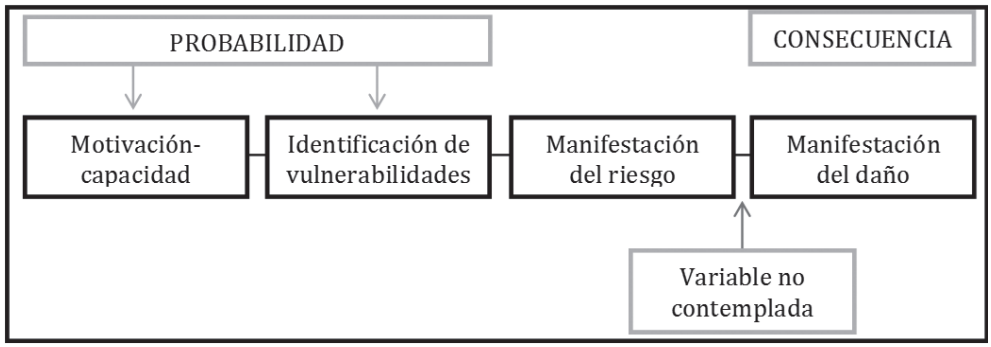

Figura 1. Interacción de la metodología consecuencia-probabilidad con la dinámica de los riesgos antrópicos antisociales.
Fuente: Diseño propio

Este planteamiento deja en evidencia el vacío sobre la fase de manifestación del riesgo, ya que el hecho de que esta exista, no necesariamente implica que haya un daño sobre el sistema vulnerado. De este modo, vale precisar que un sistema de seguridad puede tener la capacidad de detectar un riesgo durante su manifestación y generar una reacción que permita neutralizar la amenaza y evitar la manifestación del daño o pérdida.

Es así como dentro del mismo contexto de la norma ISO 31010:2009 se identifica la metodología Análisis Modal de Fallos y Efectos (AMFE), con la cual se pueden desarrollar análisis y evaluaciones del riesgo más holísticas que hacen posible el diseño de sistemas de seguridad eficaces, orientados al tratamiento integral del riesgo corporativo.

El Análisis Modal de Fallos y Efectos (AMFE)

El Análisis Modal de Fallos y Efectos es una herramienta de gran utilidad y valor, que permite identificar las variables significativas de un producto o proceso para poder determinar y priorizar los riesgos (Ghantt, 2012).

Como se mencionó, dentro de las categorías del riesgo están los puros, los especulativos y los de control (Hopkin, 2014). En especial, para los riesgos puros (asociados a la amenaza) y los de control (asociados a la incertidumbre), los posibles eventos negativos se pueden denominar como riesgos o fallos, teniendo en cuenta que la manifestación de cualquiera de estos se asocia a una posibilidad y un daño o pérdida.

Asimismo, la norma ISO 31010:2009 contempla la metodología de Análisis Modal de Fallos y Efectos (más conocida como AMFE), la cual se califica en términos de «Muy Aplicable» (por sus siglas: MA) para las siguientes actividades:

- Identificación del riesgo.
- Análisis del riesgo (consecuencia, probabilidad y nivel de riesgo).
- Evaluación del riesgo.

Esto refiere que la metodología AMFE puede ser utilizada de manera satisfactoria en las mencionadas actividades involucradas con la gestión del riesgo. Es de importancia enunciar que esta herramienta metodológica no ha sido utilizada comúnmente en la seguridad física, dado que su diseño inicial se centró en el significado cuantitativo de las variables, principalmente en la industria aeroespacial militar y, posteriormente, en procesos de la industria automotriz (Cuatrecasas Arbos, 2010), de tal manera que resulta interesante implementarlo en el campo de la seguridad física.

Como se ve, el AMFE puede constituirse en una novedosa herramienta que permita evaluar los riesgos puros que gravitan el contexto empresarial, dentro del espectro de la seguridad, si se conocen y adaptan de forma satisfactoria sus variables dentro de la dinámica de los diferentes riesgos que pueden presentarse en este campo.

La metodología AMFE consta de cuatro etapas: establecimiento de reglas fundamentales, ejecución del AMFE, resumen y reporte del análisis, y actualización del AMFE. Para utilizar el AMFE, un factor fundamental es identificar el ambiente que constituye el sistema; esto, en términos de la ISO 31000:2009, correspondería al contexto. En lo sucesivo, el AMFE permite identificar el modo en que los fallos o riesgos se podrían generar, sus causas, efectos o consecuencias y los mecanismos de detección (IEC 60812, 2006).

El AMFE presenta tres tipos principales de utilización: AMFE de sistema, AMFE de procesos y AMFE de diseño, los cuales permiten identificar las fases del riesgo a partir de la estructuración por variables planteada por Carlson (2012) (tabla 3).

Tabla 3. Propuesta para analizar las variables del riesgo según metodología AMFE

Ítem	Función	Modo Potencial de Fallo	Potencial Efecto de Fallo	Severidad (S)	Causa Potencial de Fallo	Ocurrencia (O)	Controles Actuales Preventivos	Controles Actuales Detectivos	Detección (D)	NPR	Acciones Recomendadas

Fuente: Effective FMEAs (Carlson, 2012)

Las variables que requieren una medición en el uso del AMFE son la severidad *(S)*, la ocurrencia *(O)* y la detección *(D)*, cuyo producto permite obtener el número de prioridad del riesgo *(NPR)*.

$$NPR = S * O * D$$

En donde

S: Número no dimensional que representa la severidad.

O: Denota la probabilidad de ocurrencia, interpretada como un número de clasificación y no de probabilidad real.

D: Significa detección, es decir, un estimado de la oportunidad de identificar y eliminar la falla antes de que se vea afectado el sistema.

Así, a manera de ejemplo, en el caso de la industria automotriz, el NPR se obtiene mediante la valoración de las variables anteriores, en concordancia con los criterios de severidad, ocurrencia y detección del riego, dispuestos en la norma técnica colombiana NTC-IEC 60812 (tablas 4, 5 y 6) (ICONTEC Internacional, 2007).

Tabla 4. Criterios de evaluación de la severidad

No.	SEVERIDAD
01	**Ninguna:** No hay efecto discernible.
02	**Muy menor**: Ajuste y terminado/Chirrido y traqueteo. Ítem no cumple. Defecto observado por los clientes perceptivos (menos del 25 %).
03	**Menor**: Ajuste y terminado/Chirrido y traqueteo. Ítem no cumple. Defecto observado por el 50 % de los clientes.
04	**Muy baja:** El ajuste y terminado/Chirrido y traqueteo. Ítem no cumple. Defecto observado por la mayoría de los clientes (más del 75 %).
05	**Baja:** Vehículo/ítem operable pero ítem(es) de confort/convivencia operable(s) a un nivel de desempeño reducido. Cliente un poco insatisfecho.
06	**Moderada:** Vehículo/ítem operable pero ítem(es) de confort/convivencia operable(s) a un nivel de desempeño reducido. Cliente insatisfecho.
07	**Alta:** Vehículo/ítem operable, pero a un nivel de desempeño reducido. Cliente muy insatisfecho.
08	**Muy alta:** Vehículo/ítem inoperable (pérdida de la función primaria).
09	**Peligrosa con advertencia:** Clasificación de severidad muy alta cuando un modo de falla potencial afecta la operación segura del vehículo y/o implica no conformidad con las reglamentaciones gubernamentales con advertencia.
10	**Peligrosa sin advertencia:** Clasificación de severidad muy alta cuando un modo de falla potencial afecta la operación segura del vehículo y/o implica no conformidad con las reglamentaciones gubernamentales con advertencia.

Fuente: Técnicas de análisis para la confiabilidad de sistemas. Procedimiento para análisis de modo de falla y efectos (AMFE) (ICONTEC Internacional, 2007)

Tabla 5. Criterios de evaluación de la ocurrencia

No.	Ocurrencia
01	**Remota:** La falla es improbable: <=0.010 por mil vehículos/ítems.
02	**Baja:** Relativamente pocas fallas: 0.1 por mil vehículos/ítems.
03	**Baja:** Relativamente pocas fallas: 0.5 por mil vehículos/ítems.
04	**Moderada:** Fallas ocasionales: 1 por mil vehículos/ítems.
05	**Moderada:** Fallas ocasionales: 2 por mil vehículos/ítems.
06	**Moderada:** Fallas ocasionales: 5 por mil vehículos/ítems.
07	**Alta:** Fallas repetidas: 10 por mil vehículos/ítems.
08	**Alta:** Fallas repetidas: 20 por mil vehículos/ítems.
09	**Muy alta:** La falla es casi inevitable: 50 por mil vehículos/ítems.
10	**Muy alta:** La falla es casi inevitable: 100 por mil vehículos/ítems.

Fuente: Técnicas de análisis para la confiabilidad de sistemas. Procedimiento para análisis de modo de falla y efectos (AMFE) (ICONTEC Internacional, 2007)

Tabla 6. Criterios de evaluación de la detección

No.	Detección
01	**Casi segura:** El control del diseño casi sin falta detectará una causa/mecanismo potencial del modo de falla subsiguiente.
02	**Muy alta:** Una oportunidad muy alta de que el control del diseño detecte una causa/mecanismo potencial del modo de falla subsiguiente.
03	**Alta:** Una oportunidad alta de que el control del diseño detecte una causa/mecanismo potencial del modo de falla subsiguiente.
04	**Moderadamente alta:** Una oportunidad moderadamente alta de que el control del diseño detecte una causa/mecanismo potencial del modo de falla subsiguiente.
05	**Moderada:** Una oportunidad moderada de que el control del diseño detecte una causa/mecanismo potencial el modo de falla subsiguiente.
06	**Baja:** Una oportunidad baja de que el control del diseño detecte una causa/mecanismo potencial del modo de falla subsiguiente.
07	**Muy baja:** Una oportunidad muy baja de que el control del diseño detecte una causa/mecanismo potencial del modo de falla subsiguiente.

Continúa tabla...

No.	Detección
08	**Remota:** Una oportunidad remotamente alta de que el control del diseño detecte una causa/mecanismo potencial del modo de falla subsiguiente.
09	**Muy remota:** Una oportunidad muy remota de que el control del diseño detecte una causa/mecanismo potencial del modo de falla subsiguiente.
10	**Peligrosa sin advertencia:** Clasificación de severidad muy alta cuando un modo de falla potencial afecta la operación segura del vehículo y/o implica no conformidad con las reglamentaciones gubernamentales con advertencia.

Fuente: Técnicas de análisis para la confiabilidad de sistemas. Procedimiento para análisis de modo de falla y efectos (AMFE) (ICONTEC Internacional, 2007)

Si bien lo apreciado determina los rangos de evaluación de variables pensadas principalmente para la industria automotriz, la aplicación del AMFE resulta pertinente para valorar los riesgos en la industria en general, así como también en los demás sectores económicos de un país (Cauwenbergh, 2012).

La aplicación de la metodología AMFE en la dinámica de los riesgos antrópicos

Al observar las dinámicas de manifestación del riesgo antrópico, en paralelo con la dinámica del delito, se encuentra similitud en las siguientes cuatro fases: motivación-capacidad, identificación de vulnerabilidades, manifestación del riesgo y manifestación del daño; sin embargo, al momento de evaluar el riesgo se evidencia un vacío metodológico entre las dos últimas fases.

Para la protección de la infraestructura crítica, el ciclo del riesgo se identifica desde las siguientes etapas: peligro, amenaza, fallo y daño (Scurek, 2011, pp. 1-11). En estas etapas aplicables a la infraestructura crítica, la manifestación de un riesgo no necesariamente conlleva una pérdida vinculante con el evento, toda vez que el sistema de seguridad puede tener la capacidad de detectar y neutralizar el evento de manifestación del riesgo, previo a la manifestación del daño.

La detección en un sistema de seguridad puede efectuarse a través de diferentes medios, como: alarmas, observación directa y circuito cerrado de televisión (CCTV), lo cual hace posible la detección incluso después de que el acto criminal se ha manifestado (Talbot & Jakeman, 2009). Podrían darse casos de riesgos en donde las fases de manifestación y daño ocurriesen de manera paralela, como sucede, por ejemplo, en los casos de terrorismo: en el evento del 11 de septiembre, la manifestación del riesgo fue la colisión de las aeronaves con los edificios del World Trade Center, que a su vez generó un daño inmediato en las estructuras que posteriormente colapsarían. En ese orden de ideas, la dinámica del riesgo determinada anteriormente podría definirse entonces y analizarse de manera análoga mediante la metodología de Análisis Modal de Fallos y Efectos (AMFE) de acuerdo con el esquema descrito en la figura 2.

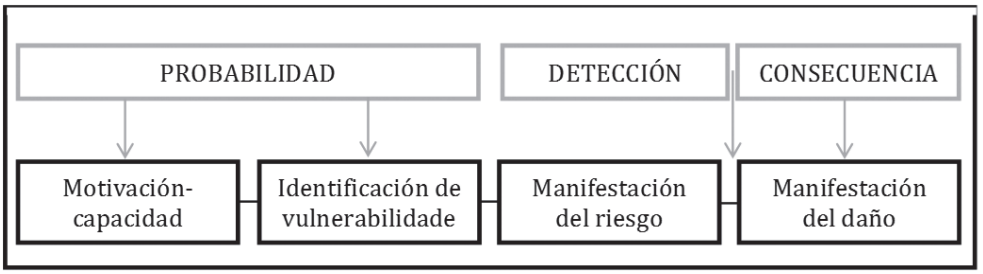

Figura 2. Análisis del riesgo antrópico (antisocial) desde la perspectiva del AMFE
Fuente: Diseño propio

El detalle de la dinámica del riesgo evidenciado en la figura anterior permite plantear que las medidas para el tratamiento del riesgo no son únicamente las orientadas a la prevención, sino que también son aquellas que habilitan su detección después de que se han manifestado. Como ejemplo del planteamiento anterior se puede tomar el riesgo de lavado de activos, descrito en su dinámica en la tabla 7.

Tabla 7. Ejemplo de la dinámica del riesgo en situación y sistema de protección, análisis de un caso particular

Dinámica del riesgo de lavado de activos	Situación presentada	Sistema de protección
Motivación-capacidad	Económica.	N/A.
Identificación de vulnerabilidades	Ausencia de medidas de *Due Diligence* para identificar a clientes.	Implementación de debida diligencia para identificar adecuadamente los clientes y proveedores dentro de un sistema de prevención del riesgo de lavado de activos.
Manifestación del riesgo	Pago de contado de mercancía en altos volúmenes.	Clasificación e interrupción de operaciones sospechosas.
Manifestación del daño	Despacho de la mercancía y cierre de la transacción.	Controles correctivos: Investigaciones y acciones de mejora

Fuente: Diseño propio

Entendiendo la dinámica propia del riesgo antrópico, es viable utilizar la metodología AMFE a este tipo de riesgos, empleando los parámetros de análisis y evaluación de las variables planteadas en la tabla 3, propuesta por Carlson (2012): severidad, ocurrencia y detección.

Es así que para iniciar con la aproximación del AMFE en lo que respecta a los riesgos antrópicos, resulta importante interpretar cada columna de la herramienta metodológica AMFE. En este sentido, la columna ítem (tabla 3) corresponde a cualquier parte, componente, dispositivo, subsistema, unidad funcional equipo o sistema que se puede considerar individualmente, de manera que solo es necesaria en el caso en que se aplique el AMFE a productos o elementos de seguridad (ICONTEC Internacional, 2007).

En el mismo orden, la columna función puede ser asimilada como su sistema de seguridad general o el proceso organizacional que quiere evaluar su dinámica frente a diferentes riesgos antrópicos (Reyes, 2004). La columna de modo potencial de fallo incluye el modo o formas potenciales en los cuales el ítem descrito en la función podría fallar. De manera analógica, en seguridad, este modo de fallo potencial podría representar el riesgo y el modo en que este se podría manifestar sobre la función (Mollah, 2005, pp. 12-20).

La columna causa potencial de fallo está constituida por el indicio de una debilidad del diseño, cuya consecuencia es el propio modo del fallo (Ministerio de Trabajo y Asuntos Sociales de España - Instituto Nacional de Seguridad e Higiene en el Trabajo, 2004), lo que en términos de vulnerabilidad corresponde a aquellas condiciones de inseguridad (Cardona A., 2003, pp. 1-18).

Cabe anotar que en cuanto a la interpretación de las variables cuantitativas del AMFE (severidad, ocurrencia y gravedad), como en el esquema de la NTC IEC 60812 las definiciones se ajustan a productos de la industria automotriz, se hace necesario interpretar la norma a la dinámica de los riesgos antrópicos para aplicarla.

Así, los ajustes a los criterios que permiten evaluar la severidad de los riesgos antrópicos se plantean en la tabla 8.

Tabla 8. Definición de los niveles de la severidad para los riesgos antrópicos

Clasificación	Severidad	Criterio
01	**Ninguna**	Sin daños perceptibles en el corto, mediano y largo plazo en la organización o el sistema afectable.
02	**Muy menor**	Los daños o pérdidas generados por la manifestación del riesgo son difícilmente perceptibles, sin embargo no generan afectación al sistema.
03	**Menor**	Los daños y pérdidas generados por la manifestación del riesgo son perceptibles. Pueden ser cargadas a los gastos normales del sistema (ASIS, 2003).
04	**Baja**	Los daños y pérdidas generados por la manifestación del riesgo son identificables y cuantificables. Pérdidas financieras bajas, sin embargo amerita control para evitar que la frecuencia genere mayor severidad.
05	**Moderada**	Los daños y pérdidas generados por la manifestación del riesgo ocasionan impacto financiero mediano (ICONTEC, 2004). En las personas producen lesiones personales con incapacidad corta. Procesos con afectaciones parciales, sin interrupción.
06	**Media**	Los daños y pérdidas generados por la manifestación del riesgo ocasionan pérdidas altas a las finanzas corporativas, aplazando el cumplimiento de los objetivos corporativos. En las personas producen lesiones personales con incapacidad considerable. En los procesos generan la interrupción parcial del funcionamiento. Baja afectación de la imagen-reputación.

Continúa tabla...

Clasificación	Severidad	Criterio
07	**Alta**	Los daños y pérdidas generados por la manifestación del riesgo ocasionan pérdidas muy altas que conllevan aplazamiento del cumplimiento de los objetivos y medidas de recorte de gastos para subsanarla. En las personas producen lesiones personales con incapacidad considerable y afectación psicológica. En los procesos generan la interrupción temporal del funcionamiento. Baja afectación de la imagen-reputación.
08	**Muy alta**	Los daños y pérdidas generados por la manifestación del riesgo ocasionan pérdidas de alto impacto que conllevan aplazamiento del cumplimiento de los objetivos estratégicos y medidas de recorte de gastos y créditos para subsanar la pérdida. En las personas producen lesiones personales graves con incapacidad temporal, afectación permanente y afectación psicológica. En los procesos generan la interrupción temporal del funcionamiento, media afectación de la imagen-reputación.
09	**Crítica**	Los daños y pérdidas generados por la manifestación del riesgo ocasionan pérdidas críticas que conllevan aplazamiento del cumplimiento de los objetivos estratégicos e interrupciones permanentes de no tratarse adecuadamente. Necesidad de recapitalización (ASIS, 2003) para manejar la crisis. En las personas producen lesiones personales graves con posibilidad de muerte. En los procesos generan la interrupción permanente del funcionamiento y afectación de la imagen-reputación.
10	**Catastrófica**	Los daños y pérdidas generados por la manifestación del riesgo ocasionan pérdidas no subsanables, con pérdida de continuidad del negocio permanente. En las personas producen la muerte. En los procesos generan la cancelación del funcionamiento y afectación grave de la imagen-reputación.

Fuente: Diseño propio

Por su parte, si bien la ocurrencia o probabilidad se evalúa usualmente con base en información histórica de eventos pasados, en la actualidad se requiere desarrollar la capacidad de prevención de eventos y crisis futuras (Mitroff & Anagnos, 2005).

Por lo anterior, la catalogación de la frecuencia basada en eventos ocurridos genera una dependencia de la información histórica que disminuye la capacidad de analizar las vulnerabilidades que producen un ambiente óptimo para la manifestación de los riesgos. El análisis debe hacerse con base en la historia y en la proyección o perspectiva futura. El planteamiento realizado en la tabla 9 orienta la utilización de eventos históricos sin desconocer la posibilidad de ocurrencia de eventos desconocidos.

Tabla 9. Definición de los niveles de ocurrencia o probabilidad

Clasificación	Ocurrencia o probabilidad	Criterio
01	**Improbable**	No se ha presentado evento y las condiciones actuales dificultan que el evento se pudiese manifestar.
02	**Remota**	No se ha presentado el evento, sin embargo el sistema de seguridad excede la capacidad de la amenaza para reducir las vulnerabilidades.
03	**Muy baja**	No se ha presentado el evento. El sistema de seguridad se considera efectivo para la protección.
04	**Baja**	No se ha presentado el evento, sin embargo el sistema de seguridad, en las circunstancias actuales, pudiese fallar y generar la manifestación del riesgo.
05	**Moderada**	Se desconoce si se ha presentado, sin embargo en las circunstancias actuales el sistema de seguridad frente al riesgo es insuficiente y presenta fallas.
06	**Media**	Podría presentarse el evento. Las condiciones de seguridad son inexistentes.
07	**Alta**	Las condiciones de ocurrencia están dadas para que el evento suceda en cualquier momento puede haber ocurrido con anterioridad.
08	**Muy alta**	El evento puede estarse presentando, las condiciones están dadas para que ocurra. El sistema es vulnerable.
09	**Frecuente**	El evento se presenta esporádicamente en el mes y el sistema de seguridad es insuficiente para evitarlo. El sistema es bastante vulnerable.
10	**Permanente**	El evento se presenta frecuentemente y puede suceder a diario o varias veces en el mes.

Fuente: Diseño propio

Finalmente, se tiene la fase de la detección, que corresponde a la probabilidad de descubrir el fallo o riesgo a través de los controles (Safety and Reliability Society, 2011).

En seguridad, la detección es el descubrimiento de un ataque por parte de un adversario que se desarrolla en una línea de tiempo, en la cual se produce la detección, evaluación de la amenaza, intercepción y neutralización del adversario (Rogers, 2006). Por eso, los riesgos antrópicos pueden ser detectados de manera posterior a su manifestación, antes de que el daño sea producido.

Como se observó en la figura 2, la manifestación del riesgo no necesariamente implica la generación del daño inmediato, sino que en muchos casos es viable que el sistema esté diseñado para detectar y recuperar el activo crítico. En otros riesgos, como el lavado de activos, también se considera la capacidad de identificar y reportar a las autoridades (Financial Action Task Force [FATF], 2013).

Por lo anterior, se pueden fortalecer los sistemas de protección en la fase de detección como alternativa paralela a la detección previa, a pesar de que el riesgo se haya manifestado; sin embar-

go, la evaluación de la detección no solo se debe medir por su efectividad en la detección, sino que, además, debe estar implícita la capacidad de neutralización para evitar la manifestación del daño. A continuación, se plantea la interpretación de la variable detección (tabla 10).

Tabla 10. Definición de los rangos de detectabilidad

Clasificación	Detección	Criterio
01	**Casi segura**	El control del sistema de seguridad, casi sin falta, detectará la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización superior al 95 %.
02	**Muy alta**	Una oportunidad muy alta de que el sistema de seguridad detecte la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización cercana al 90 %.
03	**Alta**	Una oportunidad alta de que el sistema de seguridad detecte la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización cercana al 80 %.
04	**Moderadamente alta**	Una oportunidad moderadamente alta de que el sistema de seguridad detecte la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización cercana al 70 %.
05	**Moderada**	Una oportunidad moderada de que el sistema de seguridad detecte la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización cercana al 60 %.
06	**Baja**	Una oportunidad baja de que el sistema de seguridad detecte la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización cercana al 50 %.
07	**Muy baja**	Una oportunidad muy baja de que el sistema de seguridad detecte la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización cercana al 40 %.
08	**Remota**	Una oportunidad remotamente alta de que el sistema de seguridad detecte la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización cercana al 30 %.
09	**Muy remota**	Una oportunidad muy remota de que el sistema de seguridad detecte la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización cercana al 20 %.
10	**Absolutamente incierta**	El control del diseño no detectará y no puede detectar la ocurrencia o manifestación de un riesgo. Capacidad de detección y neutralización nula o inferior al 10 %.

Fuente: Diseño propio

Existen riesgos, que, dada su dinámica, podrían no ser susceptibles de ser detectados y neutralizados una vez se han manifestado. Un claro ejemplo es el ataque terrorista generado o perpetrado desde una posición lejana a la instalación o sistema afectable, puesto que una vez se manifiesta

el riesgo, para este caso el ataque, muy difícilmente podría darse la detección y neutralización del mismo.

Las tres variables cuantitativas vistas (severidad, ocurrencia y detección), medidas en escala de uno a diez, permiten obtener como producto de la multiplicación en una escala jerárquica de uno (1) a mil (1.000) el índice o número de prioridad del riesgo (NPR). Así, y dando continuidad a la exposición de las variables que componen el AMFE, como se presentó en la Tabla 3, se procede a definir los controles actuales preventivos, los controles actuales detectivos y las acciones recomendadas.

Los controles actuales preventivos. "En este apartado se deben reflejar todos los controles existentes actualmente para prevenir las causas del fallo y detectar el efecto resultante" (INSHT, 2004, p. 4). Los controles preventivos "corresponden a la primera barrera del sistema de seguridad que se establece para reducir los riesgos. Los que sobrepasen esta línea deben ser tratados por los otros tipos de controles" (Mejía, 2006). Esta columna debe concentrar la información inherente a los elementos de retardo y detección de la amenaza del sistema de seguridad, que el resultado sea la prevención de la manifestación del riesgo.

Los controles actuales detectivos. Estos controles incluyen la capacidad en términos de probabilidad de detectar y aislar una falla o riesgo que ha sucedido (ICONTEC Internacional, 2007). En términos de seguridad física, se puede definir la capacidad que tiene el sistema de protección para detectar y neutralizar el riesgo manifestado antes de que genere el daño, como se observó en el análisis en la variable cuantitativa detectabilidad.

Con base en el resultado NPR del producto de las variables: severidad, ocurrencia (o mejor interpretado como probabilidad para seguridad) y detección, se genera un resultado cuantitativo que permite conocer el nivel de prioridad del riesgo frente a los demás.

Acciones recomendadas. Finalmente, la última columna de la matriz del Análisis Modal de Fallos y Efectos (AMFE) incluye las recomendaciones para reducir el nivel de prioridad del riesgo (NPR), desde la reducción de cualquiera de las variables: severidad, ocurrencia (o probabilidad) y detectabilidad. En la escala de 1 a 1.000, en donde se catalogan las zonas de confort, cautela, preocupación y criticidad de la organización dependiendo de la característica del riesgo (si es adverso o tolerante al riesgo) (Hopkin, 2014).

Algunos usos del AMFE diferencian adicionalmente el nivel de detección de fallas, en cuanto a seguridad. La aplicación del AMFE, dependiendo de la dinámica propia de cada riesgo, podría o no incluir la variable de detección de fallas. En este caso, si el riesgo no tuviese la propiedad de tener una clara diferenciación en la línea de tiempo entre la manifestación del riesgo y el daño, es conveniente usar el AMFE, mediante esta fórmula:

$$R = S \times P$$

En donde

S: es un número que representa la severidad, es decir, qué tanto las fallas afectarán al sistema (ICONTEC Internacional, 2007).

P: es un número que denota la probabilidad de ocurrencia del riesgo y, por ende, el efecto de la falla (ICONTEC Internacional, 2007).

Lo expresado anteriormente implica que algunos escenarios de riesgo pudiesen tener un análisis bidimensional (es decir, que en términos de las dos variables el resultado máximo sería de 100) y en otros escenarios, un análisis tridimensional, dado que no todos los riesgos diferencian entre la fase de manifestación y la del daño. En la figura 3, se pueden observar las variables que generan un elemento tridimensional para el análisis y evaluación de riesgos.

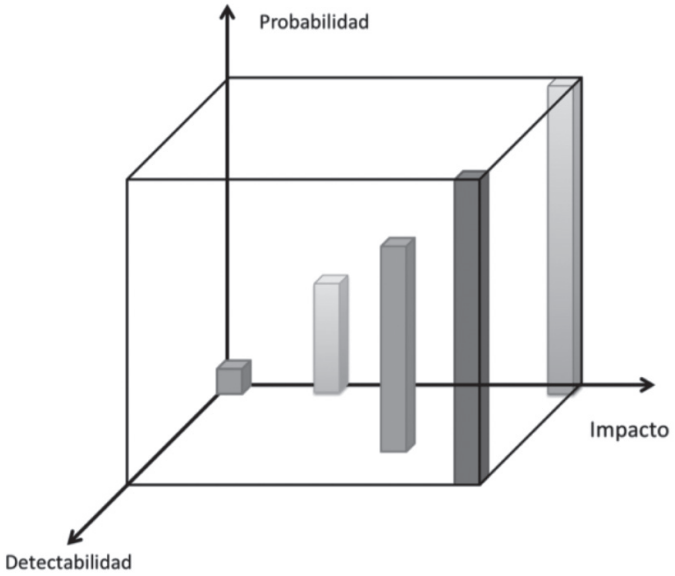

Figura 3. Perspectiva de riesgos en tres variables
Fuente: Diseño propio

A pesar de la viabilidad de poder producir una escala de resultados para entender el nivel de prioridad del riesgo (NPR), hay una dificultad interpretativa: el apetito al riesgo depende de lo que la organización defina (Hopkin, 2014). Por ejemplo, un riesgo que indique un NPR equivalente a 125 (evaluado en escala de tres variables cada una en un rango de 5) podría ubicarse dentro de una clasificación de riesgo bajo, moderado o incluso alto, dependiendo del apetito al riesgo de la organización.

Análisis de la utilización de la metodología AMFE en la seguridad corporativa

Acotada la aproximación de la metodología AMFE al análisis de los riesgos antrópicos, se expanden los conceptos de probabilidad e impacto con una variable adicional denominada detección (Carbone & Tippett, 2004, pp. 28-35). Es así que en estos tipos de riesgos es importante ver los distintos escenarios en donde se puede aplicar la variable detección y aquellos en donde el NPR debe ser orientado a la tradicional metodología de consecuencia y probabilidad.

Los criterios que inciden en la dinámica del riesgo para la evaluación de la variable detección versan, principalmente, en la línea de tiempo diferencial entre la manifestación del riesgo y la manifestación del daño con dificultad de recuperación de este.

A manera de ejemplo, uno de los casos en donde se puede ver con claridad la importancia de la variable detección es en el sector de la seguridad comercial. Allí, su principal riesgo, la merma por hurto[2], permite identificar claramente un tiempo en el que es factible detectar (identificar y recuperar) el bien o el elemento hurtado. Esta afirmación es clara y deja ver la diferencia entre la prevención del riesgo, que incide directamente en la probabilidad de ocurrencia con un sistema de protección orientado a esta labor, y la capacidad de detección, que incide en otro sistema de protección diferente y con menos impacto en los controles hacia el cliente.

En el mismo sentido, esto sucede muy favorablemente con los principales riesgos de la seguridad ciudadana. El robo se ha convertido en una de las amenazas que más afecta a los ciudadanos latinoamericanos, en donde una de cada cinco personas manifestó haber sido víctima de robo en el año 2012, lo cual muestra que se triplicó este delito sustancialmente en los últimos 25 años (Programa de las Naciones Unidas para el Desarrollo [PNUD], 2003). Cuando en la vía pública una persona es victimizada por robo, la capacidad de detección puede ser interpretada en la respuesta de las autoridades en neutralizar al agente generador del riesgo y la recuperación del bien o elemento robado.

Estos dos casos de análisis permiten generar nuevos sistemas de seguridad en los campos corporativo y ciudadano, como propuesta para el tratamiento de los riesgos en ambientes donde la prevención del riesgo resulta de difícil implementación, con una estrategia más adecuada o con menor impacto en el cliente mediante la oportuna detección (identificación y neutralización del agente generador del riesgo).

Conclusiones

Este texto realizó un análisis metodológico de la dinámica del riesgo antrópico, desde la perspectiva del *iter criminis*, para utilizar la metodología del Análisis Modal de Fallos y Efectos (AMFE), incluida en el estándar ISO 31010:2009 y hace un planteamiento ajustado para lograr su adecuada utilización en este tipo de riesgos.

Así, se concluye que el riesgo antrópico puede tener un enfoque bidimensional o tridimensional, dependiendo de la dinámica propia del tipo de riesgo y su forma de manifestación. Esto hace posible que entre la fase manifestación del riesgo y manifestación del daño pueda existir el espacio de tiempo que permita detectar y neutralizar el riesgo para evitar la ocurrencia del daño sobre el sistema.

De acuerdo con este planteamiento del riesgo antrópico, la metodología del Análisis Modal de Fallos y Efectos (AMFE) puede ser aplicada eficazmente en este y otros campos. El AMFE puede ser usado en la evaluación de riesgos antrópicos, pero se hace necesaria la redefinición del

2 Generado por personas externas, el cual comprende el seguimiento desde que la persona toma posesión del bien, hasta que logra evadir todos los controles de seguridad y culmina con la evasión total del sistema de protección.

significado de sus variables cuantitativas: severidad, ocurrencia y detectabilidad, ajustadas a la dinámica propia del riesgo antrópico en una escala de uno (1) a diez (10), como fue propuesto en este texto, con lo cual se le da un alcance gradual a cada uno de los rangos de estas variables.

La variable detectabilidad aporta una nueva perspectiva de análisis para medir los riesgos en un momento particular de las fases o etapas, permitiendo así, no solo la valoración, sino también la propuesta de mecanismos de tratamiento y control del riesgo antes de la generación del daño.

Así, la aplicación del AMFE permite un análisis integral del riesgo en cada etapa y, al mismo tiempo, plantear medidas adecuadas de tratamiento, orientadas a cada una de las variables, según el riesgo y la necesidad particular de cada sistema u organización.

Finalmente, su aplicación se amolda a aquellos tipos de riesgos antrópicos bidimensionales (severidad y ocurrencia) o tridimensionales (severidad, ocurrencia y detectabilidad), con una amplia utilidad en todos los escenarios de seguridad corporativa y seguridad ciudadana. Es importante, como en muchas metodologías, que cada modelo de organización construya su propia matriz de resultados para identificar, según su aversión o apetito por el riesgo, la significancia de los valores obtenidos y la posición de la organización frente a estos.

Referencias

1. ASIS International. (2003). *General Security Risk Assessment Guideline*.
2. Australian/New Zealand Standard. (2004). Risk Management AS/NZS 4360:2004. Sydney, Wellington, New Zealand.
3. Bernate Ochoa, F. (2008). *La distinción entre actos preparatorios y actos ejecutivos en el Código Penal*. Recuperado de: https://www.unifr.ch/ddp1/derechopenal/articulos/a_20080521_29.pdf
4. Bravo Mendoza, O., & Sánchez Celis, M. (2012). *Gestión Integral de Riesgos*. Tomo 1. 4ta Edición En: Bravo y Sanchez EU., Broder, J., & Tucker, E. (2012). *Risk Analysis and the Security Survey*. Butterworth-Heinemann.
5. Carbone, T. A., & Tippett, D. D. (2004). Project Risk Management Using the Project Risk FMEA. *Engineering Management Journal* 16 (4), 28-35.
6. Cardona A., O. (2003). *La necesidad de repensar de manera holística los conceptos de vulnerabilidad y riesgo. Una crítica y una revisión necesaria para la gestión*. Universidad de los Andes. Centro de Estudios sobre Desastres y Riesgos CEDERI. La Red., 1-18.
7. Carlson, C. (2012). *Effective FMEAs: Achieving Safe, Reliable, and Economical Products and Processes Using Failure Mode and Effects Analysis*. Ed. Wiley. New Jersey.
8. Castro Maradiaga, J. (2009). Las etapas del iter criminis, y su aplicación práctica en los tipos de injusto de homicidio y asesinato. *Revista de Derecho,* Vol. 12, 97-132. Recuperado de http://dx.doi.org/10.5377/derecho.v0i12.1004
9. Cauwenbergh Van, G. (2012). *Failure Mode Effect Analysis (FMEA): A guide to understand and use one of the most important tools in our Business Improvement Toolbox*. Ed Digital: LSSBI.COM.
10. Córdoba Ángulo, M. (1993). *La Tentativa*. Bogotá: Universidad Externado de Colombia.
11. Cuatrecasas Arbos, L. (2010). *Gestión integral de la calidad: implantación, control y certificación*. Barcelona: Profit.
12. Financial Action Task Force (FATF). (2013). *Guidance. National Money Laundering and Terrorist Financing Risk Assessment*. París, Francia. Recuperado de: http://www.fatf-gafi.org/media/fatf/content/images/National_ML_TF_Risk_Assessment.pdf
13. Ghantt, T. (2012). *Project Risk Management: Using Failure Mode Effect Analysis for Project Management*. Plumbline Publishing Group. Edición digital: www.thomasghantt.us
14. Hopkin, P. (2014). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*. IRM. London and Philadelphia.
15. ICONTEC (2004). Norma Técnica Colombiana 5254. Gestión del Riesgo. Bogotá. ICONTEC.

16. ICONTEC Internacional. (2007). Norma Técnica Colombiana NTC-IEC 60812. Sistemas de Gestión. Técnicas de análisis para la confiabilidad de los sistemas. Procedimientos para Análisis de Modos de Falla y Efectos. Bogotá: Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC).
17. International Organization for Standadization. (2009). Risk Management. Risk Assessment Techniques. ISO 31010:2009. Geneva, Switzerland.
18. International Organization for Standadization. (2009). Risk Management. Principles and Guidelines. ISO 31000:2009. Geneva, Switzerland.
19. Jiménez Martínez, J. (2010). *La teoría del delito. Aproximación al estado de la discusión*. Editorial Porrúa. Ciudad de Méjico.
20. Lozano Lozano, C. (1979). *Elementos de Derecho Penal*. Temis LTDA. Bogotá.
21. Mejía Quijano, R. (2006). *Administración de Riesgos - Un enfoque empresarial*. Medellín: Universidad EAFIT.
22. Ministerio de Trabajo y Asuntos Sociales de España - Instituto Nacional de Seguridad e Higiene en el Trabajo. (2004). Notas Técnicas de Previsión. *NTP 679: Análisis modal de fallos y efectos. AMFE*. España.
23. Mitroff, I., & Anagnos, G. (2005). *Managing Crises Before They Happen: What Every Executive and Manager Needs to Know about Crisis Management*. New York: American Management Association - AMACOM.
24. Mollah, A. (2005). *Aplication of Failure Mode and Effect Analysis (FMEA) for Process Risk Assessment*. Focus On: Project Management, pp. 12-20.
25. O'Byrne, P. (2008). *The dissection of risk: a conceptual analysis*. Nursing Inquiry 15(1), 30-39.
26. Ostrom, L., & Wilhelmsen, C. (2012). *Risk Assessment: Tools, Techniques, and Their Applications*. Ed. Wiley. New Jersey.
27. Programa de las Naciones Unidas para el Desarrollo — PNUD—. (2003). *Informe Regional de Desarrollo Humano 2013-2014. Seguridad ciudadana con rostro humano: diagnóstico y propuestas para América Latina*. Nueva York: Alfa Omega Impresores.
28. Reyes Meléndez, F. (2004). Disertación. *A selection and comparison of risk assessment methods and models to be used for the international ship and port facility security code*. Malmö, Sweden.
29. Rogers, B. (2006). Engineering Principles for Security Managers. En M. Gill, *The Handbook of Security*. Palgrave Macmillan, pp. 66 – 89.
30. Safety and Reliability Society. (2011). *Applied R&M Manual for Defence Systems Part C - R&M Related Techniques*. London - UK.
31. Salas Beteta, C. (2007). *El íter criminis y los sujetos activos del delito*. Revista Internauta de Práctica Jurídica. Número 19, 1-15. Retrieved from: https://www.uv.es/ajv/art_jcos/art_jcos/num19/RIPJ_19/EX/19-11.pdf
32. Scurek, R. (2011). Risk analysis of a critical infrastructure facility. *The Science for Population Protection,* 03(1), 1-11.
33. Talbot, J., & Jakeman, M. (2009). *Security Risk Management Body of Knowledge*. Ed. Wiley. New Jersey.
34. The International Electrotechnical Commission (IEC). (2006). Norma. IEC 60812 Analysis techniques for system reliability Procedure for failure mode and effects analysis (FMEA). Geneva, Switzerland.
35. Valero Ramos, R., & Cruz Tordesillas, J. (2002). *Manual de seguridad*. Madrid: Autor-Editor.
36. Zambrano Pasquel, A. (2012). *La teoría del delito y el código orgánico integral penal*. Retrieved from: http://www.alfonsozambrano.com/doctrina_penal/22062014/dp-teoria_delito_COIP.pdf