Toma de decisiones en la gestión de riesgos cibernéticos: una aproximación fenomenológico-hermenéutica

Gloria Cristina Pabón Noreña[1], *Claudia Marcela Palacio Henao*[2], *Horacio Manrique Tisnés*[3]

PALABRAS CLAVE
ciberseguridad, fenomenología-hermenéutica, gestión de riesgos cibernéticos, incertidumbre, toma de decisiones.
CLASIFICACIÓN JEL
M15, O32, O33.
RECIBIDO
07/10/2021
APROBADO
05/10/2022
SECCIÓN
Gestión de tecnologías, información y comunicación

Resumen: Los ciberataques aumentan y sus impactos son difíciles de estimar. El desconocimiento del tipo de riesgo genera alta complejidad y baja capacidad de predicción. En consecuencia, los gerentes toman decisiones basados en su experiencia e intuición en escenarios de incertidumbre. Esta investigación explora factores intervinientes en la gestión de riesgo cibernético (GRC) desde la perspectiva de los decisores, mediante diseño cualitativo y método fenomenológico-hermenéutico. Se entrevistaron ocho directivos con amplia experiencia en el campo de la ciberseguridad en organizaciones colombianas grandes. Como resultado del análisis, desde la experiencia de los entrevistados, se identificaron 191 unidades de sentido que se agruparon en 37 subcategorías, nueve categorías y dos supracategorías, que se integran en un esquema cualitativo, representando la toma de decisiones (TD) desde la perspectiva de decisores en ciberseguridad. Este esquema cualitativo es un aporte necesario, novedoso y original a la comprensión del proceso de TD en la gestión de las tecnologías de la información y la comunicación (TIC), pues permite conocer factores intervinientes en la TD para la GRC, desde la perspectiva de los decisores. Se encontró que, aunque la experiencia del decisor es muy importante, la madurez de la organización incide significativamente en la forma de gestión y toma decisiones. Finalmente, se señalan las limitaciones del estudio.

Citación sugerida: Pabón-Noreña, G., Palacio-Henao, C, & Manrique-Tisnés, H. (2024). Toma de decisiones en la gestión de riesgos cibernéticos: una aproximación fenomenológico-hermenéutica. *Innovar, 34*(93), e98107. https://doi.org/10.15446/innovar.v34n93.98107

DECISION-MAKING IN CYBER RISK MANAGEMENT: A PHENOMENOLOGICAL-HERMENEUTICS APPROACH

Abstract: Cyberattacks are increasing and their impact is difficult to estimate. Lack of awareness on the types of risks generate high complexity and low predictive capacity. Consequently, business managers make decisions based on their experience and intuition in the face of uncertainty scenarios. This research explores the factors involved in cyber risk management (CRM) from the perspective of decision-makers, using a qualitative design and a phenomenological-hermeneutic method. Eight executives with extensive experience in the field of

[1] M. Sc. en Administración de riesgos, Universidad EAFIT; Medellín, Colombia; Rol del autor: intelectual, experimental y comunicativo; gcpabonn@eafit.edu.co; http://orcid.org/0000-0002-1843-200X
[2] M. Sc. en Administración de Riesgos, Universidad EAFIT; Medellín, Colombia.; Rol del autor: intelectual, experimental y comunicativo; cmpalacioh@aefit.edu.co; http://orcid.org/0000-0002-4455-2873
[3] Ph. D. en Psicología, Universidad EAFIT; Medellín, Colombia; Grupo de investigación: El método analítico y sus aplicaciones en las ciencias sociales y humanas; Rol del autor: intelectual y comunicativo; hmanriqu@eafit.edu.co; http://orcid.org/0000-0002-7621-7391

cybersecurity at large Colombian organizations were interviewed. As a result of the analysis, 191 units of meaning were identified from the experience of interviewees. These units were grouped into 37 subcategories, nine categories, and two supercategories, which are integrated into a qualitative framework representing decision-making (DM) from the perspective of decision-makers in cybersecurity. This qualitative framework is a necessary, novel, and original contribution to understanding the DM process in the management of information and communication technologies (ICT), as it allows for an understanding of factors involved in DM for CRM from the perspective of those responsible for making decisions. It was found that although the decision-maker's experience is important, the maturity of the organization significantly affects the overall management and decision-making process.
Keywords: Cybersecurity, phenomenology-hermeneutics, cyber risk management, uncertainty, decision-making.

TOMADA DE DECISÃO NA GESTÃO DO RISCO CIBERNÉTICO: UMA ABORDAGEM FENOMENOLÓGICO-HERMENÊUTICA

Resumo: os ataques cibernéticos estão aumentando e seus impactos são difíceis de estimar. O desconhecimento do tipo de risco gera alta complexidade e baixa previsibilidade. Consequentemente, os gerentes tomam decisões com base em sua experiência e intuição em cenários incertos. Esta pesquisa explora os fatores envolvidos no gerenciamento de riscos cibernéticos (GRC) sob a perspectiva dos tomadores de decisão, usando um projeto qualitativo e um método fenomenológico-hermenêutico. Foram entrevistados oito gerentes com ampla experiência no campo da segurança cibernética em grandes organizações colombianas. Como resultado da análise, a partir da experiência dos entrevistados, 191 unidades de significado foram identificadas e agrupadas em 37 subcategorias, nove categorias e duas supracategorias, que foram integradas em um esquema qualitativo, representando a tomada de decisão (TD) da perspectiva dos tomadores de decisão em segurança cibernética. Essa estrutura qualitativa é uma contribuição necessária, nova e original para a compreensão do processo de TD no gerenciamento de tecnologias de informação e comunicação (TIC), pois fornece uma visão dos fatores envolvidos na TD para GRC, sob a perspectiva dos tomadores de decisão. Descobriu-se que, embora a experiência do tomador de decisões seja muito importante, a maturidade da organização tem um impacto significativo na forma como ela gerencia e toma decisões. Por fim, são observadas as limitações do estudo.
Palavras-chave: segurança cibernética, fenomenologia-hermenêutica, gestão de riscos cibernéticos, incerteza, tomada de decisões.

INTRODUCCIÓN

Con la llegada de nuevas tecnologías como inteligencia artificial, computación cuántica, Internet de las cosas, redes de quinta generación, nube de tecnología, *blockchain*, además del aumento del trabajo en casa como alternativa laboral en la pandemia, se ha dado lugar a nuevas oportunidades, pero también a nuevas formas de ciberataques, incrementando la inversión en mitigación del riesgo en 50% de 2019 a 2020 (World Economic Forum [WEF], 2020). Sin embargo, estos no parecen estar disminuyendo. Por ejemplo, los ataques *ramsomware* se han incrementado en un 435% en 2020 (WEF, 2022). En 2020 el riesgo cibernético (RC) fue el segundo más preocupante para los negocios para los siguientes diez años (WEF, 2020). La mayor vulnerabilidad parece ser el error humano con un 95% (WEF, 2022).

Gestionar el RC trasciende aspectos tecnológicos convirtiéndose en un tema de organizaciones estratégico, llevando a establecer un mayor compromiso gerencial y movilización hacia una cultura de

ciberseguridad que apalanque la toma de decisiones (TD) (Balawejder et al., 2019). "A medida que cambia el panorama de las amenazas cibernéticas, las organizaciones deben actualizar sus estrategias de ciberseguridad" (Lee, 2020, p. 9). Solo 19% de los decisores confían en que sus empresas abordarán efectivamente un incidente de ciberseguridad (Jalali et al., 2019). Estos datos evidencian que muchas compañías ignoran o subestiman los RC o dependen de soluciones tradicionales para su gestión.

Por otra parte, Eling et al. (2021) muestran avances desde que aparecieron los primeros artículos de ciberseguridad: Madnick (1978) acuña el término *seguridad computacional*; Hovav y D'Arcy (2003) fueron primeros en publicar en una revista de administración de riesgos; Eling y Wirfs (2019) diferencian entre RC de la vida cotidiana (asegurables) y RC extremos (no asegurables). Asimismo, hay avance desde que Von Solms y Van Niekerk (2013) definieron el concepto de ciberseguridad. También hay progreso desde que McAfee y Haynes (1989) advirtieron los riesgos de los ataques con virus y gusanos informáticos, hasta estudios como el de Kamiya et al. (2019) que sugieren que las organizaciones con mayor apalancamiento tienden a ser más vulnerables a los ciberataques, pues no cuentan con recursos para investigar.

Sin embargo, la mayoría de los estudios se centran en asuntos técnicos, desconociendo la investigación interdisciplinaria que integre áreas como psicología, economía y factores humanos, buscando así aportar a la investigación en ciberresiliencia o capacidad organizacional de reaccionar rápidamente y reponerse a los ciberataques (Collier et al., 2013; Eling et al., 2021). Por eso, el enfoque de TD es importante para estudiar

experiencias de personas que han enfrentado ciberataques organizacionales, al identificar elementos clave en sus reacciones que sirvan para comprender factores que influencian la gestión de riesgo cibernético (GRC) desde la perspectiva de los decisores.

Por otro lado, algunas investigaciones muestran que, cuando los humanos se enfrentan a escenarios de baja probabilidad y alta consecuencia y a escenarios de alta incertidumbre, como es el caso de los RC, sus percepciones son influenciadas por emociones como miedo, ansiedad o preocupación, haciendo que se concentren en proteger activos de su organización a corto plazo, a costa de la planificación a largo plazo (De Smidt & Botzen, 2018; WEF, 2022).

Con el auge de la economía comportamental, tales percepciones han sido revisadas, pues los decisores, al igual que los otros miembros de la organización, son propensos a errores cognitivos referidos a cómo interpretan y reaccionan ante la información de posibles riesgos (Jalali et al, 2019). En general, se requiere una comprensión más precisa de los elementos que contribuyen a movilizar a los decisores frente a algunos riesgos e ignorar otros. En GR este elemento cognitivo es importante para entender los riesgos que se enfrentan y convertir el conocimiento en acciones efectivas (Hersing, 2017).

Los resultados de este estudio constituyen un aporte necesario, novedoso, original y plausible a la comprensión del proceso de TD en el área de las tecnologías de la información y la comunicación (TIC), pues permiten conocer factores intervinientes en la TD, desde la perspectiva de los decisores, en el campo disciplinar de la gestión, en general (Kahneman & Klein, 2009; Simon, 1987), y la gestión de RC, en particular (Proctor & Chen, 2015; Ramrathan & Sibanda, 2017).

La pregunta de investigación del presente estudio es la siguiente: *¿Cuáles son los factores influenciadores de la TD en la GRC en algunas empresas de Colombia?* Esta investigación busca explorar factores influenciadores de la TD en la GRC, mediante una aproximación fenomenológico-hermenéutica, que analiza sus características desde la perspectiva de los decisores. Esta área de conocimiento se encuentra en evolución tanto para la academia como para diferentes sectores empresariales y gubernamentales; de allí la relevancia y vigencia de la investigación (Eling et al., 2021; WEF, 2022).

A continuación, en los referentes conceptuales, se plantean los principales enfoques de TD, desde la perspectiva del procesamiento dual (Kahneman & Klein, 2009), y su relación con la GRC, desde los enfoques y necesidades actuales, en el denominado enfoque de ciberresiliencia (Eling et al., 2021). Luego, se presenta el diseño metodológico de esta investigación, consistente en una aproximación cualitativa (Levitt et al., 2018), con un método fenomenológico-hermenéutico (De Castro et al., 2007; Laverty, 2003), que permite una aproximación al sentido de que los decisores asignan al proceso de TD en administración (Kordeš, 2009; Manrique & De Castro, 2019) y en ciberseguridad (Ramrathan & Sibanda, 2017), captando elementos psicológicos y organizacionales fundamentales. Esta metodología, combinada con la propuesta de Gioia et al. (2013) inspirada en la teoría fundamentada, posibilitó obtener un esquema cualitativo en el que se representa el proceso de TD en ciberseguridad desde la perspectiva de los decisores. Este esquema integra aportes fundamentales del presente trabajo: el proceso de TD en GRC implica factores del decisor, factores organizacionales y tres posibles escenarios: administración del riesgo, enfrentar un ataque cibernético y aprendizaje.

REVISIÓN DE LITERATURA

Toma de decisiones

Los modelos normativos tradicionales de TD se basan comúnmente en la lógica y la racionalidad (Kahneman & Klein, 2009). No obstante, desde los actuales modelos descriptivos de procesamiento dual, la TD está influenciada, además, por variables intuitivas y afectivas (Builes, 2022; Hersing, 2017; Manrique & De Castro, 2019). Para la aproximación de racionalidad limitada (Simon, 1987), las personas deciden según lo satisfactorio (no lo óptimo). De acuerdo con una perspectiva naturalista, las personas se basan en impulsos, intuición, creencias personales o experiencias anteriores (Manrique, 2019).

Actualmente, se acepta que la TD se basa en dos sistemas cognitivos (Kahneman & Klein, 2009): el sistema 1, el *intuitivo*, se caracteriza por un procesamiento automático, asociativo, rápido, sin esfuerzo y emocional; el sistema 2, el *reflexivo*, se caracteriza por ser controlado, deliberado, que requiere esfuerzo y consciencia, y es afectivamente neutro. Ambos sistemas trabajan a la vez logrando decisiones válidas. Así, el sistema 1 es necesario para el buen funcionamiento del sistema 2 (Damasio, 2007).

Según el Banco Mundial (2015), las decisiones humanas se apoyan en tres principios: i) *pensamiento automático* (Kahneman & Klein, 2009), que simplifica los problemas, dado que completa la información faltante con creencias acerca del mundo; ii) *pensamiento social* (Sunstein & Thaler, 2017), según el cual las personas imitan y aprenden de otros; iii) *modelos mentales* (Hogarth, 2010), como conceptos, estereotipos, creencias, que guían la acción según la situación y la cultura. La mayoría de las personas creen que deciden racionalmente, pero con frecuencia actúan automáticamente, influenciadas por su entorno social y modelos mentales compartidos.

Bashir et al. (2017) clasifican los estilos de TD en racional, intuitivo, dependiente, evitativo y espontáneo: los decisores racionales se basan en una evaluación metódica de las diferentes opciones; los intuitivos están más influenciados por su "instinto" y presentimiento; los dependientes buscan el consejo y la orientación; los evasivos evitan tomar decisiones para no asumir la responsabilidad; los espontáneos buscan resolver las situaciones rápidamente.

En las investigaciones recientes, se incluye la intuición como un factor relevante en TD (Gigerenzer, 2008). Su base es la experiencia y surge de asociaciones rápidas, mediante juicios cargados afectivamente, no-conscientes y cuyo resultado se puede manifestar en sentimientos (Manrique, 2019). De acuerdo con Ramrathan y Sibanda (2017), la intuición es efectiva en situaciones en las cuales la información y el tiempo son limitados, y los objetivos, las variables y alternativas de solución son ambiguos, existiendo incertidumbre. La experiencia es un factor clave en su formación y aplicación pues, a partir del aprendizaje implícito, las personas desarrollan estructuras cognitivas que fundamentan la intuición (Hogarth, 2010).

Riesgos cibernéticos

Las nuevas tecnologías de Internet, redes informáticas, sistemas de información, inteligencia artificial e Internet de las cosas, entre otras, han generado cambios en las formas de relación humana. El uso del Internet aumentó con un crecimiento exponencial entre el 2000 y el 2017 de un 290%, que ha beneficiado a personas y organizaciones, pero también ha generado nuevas amenazas (Karake et al., 2017). Dichas amenazas pueden

ser de origen interno o externo a la organización, causadas por individuos u organizaciones, e incidir en herramientas tecnológicas como las mencionadas. Lo anterior hace referencia a lo que se denomina riesgo cibernético (RC) (Von Solms & Van Niekerk, 2013), que se asocia a fallas en la tecnología y sistemas de información, con impactos en el ámbito financiero, la operación y la reputación de una organización (Eling & Wirfs, 2019). Los impactos financieros son difíciles de calcular, pues muchas organizaciones pueden estar bajo ataque cibernético, pero desconocerlo (Karake et al., 2017). Los ataques cibernéticos continúan aumentando y son más sofisticados. A medida que aumenta la capacidad en las organizaciones para enfrentar estos eventos, aparecen nuevas formas y vulnerabilidades (Eling et al., 2021). Entonces, la pregunta frente a un ataque cibernético no es si puede pasar, sino cuándo y con qué impacto (Jalali et al., 2019). Dichos ataques no tienen fronteras geográficas y son difíciles de detectar y anticipar, lo que aumenta la potencialidad de desencadenar riesgos con alto impacto económico, reputacional y legal (Sheppard et al., 2013). Por eso, una adecuada GRC implica que las organizaciones identifiquen las amenazas y evalúen vul-nerabilidad e impactos esperados (Sheppard et al., 2013). Además, requiere un abordaje sistemático que reconozca las interacciones entre sistemas cibernéticos, físicos y conducta humana, con el fin de prevenir o mitigar eventos no deseados (Eling et al., 2021; Jalali et al., 2019).

Toma de decisiones y riesgos cibernéticos

Se espera que los gerentes sean procesadores de información sofisticados para una TD relacionada con el riesgo de acuerdo con el entorno organizacional, incentivos económicos, sistemas de información y variables disponibles. Sin embargo, a menudo estos tienen una permanencia limitada en las organizaciones y pocas opciones para enfrentar los riesgos, así como son propensos a una serie de sesgos cognitivos (Jalali et al, 2019). Además, la falta de flexibilidad, adaptabilidad y dimensionamiento para atender un incidente cibernético puede afectar los mejores planes de respuesta (Sheppard et al., 2013). Por otra parte, en las organizaciones, factores como la influencia económica, social y política, o los procedimientos inciden en el proceso de TD (Kamiya et al., 2019). Según Manrique y De Castro (2019), "las decisiones individuales tienen efectos sobre lo colectivo. En una organización empresarial, cada persona se encuentra en un nivel jerárquico y, de acuerdo con ese nivel, deberá tomar decisiones de mayor o menor alcance" (p. 251), teniendo en cuenta que esta libertad de decidir lleva consigo una responsabilidad ética (Manrique, 2019). Las personas representan un elemento crucial en la ciberseguridad sin importar su nivel jerárquico, siendo los empleados el eslabón más débil (Proctor & Chen, 2015). En este sentido, es fundamental que las organizaciones tengan presente el sentido de los decisores en la gestión de sus riesgos (Hersing, 2017).

Además, el desarrollo tecnológico informacional no implica que el ser humano pierda importancia en la TD organizacional, dado que es él quien está llamado a liderar los procesos basados en nuevas tecnologías y a servirse de ellas (Eling et al., 2021). En última instancia, el ser humano sigue tomando las decisiones, al establecer los parámetros de funcionamiento de las nuevas tecnologías informacionales (Ramrathan & Sibanda, 2017).

El proceso de TD en la gestión en ciberseguridad ha de ser mejor comprendido con la finalidad de determinar la forma en que se integran los aspectos psicológicos con factores organizacionales, y revisar formas de fortalecer la prevención de la materialización del RC (Jalali et al., 2019). Este enfoque interdisciplinario puede contribuir a generar ciberresiliencia en las organizaciones (Collier et al., 2013; Eling et al., 2021; Zhang et al., 2016).

Collier et al. (2013) plantean cuatro dominios de ciberseguridad: i) físico (hardware y software que constituyen redes de ciberseguridad), ii) informacional (monitoreo, almacenamiento y visualización de la información), iii) cognitivo (percepción y uso de la información para la toma de decisiones) y iv) social (consideraciones éticas, culturales, legales, políticas, entre otras). El presente estudio se ubica en el dominio cognitivo. Las principales aproximaciones de investigación en este dominio son las siguientes:

1. *Factores humanos.* Es el estudio interdisciplinario (ergonomía, ingeniería, sociología, psicología, etc.) de la interacción del ser humano con máquinas, sistemas y procesos. Por ejemplo, Proctor y Chen (2015) muestran la importancia que las decisiones y acciones de los seres humanos tiene para las medidas de seguridad y, en consecuencia, la necesidad de integrarlas a la ciencia de la seguridad.

2. *Métodos matemáticos.* Son utilizados para el estudio de procesos y conductas. Por ejemplo, partiendo de la teoría de juegos, Zhang et al. (2016) analizaron la influencia de la racionalidad limitada en el juego estocástico de ciberataque-defensa. Los autores construyeron un modelo de juego estocástico con un algoritmo con capacidad de aprendizaje en línea, lo que posibilita una buena estrategia de defensa.

3. *Psicología cognitiva y comportamental.* Por ejemplo, Zeijlemaker et al. (2022) encontraron que los decisores en ciberseguridad que tienen bajo desempeño usan estrategias sobrerreactivas en lugar de proactivas. Además, M'manga et al. (2019) proponen un modelo normativo de toma de decisiones de ciberseguridad en situaciones de riesgo e incertidumbre. Su diseño se basó en la literatura sobre TD. El modelo resulta interesante porque muestra el proceso cognitivo detallado de toma de decisiones (enfoque activo o reactivo, búsqueda de información, generación, validación y selección de opciones, entre otros elementos), aunque desatiende la influencia de los factores organizacionales.

El aporte del presente trabajo se ubica en la tercera aproximación de estudio de TD en ciberseguridad, complementando propuestas como las de M'manga et al. (2019) y Zeijlemaker et al. (2022), mostrando factores intervinientes en la TD en GRC desde la perspectiva de los decisores, lo que permitirá comprender mejor el sentido atribuido por ellos.

MÉTODO

Enfoque y alcance

Se utilizó un enfoque cualitativo, que busca la comprensión de los fenómenos desde la experiencia de las personas (Levitt et al., 2018). Se utilizó el método fenomenológico-hermenéutico, caracterizado por "partir de la perspectiva de la misma persona, tratando de encontrar y comprender el significado que le da a su propia experiencia" (De Castro et al., 2007, p. 3). Este método se centra en el significado de la experiencia humana (fenomenología) (Giorgi, 2010) y la interpretación y comprensión de sus acciones en el contexto (hermenéutica) (Laverty, 2003). El estudio tuvo un alcance exploratorio que permitió conocer cómo los participantes de la investigación experimentan la TD en un escenario de GRC (Hernández et al., 2006; Kordeš, 2009; Ramrathan & Sibanda, 2017).

Instrumentos y participantes

Debido a la necesidad de conocer los sentidos atribuidos al proceso de TD por los decisores en ciberseguridad y, en coherencia con el diseño metodológico, la recolección de la información se realizó a través de entrevistas semiestructuradas, con un protocolo de preguntas abiertas flexibles que permitió comprender la TD desde el punto de vista de los participantes (Levitt et al., 2018).

Específicamente, la consigna inicial para los entrevistados fue "Narre, detalladamente, una situación de GRC que le haya impactado". Se entrevistaron ocho personas con amplia experiencia en cargos de nivel directivo y respon-sabilidad en la GRC (tabla 1), que representan grandes compañías colombianas, algunas multilatinas y líderes en los sectores económicos a los que pertenecen. Esto justifica la selección de los ocho participantes (tabla 1).

El muestreo fue por conveniencia (Hernández et al., 2006), para obtener la mejor información en el menor tiempo posible, y con el criterio de que los participantes proporcionaran información suficiente y estuvieran dispuestos a participar. El número de entrevistados se definió por criterio de disposición de los participantes a contribuir en la investigación y teniendo en cuenta la recomendación del número óptimo de participantes en estudios fenomenológicos (Hernández et al., 2006). Su participación fue voluntaria, autorizando el uso de la información con fines académicos, a través de un consentimiento informado verbal, el cual quedó grabado al final de cada una de las entrevistas, con la claridad de que se eliminarían datos que permitieran identificar al entrevistado y su empresa. Los entrevistados se contactaron vía telefónica, primero, y se realizó la entrevista presencial en su lugar de trabajo, después.

Las entrevistas, que duraron entre 32 y 74 minutos (54 minutos en promedio), se grabaron en audio y se transcribieron. Posteriormente, se analizó en detalle la información, siguiendo la propuesta de Giorgi (2010), en la versión fenomenológico-hermenéutica de De Castro et al. (2007), que consiste en

1. Leer y releer la transcripción de las entrevistas.
2. Segmentar la entrevista completa en unidades de sentido.
3. Transformar las unidades de sentido en lenguaje técnico.
4. Identificar reacciones, prejuicios o interpretaciones como investigadores y contrastar los hallazgos de las entrevistas con los referentes teóricos. Este paso se relaciona directamente con el proceso de *reflexividad* (Levitt et al., 2018), mediante el que los investigadores reflexionan sobre la información obtenida en las entrevistas, a la luz de sus saberes previos y la literatura especializada.

Tabla 1.
Caracterización general de los entrevistados.

Características	1	2	3	4	5	6	7	8
Género	Masculino	Masculino	Masculino	Femenino	Masculino	Masculino	Masculino	Masculino
Experiencia directiva (años)	10	10	9	8	11	30	20	19
Formación básica	Ingeniero de sistemas	Ingeniero de sistemas	Ingeniero de sistemas	Ingeniera biomédica	Ingeniero de sistemas	Ingeniero de sistemas	Ingeniero de sistemas	Ingeniero informático
Nivel máximo de formación	Magíster en administración y finanzas	Magíster en administración de riesgos	Estudiante de maestría	Magíster en administración, economía e Ingeniería industrial	Especialista en seguridad informática	Magíster en gestión de negocios	Ingeniero de sistemas	Especialista en redes y certificado como analista forense
Cargo	Director de tecnología	Oficial de seguridad de la información	Oficial de seguridad de la información	Director de control interno y riesgos de tecnologías de la información (TI)	Auditor en TI	Jefe de la unidad de servicios de procesamiento de datos	Director de ciberseguridad y seguridad de la información	Jefe de operación de ciber-seguridad
Especialidad	Tecnología e infraestructura	Tecnología Seguridad de la información Infraestructura y arquitectura de servicios	Tecnología	Tecnología Seguridad de la información	Auditoría	Tecnología	Tecnología y telecomunicaciones	Tecnología Seguridad informática
Sector de la organización	Servicios de ingeniería	Sector público	Producción de alimentos	Servicios financieros	Producción de alimentos	Servicios públicos domiciliarios	Servicios financieros	Servicios financieros
Tamaño de la organización	Mediana Empresa	Gran Empresa	Gran Empresa	Gran Empresa	Gran Empresa	Gran Empresa	Gran Empresa	Gran Empresa
Hace parte de un grupo económico	No	No	Sí	Sí	Sí	No	Sí	Sí
Operación	América Latina	Estatal	Nacional	América Latina	Nacional	América Latina	América Latina	América Latina
Fecha de la entrevista	14 de agosto 2019	30 de agosto 2019	16 de septiembre 2019	23 de septiembre 2019	18 de noviembre 2019	28 de noviembre 2019	6 de diciembre 2019	18 de diciembre 2019
Duración de la entrevista (minutos)	74	32	71	50	51	34	53	66

Fuente: Elaboración propia.

Para estos procesos se utilizó una tabla de análisis (en Microsoft Excel®), propuesta por De Castro et al. (2007) y modificada por (Manrique & De Castro, 2019) (tabla 2).

Tabla 2.

Tabla de análisis de los datos.

Unidades de sentido	Transformación en lenguaje técnico	Reacciones, prejuicios, interpretaciones	Referentes teóricos

Fuente: elaboración propia con base en De Castro et al. (2007).

Luego, se codificaron las unidades de sentido siguiendo la propuesta de Gioia et al. (2010), inspirada en la teoría fundamentada. Estos códigos se revisaron, unificaron lingüísticamente y clasificaron en subcategorías emergentes. Después, al agrupar las subcategorías por criterio de relación conceptual, emergieron las categorías que, a su vez, se agruparon en supracategorías (tabla 3), obteniendo como resultado la estructura categorial (figuras 1 y 2).

Tabla 3.

Tabla de segmentación en categorías.

Unidades de sentido	Subcategorías	Categorías	Supracategorías

Fuente: elaboración propia con base en Manrique y De Castro (2019).

Con base en la estructura categorial, se construyó un *esquema cualitativo* de la experiencia de TD en GRC desde la perspectiva de los entrevistados, basado en una interpretación de la interacción entre las categorías (figura 3).

Con base en estos instrumentos de análisis cualitativo se realizó un proceso de triangulación (Levitt et al., 2018). Dos autores elaboraron una interpretación inicial de los datos, mientras que el tercero revisaba críticamente, antes de llegar al consenso, asumiendo la perspectiva de alguien externo (Gioia et al., 2013), técnica que busca garantizar mayor integridad metodológica (Levitt et al., 2018). De esta manera, se contrastaron interpretaciones de los hallazgos obtenidos, con los propios entrevistados, quienes contribuían con el avance, lo que implicó incluir temas no percibidos inicialmente, revisar planteamientos actualizados y modificar interpretaciones no coherentes con los datos y bibliografía disponible. Finalmente, tres investigadores externos revisaron los procesos y las categorías y realizaron recomendaciones.

RESULTADOS

Durante el análisis de resultados, a partir de 431 minutos de grabación en audio, trascritos en 76 páginas, se identificaron 191 unidades de sentido, que dieron lugar a 37 subcategorías, nueve categorías y dos supracategorías, siguiendo la propuesta de Gioia et al. (2013). Estos elementos categoriales son la base de la *estructura de los datos* (figuras 1 y 2), esquema en el que se muestra la relación entre supracategorías,

categorías y subcategorías, que representan la experiencia de la TD para la GRC, desde la experiencia de los decisores.

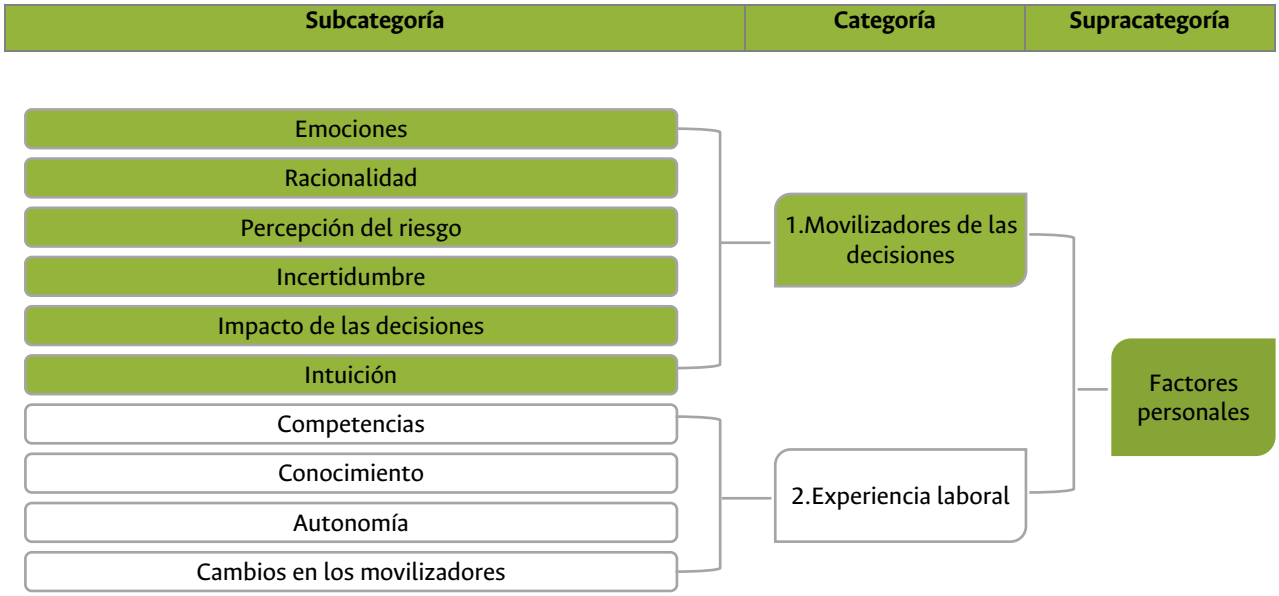

Figura 1. Estructura de los datos: supracategoría *factores personales*, categorías y subcategorías. Fuente: elaboración propia con base en Gioia et al. (2013).

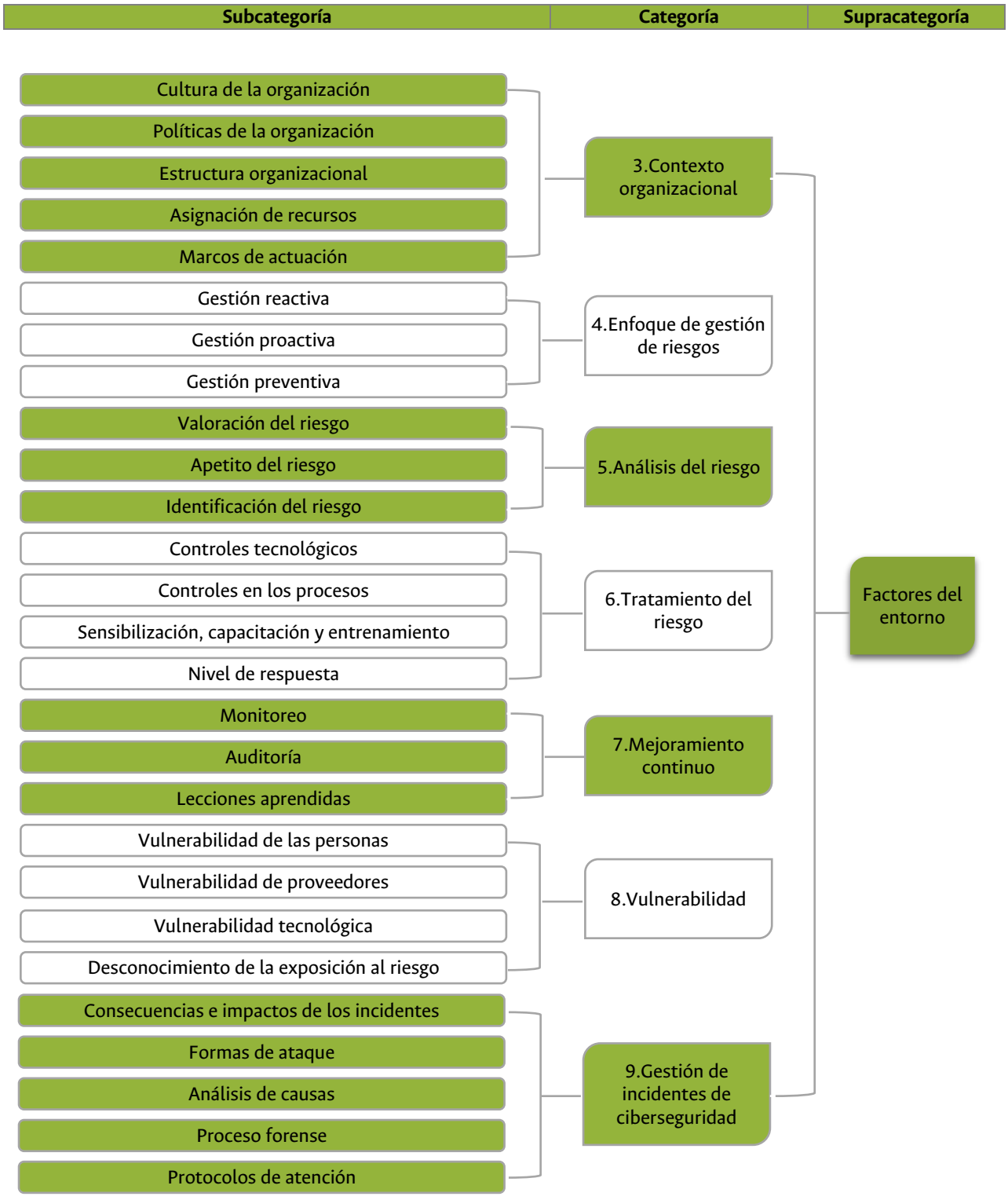

Figura 2. Estructura de los datos: supracategoría *factores del entorno*, categorías y subcategorías. Fuente: elaboración propia con base en Gioia et al. (2013).

A continuación, para cada supracategoría, se describen las categorías y subcategorías que la componen, mostrando la comprensión desde la perspectiva de los entrevistados para luego extraer algunos aprendizajes.

Primera supracategoría: factores personales

Estos factores hacen referencia a aquellas características del individuo que influencian la TD: *movilizadores de las decisiones en la gestión de riegos cibernéticos* y *experiencia laboral.*

Movilizadores de las decisiones

Los movilizadores de las decisiones son aquellas condiciones que movilizan a las personas para tomar una acción frente a un RC. Desde la perspectiva de los entrevistados, estos elementos son *emociones*, *racionalidad*, *percepción del riesgo*, *incertidumbre*, *impacto de las decisiones* e *intuición.* Las emociones y la intuición se evidencian en las siguientes palabras de los entrevistados:

> Uno tiene que pensar mucho con cabeza fría y normalmente los directivos lo ponen a uno a correr, y ahí es importante que el equipo dé respuesta a incidentes, maneje el estrés, porque todo mundo está encima en el momento del problema y uno tiene que aprender a controlarse. (6, 1.1, 89)[1]

> 'Intuición' en un incidente es como que tú empiezas a sospechar más o menos por dónde viene el ataque [...] pero para llegar a esa intuición es necesario juntar un montón de cosas y conectarlas en el cerebro: conocimiento desde la experiencia, haber aprendido de otros incidentes y conocimiento de la información que te está entregando el entorno. (8, 1.6, 189)

Por otra parte, los decisores también son movilizados por su *racionalidad*, *percepción del riesgo*, *impacto de las decisiones* e *incertidumbre.* En palabras de los entrevistados: "Cuando uno analiza un riesgo, siempre tiene que tomar decisiones bajo algún nivel de incertidumbre" (4, 1.4, 163).

Experiencia laboral

La experiencia laboral se refiere a las vivencias que acumula una persona en el desarrollo continuo, retroalimentado y corregido, de un conjunto de actividades directamente relacionadas con su cargo (Hogarth, 2010). Los datos sugieren que las *competencias* que desarrollan los decisores en su proceso laboral, además del criterio formado a través de sus vivencias y su *conocimiento* (Jalali et al., 2019), generan *cambios en los movilizadores* de sus decisiones y fortalecen su capacidad de *autonomía* para hacer sus propias elecciones. En palabras de los entrevistados: "en un cargo de gestión de riesgos las personas tienen que ser muy recursivas, que lean mucho, y que esto se les vuelva amor y pasión porque esto no es de estandarización" (3, 2.1, 80).

Los entrevistados conciben la GRC como un acto cotidiano que trasciende la frontera de la organización. Aunque existan diferentes estándares o protocolos que soporten sus decisiones, parece fundamental equilibrar el conocimiento y la experiencia con el contexto de la situación (Gigerenzer, 2008). Para esto, se requiere que los decisores tengan motivación y apertura con el ánimo de seguir aprendiendo sobre riesgos y proteger la organización (Hogarth, 2010). También importa el compromiso y la confianza de la alta gerencia

[1] La codificación utilizada para las citas de los testimonios es la siguiente: número de entrevista, número de subcategoría y número de unidad de sentido.

para generar empoderamiento en la TD; esto es coherente con lo planteado por Schwartz (2011) sobre la importancia de la confianza para fortalecer la moral de la organización. En palabras de los entrevistados:

> La organización ha madurado mucho en la atención de incidentes y "madurado mucho" significa que el equipo directivo, es consciente de los riesgos de ciberseguridad y del esfuerzo y del gran conocimiento que se necesita por parte del equipo técnico; generando menos presión y más confianza en el grupo que tenemos. (8, 2.3, 183)

Segunda supracategoría: factores del entorno

Desde la comprensión de los entrevistados, en la TD, además de los factores personales, también influyen factores del entorno; específicamente, para la GR parecen ser importantes: *contexto organizacional*, *madurez en la gestión*, *análisis del riesgo*, *tratamiento del riesgo*, *seguimiento a la gestión*, *vulnerabilidad*, *gestión de incidentes de ciberseguridad.*

Contexto organizacional

Una adecuada gestión del riesgo tiene en cuenta el contexto interno y externo de la organización, que influye significativamente en la TD (International Organization for Standardization [ISO], 2018). Frente al contexto interno, los entrevistados consideran que elementos como la *cultura de la organización*, las *políticas de la organización* y los *marcos de actuación* son el vehículo para traducir el comportamiento deseado por la dirección, lo cual es coherente con lo hallado por Isaca (2012). En palabras de los entrevistados: "nosotros generamos cultura al escribir la política [de seguridad] y llevarla a aprobar a la junta directiva" (4, 3.2, 142).

> Casi todas las compañías se miden con COBIT[2], [...] para que tengan su proceso de gobierno que lo enmarca, su proceso de operación, su proceso de seguridad, su proceso de gestión, su proceso de riesgos, todo para Tecnologías de la información. (5, 3.5, 103)

Los entrevistados plantean que el comportamiento deseado de la organización se expresa en su *estructura organizacional* y la *asignación de recursos* como apoyo a la GR. Para ellos, es importante la definición de un gobierno para la GRC, que impulse la definición de unas políticas y unos marcos de actuación, facilitando la TD. Estos marcos generalmente están soportados en estándares internacionales, buscando las mejores prácticas a través de la definición de procesos, rendición de cuentas, recursos y acciones claras para toda la organización (Karake et al., 2017). La estructura organizacional que definen para gestionar el riesgo depende de la realidad e intención de cada organización, así como crear una fuerte cultura de seguridad, basada en el liderazgo correcto, en todos sus grupos de interés (Moon, 2021). En palabras de los entrevistados: "No hay una receta y cada compañía hace una interpretación distinta y por eso vas a encontrar muchísimos modelos [de GRC]" (7, 3.3., 119).

Enfoque en la gestión de riesgos

Otro elemento que influye en la TD es cómo opera la GR en la organización. Esto se ve reflejado especialmente en su nivel de madurez: *enfoque reactivo*, *enfoque preventivo* y *enfoque proactivo.* Según los entrevistados, en algunas organizaciones la consciencia para gestionar los riesgos ha surgido de los eventos materializados, pues desconocen el riesgo o lo subestiman y, entonces, la GRC no hace parte de su proceso de

[2] COBIT: Marco de referencia para la gobernanza y gestión de las tecnologías de información en la organización (Isaca, 2012)

gestión; su enfoque es *reactivo*, lo que las hace altamente vulnerables (Marotta & McShane, 2018). En palabras de un entrevistado: "Después de ese ataque en el que tuvimos la empresa todo el día sin correo... [...] Entonces fue ahí donde la empresa comenzó a tomar un poquito más de conciencia" (1, 4.1, 5).

Otros, por el contrario, manifiestan que comprendieron que el principal mecanismo es la prevención; es decir, la organización es consciente de que está expuesta a un riesgo y define que es necesario analizarlo e intervenirlo bajo unos marcos de actuación que apalanquen la gestión, por lo que su enfoque es preventivo. En palabras de uno de los entrevistados: "yo creo que lo más importante es trabajar en la prevención" (7, 4.3, 130).

Por último, hay organizaciones que tienen consolidado su proceso de GR, buscando mejorar continuamente sus controles y el entendimiento global del riesgo. En esa medida, analizan e implementan mejores prácticas a nivel mundial y comparten aprendizajes con sus homólogos, apalancándose en nuevas tecnologías; su enfoque es más *proactivo* (Marotta & McShane, 2018). En palabras de un entrevistado: "[...] estamos [buscando] cada día cómo mejoramos nuestro control, cómo mejoramos en la detección, y apoyándonos mucho con [...] inteligencia artificial y *machine learning*" (7, 4.2, 129).

Análisis del riesgo

Una adecuada GR busca entender y analizar los riesgos a los que se encuentra expuesta la organización (Sheppard et al., 2013). Los datos sugieren que, para implementar este proceso, es importante tener una clara *identificación de los riesgos*, una *valoración del riesgo* que facilite priorizarlos y contrastarlos con el *apetito del riesgo*, y así tomar mejores decisiones al momento de tratarlos. En palabras de un entrevistado:

> Estamos aprendiendo porque queremos valorar el riesgo cibernético como valorábamos el riesgo operativo [...]; ahí es donde tomar decisiones con base en la valoración de riesgos cibernético se convierte en una de las principales herramientas que podría tener. (7, 5.1, 132)

Los entrevistados conciben el riesgo desde tres agrupadores: tecnología, procesos y personas, lo cual es coherente con el enfoque de ciberresiliencia (Eling et al., 2021; Zhang et al., 2016). Asimismo, los caracterizan de acuerdo con la vulnerabilidad que deban proteger: seguridad, integridad, confidencialidad y disponibilidad de la información. Además, reconocen que, por las características del ciberriesgo, este puede trascender a otros riesgos como el incumplimiento normativo y el riesgo sistémico. En palabras de un entrevistado: "Nosotros concebimos el riesgo de seguridad de información en tres elementos: la tecnología, los procesos y las personas. Las tres cosas pueden ser fuente de riesgo y [...] control del riesgo" (4, 5.3, 141).

Tratamiento del riesgo

Seleccionar e implementar las medidas para abordar el riesgo es otro de los retos que enfrentan los decisores. Los entrevistados tienen en cuenta aspectos como el *nivel de respuesta* que tiene establecido la organización para la implementación de *controles tecnológicos*, *controles en los procesos* (incluye controles de las personas) así como *sensibilización, capacitación y entrenamiento* y *nivel de respuesta*. En palabras de dos entrevistados: "¿Cómo empiezo a generar acciones para mejorar los niveles de protección a nivel de mi mapa de riesgos, para que cada vez sea más cercano a los riesgos tolerables?" (7, 6.4, 130). "La primera barrera de protección es la persona, porque yo puedo tener el antivirus que quiera, [...] y a un empleado le llegó un correo de *phishing* y él da clic y ya" (4, 6.3, 143).

Los datos sugieren que para el tratamiento de los riesgos es importante tomar decisiones todos los días y en muchos ámbitos, idealmente desde un enfoque preventivo, gestionando elementos como la obsolescencia tecnológica y el manejo de vulnerabilidades; también, instalando salvaguardas desde el punto de vista de los empleados y salvaguardas desde aspectos técnicos (Zhang et al., 2016); además, reconociendo buenas prácticas como seguridad en capas, es decir, la organización debería ser redundante en los controles establecidos para protegerse. Asimismo, un elemento que puede favorecer el tratamiento del riesgo es la generación de redes con los proveedores de tecnología, industrias afines, gobierno y demás grupos de interés, como soporte a la gestión de la organización. En palabras de uno de los entrevistados: [...] cinco controles que son muy importantes, porque tienen cobertura en casi toda la organización: el *Firewall,* los IPS que es un sistema de prevención de intrusos [...], el antivirus, el sistema filtrado de navegación y el sistema de correo (8, 6.1, 188).

Además, es importante resaltar que el aspecto más valioso para todos los entrevistados fue la necesidad de promover una fuerte cultura de GR, que incentive el empoderamiento en la prevención y mitigación en ciberseguridad (Moon, 2021). En palabras de uno de los entrevistados: "Los empleados los tenemos también segmentados por grupos; no es lo mismo llevar un mensaje de cultura a un área que a otra" (4, 6.3, 164).

Mejoramiento continuo

La GR mejora continuamente a través del aprendizaje y la experiencia (ISO, 2018). Los datos sugieren que el *monitoreo* y la *auditoría* son herramientas que permiten identificar *lecciones aprendidas*, facilitando los ajustes necesarios a los procesos y las TD futuras.

Las lecciones aprendidas juegan un papel preponderante para enfrentar proactivamente el riesgo (Zeijlemaker et al., 2022). Según los entrevistados, las organizaciones reconocen en el monitoreo y las auditorías metodologías valiosas para comprender la efectividad de sus controles y el funcionamiento de sus procesos, con el fin de apalancar su TD y la conciencia de ciberseguridad. También, reconocen que es esencial tener una comprensión holística del entorno en el que se encuentran, para entender mejor sus sistemas de gestión y estar preparados al afrontar nuevos retos (Marotta & McShane, 2018). En palabras de un entrevistado:

> Se han contratado firmas importantes reconocidas en el medio [...]. Entonces, lógicamente, cuando te hacen una auditoría yo siempre lo miro por el lado de qué me van a detectar [...] yo siempre soy muy abierto a recibir todas esas sugerencias. (3, 7.2, 74)

Vulnerabilidad

El reconocimiento e identificación de las vulnerabilidades de una organización son necesarias para prevenir o mitigar la posibilidad de que se materialice un riesgo. Los datos sugieren que estas vulnerabilidades generalmente se encuentran asociadas a *las personas*, *los proveedores* y *la tecnología*, además del *desconocimiento a la exposición al riesgo.* En palabras de un entrevistado:

> En ciberseguridad, existen dos tipos de compañías: las que ignoran que están siendo atacadas y las que saben que están siendo atacadas, pero no saben que son vulnerables. [...] todas van a enfrentar un ciberataque. Las preguntas son: ¿cuándo? y ¿cómo van a reaccionar? (7, 8.4, 134)

La mayor preocupación de los entrevistados es la vulnerabilidad de las personas de la organización: "La cadena se rompe por el eslabón más débil y el eslabón más débil es el empleado" (2, 8.1, 46). Según

Zeijlemaker et al. (2022), un elemento clave para cerrar esta brecha consiste en reconocer la importancia del comportamiento humano al diseñar, construir y utilizar la tecnología y los sistemas de información para prevenir y mitigar efectivamente dichas vulnerabilidades y fortalecer una cultura proactiva de GRC.

Gestión de incidentes de ciberseguridad

Para enfrentar adecuadamente los ciberataques, es necesario realizar un exhaustivo *análisis de causas* y un *proceso forense*, que permita determinar y evaluar las *consecuencias e impactos de los incidentes*, además de establecer los *protocolos de atención.* En palabras de los entrevistados:

> [Cuando] se estabiliza [el] riesgo que tiene la organización, [...] se convoca una mesa para recoger todas las bitácoras y las experiencias, como qué funcionó y qué no, para generar reportes a los órganos de control [...] que incluyen el análisis forense más completo y más detallado, las acciones que se tomaron, las comunicaciones que se compartieron, las lecciones aprendidas. (8, 9.5, 182)

Finalmente, los entrevistados reportaron varias formas de ataque cibernético, como ingeniería social (2, 9.2, 50), *ransomware* (4, 9.2, 150), *phishing* (6, 9.2, 84), *malware* (8, 9.2, 173), entre otros, y reconocen que los RC son muy cambiantes. Esto requiere monitorear en el mundo nuevas amenazas de ciberseguridad: *deepfakes*, *smart contract hacking*, *machine learning poisoning* (Eling et al., 2021).

DISCUSIÓN

La creciente amenaza cibernética y el daño potencial causado por los ataques convierten este riesgo en tendencia mundial. Además, la necesidad de mejoramiento de los procesos de GRC y la TD bajo incertidumbre obliga a las organizaciones a ser más proactivas y a tomar iniciativas en el desarrollo de sus propias capacidades de defensa y respuesta para generar una sólida cultura y una estrategia de GRC adaptable, integrada y deliberada (Sheppard et al., 2013). Pero los factores humanos que intervienen en la TD, ampliamente estudiados en otros ámbitos (Kahneman & Klein, 2009), requieren una mayor comprensión en este (Proctor & Chen, 2015).

Los datos sugieren que los decisores analizan rápidamente los riesgos e impactos de las situaciones, por lo que las emociones (y sesgos), en ocasiones, complementan su razonamiento lógico en búsqueda de elecciones óptimas, lo cual es coherente con lo planteado en la literatura (Jalali et al., 2019; Proctor & Chen, 2015). Para estas elecciones, los decisores buscan la mayor cantidad de información disponible para disminuir su nivel de incertidumbre. En ausencia de esta información, la intuición se vuelve un factor importante para responder a la situación de riesgo (Ramrathan & Sibanda, 2017).

Además, la capacidad de una organización para gestionar efectivamente los riesgos y lograr su estrategia está determinada por el entendimiento y alineación con el contexto que la rodea (ISO, 2018). También su compromiso y acción gerencial se refleja en sus políticas, marcos de actuación, asignación de recursos, roles y responsabilidades claras y coherentes (Karake, 2017), teniendo en cuenta que es crucial promover una cultura de GRC alrededor del sentido común y la ética, como pilares que delimitan la forma en que se toman decisiones en la organización (Schwartz, 2011).

Por otra parte, en la TD para la GRC es relevante la madurez de la organización, considerando que lo ideal es promover una GRC que intervenga desde las etapas tempranas, es decir, ir un paso adelante para prevenir, alertar y blindarse ante un posible ataque (WEF, 2020). Además, se sugiere, a partir de los datos de las entrevistas, que es importante fomentar el mejoramiento continuo y la resiliencia, de forma tal que la organización logre llevar y mantener el riesgo en un nivel aceptable, y que adicionalmente sea capaz de adaptarse a las condiciones cambiantes a través de la detección, la anticipación y el aprendizaje para su gestión, lo que es coherente con lo planteado por Eling et al. (2021) y Zhang et al. (2016).

Igualmente, en la GRC, la etapa de valoración parece ser determinante para la TD en los entrevistados, para entender a profundidad el riesgo. De ahí que sería necesario identificar y analizar en la organización cuáles son sus activos e infraestructura crítica (*hardware*, *software* y redes), es decir, el dominio físico; adicional a esto, se debe integrar otros dominios como el informativo, el cognitivo y el social (Collier et al., 2013). Otro factor de éxito es lograr establecer una metodología de valoración y cuantificación, más allá de las usadas tradicionalmente en los riesgos operativos, que facilite establecer el nivel de criticidad ajustado y poder así contrastarlo con el apetito de riesgos de la organización para definir la aceptabilidad del riesgo y el nivel de respuesta óptimo (Eling et al., 2021).

Los datos sugieren que se pueden tener todos los controles y se puede estar acompañado de muy buenas herramientas tecnológicas, pero cada vez los ataques son mucho más sofisticados (Eling et al., 2021); por ejemplo, los ataques de día cero, que explotan vulnerabilidades desconocidas por la organización y los fabricantes de tecnología con grandes impactos para las organizaciones, dado que todos los controles de seguridad y la capacidad de reaccionar se ponen a prueba, pues no existe una vacuna u otro control que prevenga ese ataque (Zhang et al., 2016). Por eso, es importante reconocer que todas las organizaciones son susceptibles de enfrentar un ataque cibernético y que en ocasiones sus controles serán insuficientes, es decir, deberán estar preparadas para responder efectivamente (Kamiya et al., 2020). Durante la atención de incidentes de ciberseguridad, las habilidades y el conocimiento del equipo técnico y las tecnologías para identificar comportamientos o patrones de los vectores de ataque son preponderantes (Sheppard et al., 2013). Al parecer, estos acortan enormemente el análisis de causas, el proceso forense, es decir, la evaluación general de la situación, facilitando la mitigación y remediación del impacto (8, 9.4, 173). Adicionalmente, la interacción con otros expertos de ciberseguridad, con otras compañías y redes de inteligencia, parece ser un factor clave para entender qué puede estar pasando durante un ataque y atenderlo oportuna y efectivamente (Balawejder et al., 2019). Por eso, es relevante comprender mejor el proceso de toma de decisiones en la gestión de la ciberseguridad, desde la experiencia de los decisores.

Esquema cualitativo de la experiencia de TD en GRC

A continuación, con base en los hallazgos de este estudio, y siguiendo la metodología de Gioia et al. (2013) descrita en la sección medológica, se propone un esquema cualitativo que capta la experiencia de la TD en la GRC de los informantes en términos teóricos (figura 3). El esquema cualitativo está constituido por las categorías (recogidas en las figuras 1 y 2), articuladas de manera dinámica, y presenta tres escenarios de la TD en la GRC: administración del riesgo, enfrentar un ataque cibernético y aprendizaje.

Figura 3. Esquema cualitativo que representa la TD en la GRC desde la perspectiva de los decisores entrevistados. Fuente: elaboración propia con base en Gioia et al. (2013).

De acuerdo con la figura 3, desde la perspectiva de los decisores, la GRC se vive particularmente en tres escenarios: i) la administración del riesgo, ii) enfrentamiento de un ataque cibernético y iii) el aprendizaje. Sin embargo, la forma en la que los decisores enfrentan dichos escenarios siempre estará delimitada, de forma transversal, por factores personales como la *experiencia* y los factores que *movilizan sus decisiones*, y por factores del entorno como el *contexto de la organización* y su *enfoque de* GR, lo cual es congruente con lo planteado por Bashir et al. (2017). No obstante, esta propuesta descriptiva difiere de otras, como la de M'manga et al. (2019), que no tiene en cuenta factores organizacionales, sino solo factores internos al proceso cognitivo, y es normativa, pues se basa en la literatura (y no directamente en la experiencia de los decisores). En este sentido, la propuesta aquí presentada puede ser complementaria a la de M'manga et al. (2019).

Primer escenario: administración del riesgo

El primer escenario, la administración del riesgo, está enmarcado en las decisiones tomadas para identificar, valorar, prevenir y mitigar el riesgo, dado que los decisores se enfrentan a un sinnúmero de elecciones. Una de estas elecciones, y posiblemente la más importante, está relacionada con el *análisis de riesgos*, principalmente en el proceso de valoración, en el que determinar la probabilidad e impacto del riesgo, en muchas ocasiones, representa el primer obstáculo, dada la falta de información para evaluarlo (De Smidt & Botzen, 2018). Además, la imprevisibilidad y el rápido desarrollo del RC hacen que la etapa de identificación se dificulte aún más; por esta razón, la resiliencia se convierte en una estrategia útil para complementar la gestión de este tipo de riesgos, mediante la detección, anticipación y aprendizaje (Eling, et al., 2021; Zhang et al., 2016).

Otra elección que se da en el proceso de GRC está asociada al momento en que se definen y seleccionan las medidas de *tratamiento del riesgo* más apropiadas para la organización y, en consecuencia, cómo se asignarán los recursos (Kamiya et al., 2020). En consecuencia, el reto más importante que enfrenta el decisor parece ser equilibrar los costos de implementar las acciones con los beneficios esperados y garantizar un balance entre apetito y estado actual del riesgo (WEF, 2022). Sin embargo, es importante señalar que Jalali et al. (2019), en su estudio basado en un juego de simulación, no encontraron diferencia entre administradores expertos y novatos en la poca comprensión de mecanismos de retrasos potenciales en el desarrollo de capacidades en ciberseguridad, ni en los errores al lidiar con la incertidumbre de los incidentes cibernéticos, y lo explican por heurísticas que operan en ambos grupos. No obstante, los expertos aprendieron mejor la necesidad de una toma de decisiones proactiva mediante un proceso iterativo. Según los autores, estos hallazgos muestran la importancia de capacitaciones en habilidades de pensamiento sistémico y sientan bases para investigar sesgos mentales sobre las complejidades que implica la ciberseguridad.

Segundo escenario: Enfrentar un ataque cibernético

El segundo escenario es el momento de enfrentar un ataque cibernético. En este escenario se ponen a prueba todas las acciones definidas en el primer escenario y quedan expuestas todas las *vulnerabilidades* de la organización. Los datos sugieren que *gestionar un incidente de ciberseguridad* hace que los decisores usen de manera preponderante su intuición, conocimiento y *experiencia* para tratar de identificar el vector de ataque, contener el incidente y remediar la situación, lo cual es coherente con lo planteado por Moon (2021) en el campo de la administración de riesgos.

Para favorecer el proceso de gestión de un incidente, en algunas organizaciones se reconoce, como factor clave de éxito, la conformación de comités de crisis para la atención de incidentes de ciberseguridad. Este parece ser uno de los mecanismos más importantes, ya que facilita la TD consensuada en todos los niveles de la organización, tanto operativo, táctico, como estratégico, potenciando las capacidades dadas por su experticia y nivel de responsabilidad. Este comité para la TD ha sido tan relevante para algunas organizaciones que trascienden de lo reactivo a lo preventivo, es decir, han pasado de actuar únicamente cuando se materializa el riesgo a participar en la definición y análisis de las vulnerabilidades para actuar desde etapas tempranas (Balawejder et al., 2019). Esto es relevante toda vez que, en algunos estudios como el de Zeijlemaker et al. (2022) y Shreeve et al. (2021), los administradores estudiados en juegos de simulación tienden al pensamiento reactivo. En cambio, desde la perspectiva de los entrevistados, las organizaciones tienden a ser más conscientes respecto a la importancia de la prevención.

Durante el proceso de *gestión de incidentes* surge un aspecto muy interesante frente al papel de las emociones, es decir, los decisores entrevistados manifestaron emociones como lo que ellos llaman 'incertidumbre', por no saber qué está pasando; angustia y miedo, por no controlar la situación; culpa, por no haber detectado la vulnerabilidad a tiempo; frustración e intranquilidad, por no identificar la causa; "adrenalina" (8, 1.1, 185), como una sensación casi adictiva que impulsa a resolver situaciones, y "triunfo" y "alegría", cuando sí se identifica la situación amenazante. Todas estas emociones inhiben o facilitan la gestión del incidente, y en ocasiones sustituyen la racionalidad dependiendo de factores como la presión de tiempo, el grado de experiencia y la inteligencia emocional (Moon, 2021).

Tercer escenario: Aprendizaje

El tercer escenario está orientado a capitalizar el aprendizaje. Aquí la organización ya ha implementado las acciones propuestas para la administración del riesgo (primer escenario) o ha superado las presiones que conlleva enfrentar un ataque cibernético (segundo escenario) y se dispone a implementar el aprendizaje, para *mejorar continuamente*. Los entrevistados reconocen la necesidad de apoyarse en nuevas tecnologías como inteligencia artificial, *machine learning*, inteligencia de amenazas, entre otros, para brindar protecciones más sólidas (7, 6.1, 129-130). Sin embargo, no mencionan la necesidad de hacer frente a los delitos cibernéticos a través de redes colaborativas con el Estado, proveedores de tecnologías, con su cadena de suministro y los mismos empleados, dada la magnitud del impacto de este tipo de riesgo, al trascender las fronteras de la organización (WEF, 2022), asunto para tener en cuenta en las capacitaciones que se realicen con los administradores de riesgo.

Los decisores entrevistados también reconocen que existen otros factores que dificultan o favorecen la TD en la GRC. Entre los factores que dificultan está la vulnerabilidad de los empleados (*insiders*), quienes toman sus propias decisiones y se han convertido, probablemente, en el mayor reto para la organización (7, 8.1, 126). En este sentido, fomentar e incentivar una cultura de prevención es imperativo para los gestores de riesgo, tanto como explorar nuevas tecnologías para salvaguardar la organización (Lee, 2020). Con respecto a los factores que favorecen la GRC, se encuentra que los decisores reconocen en la autonomía un mecanismo que promueve una TD con menos presión y más confianza para enfrentar una situación, coincidiendo en ello con Balawejder et al. (2019).

CONCLUSIÓN

Este estudio responde al llamado a investigar elementos clave de la GRC (Eling et al., 2021). El esquema cualitativo de la TD en GRC presentado es un aporte necesario, novedoso y plausible al estudio de la gestión, en general, y de las TIC, en particular, desde la perspectiva de los decisores. Mediante este esquema se destacan factores intervinientes en la TD en la GRC. Estos factores son personales (movilizadores de decisiones, experiencia) y organizacionales (contexto organizacional y enfoque de GR), e influencian tres escenarios: administración del riesgo (análisis del riesgo, tratamiento del riesgo), enfrentamiento a un ataque cibernético (vulnerabilidad, gestión del incidente) y aprendizaje (mejoramiento continuo). Algunos de estos factores han sido reportados en la literatura revisada (Eling et al., 2021; Proctor & Chen, 2015; Ramrathan, & Sibanda, 2017), pero en esta propuesta se integran de manera novedosa, constituyendo un esquema cualitativo, lo cual establece una contribución significativa a la GRC.

Encontramos que puede ser de ayuda para la TD en GRC considerar el desarrollo de factores personales en los tomadores de decisiones como la inteligencia emocional (Moon, 2021), la formación de la intuición (Builes, 2022) y el análisis de las experiencias (Manrique & De Castro, 2019). Asimismo, es relevante considerar el contexto organizacional y un enfoque de GR preventivo, siendo importante un ambiente de aprendizaje y capacitación en el que los diferentes niveles jerárquicos conozcan los RC más críticos y la forma de prevenirlos, pues el eslabón más débil es cada empleado (Proctor & Chen, 2015), sin importar su nivel jerárquico. Así habrá una mejor articulación entre empleados y organización, posibilitando mayor flexibilidad, adaptabilidad y dimensionamiento para mitigar el riesgo de un incidente de ciberseguridad (She-

ppard et al., 2013). El ser humano, con la complejidad psicológica que implica, sigue siendo muy relevante en la TD organizacional, aunque exista un gran desarrollo tecnológico informacional, pues es quien debe liderar los procesos cibernéticos (Eling et al., 2021; Ramrathan & Sibanda, 2017).

Con el modelo cualitativo que presentamos, contribuimos a la comprensión de la TD en GRC, mostrando cómo se integran algunos aspectos psicológicos con factores organizacionales (Jalali et al., 2019). Esta aproximación interdisciplinaria puede contribuir a generar ciberresiliencia organizacional (Eling et al., 2021).

Como limitaciones y futuras líneas de investigación, señalamos la importancia de complementar el esquema cualitativo de TD en GRC propuesto con las experiencias de otros actores organizacionales de diferentes niveles jerárquicos. Asimismo, es importante tener en cuenta qué modificaciones tendría el esquema cualitativo en experiencias de situaciones de contingencia en las que el enfoque preventivo ya no es aplicable debido a la materialización del RC.

DECLARACIÓN DE CONFLICTOS DE INTERÉS

Los autores no manifiestan conflictos de interés institucionales ni personales.

REFERENCIAS BIBLIOGRÁFICAS

Balawejder, B., Dankiewicz, R., Ostrowska-Dankiewicz, A., & Tomczyk, T. (2019). The role of insurance in cyber risk management in enterprises. *Humanities and Social Sciences*, *24*(4), 19-32. http://doi.prz.edu.pl/pl/publ/einh/492

Banco Mundial. (2015). *Informe sobre el desarrollo mundial 2015: mente, sociedad y conducta*. Grupo Banco Mundial. https://www.worldbank.org/en/publication/wdr2015

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers & Security*, *65*, 153-165. https://doi.org/10.1016/j.cose.2016.10.007

Builes, I. (2022). *Pensamiento intuitivo, lógica y toma de decisiones*. Universidad EAFIT.

Collier, Z., Linkov, I., & Lambert, J. (2013). Four domains of cybersecurity: A risk-based systems approach to cyber decisions. *Environment Systems and Decisions*, *33*(4), 469-470. https://doi.org/10.1007/s10669-013-9484-z

Damasio, A. (2007). *El error de Descartes.* Crítica.

De Castro, A., Cardona, E., Gordillo, M., & Támara, S. (2007). Comprensión de la experiencia de ansiedad en un estudiante que pertenece a un grupo artístico de la Universidad del Norte de la ciudad de Barranquilla. *Psicología Desde el Caribe*, *19*, 49-80. https://www.redalyc.org/pdf/213/21301904.pdf

De Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 239-274. https://doi.org/10.1057/s41288-018-0082-7

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and future research directions. *Risk Management and Insurance Review*, *24*, 93-125. https://doi.org/10.1111/rmir.12169

Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? *European Journal of Operational Research*, 272(3), 1109-1119. https://doi.org/10.1016/j.ejor.2018.07.021

Gigerenzer, G. (2008). *Decisiones instintivas.* Ariel.

Gioia, D., Corley, K., & Hamilton, A. (2013). Seeking qualitative rigor in inductive research: Notes on the Gioia methodology. *Organizational research methods*, *16*(1), 15-31. https://doi.org/10.1177%2F1094428112452151

Giorgi, A. (2010). *The descriptive phenomenological method in psychology. A modified Husserlian approach.* Duquesne University Press.

Hernández, R., Fernández, C., & Baptista, P. (2006). *Metodología de la investigación*. McGraw-Hill.

Hersing, W. (2017). Managing cognitive bias in safety decision-making: Application of emotional intelligence competencies. *Journal of Space Safety Engineering*, *4*(3-4), 124-128. https://doi.org/10.1016/j.jsse.2017.10.001

Hogarth, R. (2010). Intuition: A challenge for psychological research on decision-making. *Psychological Inquiry*, 21(4), 338-353. https://doi.org/10.1080/1047840X.2010.520260

Hovav, A., & D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, *6*(2), 97-121. https://doi.org/10.1046/J.1098-1616.2003.026.x

International Organization for Standardization [ISO]. (2018). *ISO 31000: Risk management – Guidelines*. ISO. https://www.iso.org/standard/65694.html

Isaca, C. (2012). COBIT 5. Un marco de negocio para el gobierno y la gestión de las TI de la Empresa. Rolling Meadows. https://articulosit.files.wordpress.com/2013/07/cobit5-framework-spanish.pdf

Jalali, M., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, *28*(1), 66-82. https://doi.org/10.1016/j.jsis.2018.09.003

Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise: A failure to disagree. *American Psychologist*, *64*(6), 515-526. https://doi.org/10.1037/a0016755

Kamiya, S., Kang, J-K., Kim, J., Milidonis, A., & Stulz, R. (2019). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. [Fisher College of Business Working Paper No. 2018-03-004]. *Journal of Financial Economics (JFE)*, 1-78. http://dx.doi.org/10.2139/ssrn.3135514

Karake, Z., Shalhoub, R., & Ayas, H. (2017). *Enforcing cybersecurity in developing and emerging economies: Institutions, laws and policies*. Edward Elgar Publishing. https://doi.org/10.4337/9781785361333

Kordeš, U. (2009). The phenomenology of decision-making. *Interdisciplinary Description of Complex Systems*, 7(2), 65-77. http://indecs.eu/2009/indecs2009-pp65-77.pdf

Laverty, S. (2003). Hermeneutic phenomenology and phenomenology: A comparison and methodological considerations. *International Journal of Qualitative Methods*, 2(3), 21-35. https://doi.org/10.1177/160940690300200303

Lee, I. (2020). Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management. *Future Internet*, 12(9), 1-21. https://doi.org/10.3390/fi12090157

Levitt, H., Bamberg, M., Creswell, J., Frost, D., Josselson, R., & Suárez-Orozco, C. (2018). Journal article reporting standards for qualitative primary, qualitative meta-analytic, and mixed methods research in psychology: The APA publications and communications board task force report. *American Psychologist*, 73(1), 26-46. https://doi.org/10.1037/amp0000151

Madnick, S. (1978). Management policies and procedures needed for effective computer security. *Sloan Management Review*, *20*(1), 61-74. https://pubmed.ncbi.nlm.nih.gov/10239542/

M'manga, A., Faily, S., Mcalaney, J., Williams, C., Kadobayashi, Y., & Miyamoto, D. (2019). A normative decision-making model for cyber security. *Information and Computer Security*, *27*(5), 636-646. https://doi.org/10.1108/ICS-01-2019-0021

Manrique, H. (2019). *La toma de decisiones: entre la intuición y la deliberación.* Universidad EAFIT.

Manrique, H., & De Castro, A. (2019). Toma de decisiones: intuición y deliberación en la experiencia de los decisores. *Innovar*, *29*(73), 149-164. https://doi.org/10.15446/innovar.v29n73.78028

Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. *Risk Management and Insurance Review*, *21*(3), 435-452. https://doi.org/10.1111/rmir.12109

McAfee, J., & Haynes, C. (1989). *Computer viruses, worms, data diddlers, killer programs, and other threats to your system: What they are, how they work, and how to defend your PC, Mac or mainframe.* St. Martin's Press.

Moon, J. (2021). Effect of emotional intelligence and leadership styles on risk intelligent decision-making and risk management. *Journal of Engineering, Project & Production Management*, *11*(1), 71-81. https://doi.org/10.2478/jeppm-2021-0008

Proctor, R., & Chen, J. (2015). The role of human factors/ergonomics in the science of security: Decision-making and action selection in cyberspace. *Human Factors*, *57*(5), 721-727. https://doi.org/10.1177/0018720815585906

Ramrathan, D., & Sibanda, M. (2017). The impact of information technology advancement on intuition in organisations: A phenomenological approach. *The Journal of Developing Areas*, *51*(1), 207-221. https://doi.org/10.1353/jda.2017.0012

Schwartz, B. (2011). Practical wisdom and organizations. *Research in Organizational Behavior*, *31*, 3-23. https://doi.org/10.1016/j.riob.2011.09.001

Sheppard, B., Crannell, M., & Moulton, J. (2013). Cyber first aid: Proactive risk management and decision-making. *Environment Systems and Decisions*, *33*(4), 530-535. https://doi.org/10.1007/s10669-013-9474-1

Simon, H. (1987). Making management decisions: The role of intuition and emotion. *Academy of Management Perspectives*, *1*(1), 57-64. https://doi.org/10.5465/ame.1987.4275905

Shreeve, B., Hallet, J., Edwards, M., Anthonysamy, P., Frey, S., & Rashid, A. (2021). "So if Mr Blue Head here clicks the link..." Risk thinking in cyber security decision making. ACM Transactions on Privacy and Security, *24*(1), 1-29. https://doi.org/10.1145/3419101

Sunstein, C., & Thaler, R. (2017). *Un pequeño empujón.* Taurus.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

World Economic Forum [WEF]. (2020). *The Global Risks Report 2020*. WEF. https://www.weforum.org/reports/the-global-risks-report-2020.pdf

World Economic Forum [WEF]. (2022). *The Global Risks Report 2022*. WEF. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Zeijlemaker, S., Rouwette, E.A.J.A., Cunico, G., Armenia, S., Von Kutzschenbach, M. (2022). Decision-makers' understanding of cyber-security's systemic and dynamic complexity: Insights from a board game for bank managers. *Systems*, *10*(49), 1-25. https://doi.org/10.3390/systems10020049

Zhang, M., Wang, L., Jajodia, S., Singhal, A., & Albanese, M. (2016). Network diversity: A security metric for evaluating the resilience of networks against zero-day attacks. *IEEE Transactions on Information Forensics and Security*, *11*(5), 1071-1086. https://doi.org/10.1109/TIFS.2016.2516916