Cuadernos de RES PUBLICA en derecho y criminología
Nº 8 / 2026 ISSN: 2990-0697 DOI: 10.46661/respublica.13640.

Gobernanza de la seguridad corporativa en la era digital. Desafíos estratégicos y ciberamenazas en Colombia y América Latina

Corporate security governance in the digital age. Strategic challenges and cyber threats in Colombia and Latin America

Manuel Guillermo Carrascal Jacome
Universidad Militar Nueva Granada. Bogotá (Colombia)
manuel.carrascal@unimilitar.edu.co
ORCID: 0000-0001-5130-3229

Resumen

Este artículo analiza la gobernanza de la seguridad corporativa en la era digital, con énfasis en los desafíos estratégicos y las ciberamenazas en Colombia y América Latina. La investigación se fundamenta en la teoría de la gestión del riesgo, la cual sirve como marco analítico principal para comprender cómo las organizaciones identifican, evalúan y responden a los riesgos cibernéticos emergentes. Los resultados evidencian que la seguridad corporativa ha transitado de una función operativa a un componente estratégico de la gobernanza organizacional, lo que requiere una participación activa de la alta dirección. No obstante, persisten brechas significativas en la región, incluyendo limitadas capacidades en ciberseguridad, fragmentación regulatoria y una insuficiente integración entre seguridad y estrategia corporativa. Asimismo, los factores humanos y la cultura organizacional continúan siendo vulnerabilidades críticas. El estudio destaca la necesidad de modelos de gobernanza integrales que articulen la gestión del riesgo, la resiliencia, las capacidades tecnológicas y la cooperación regional.

Palabras clave: Gobernanza de la seguridad corporativa; Ciberseguridad; Gestión del riesgo; Transformación digital; Resiliencia organizacional; América Latina.

Abstract

This article analyzes corporate security governance in the digital era, focusing on strategic challenges and cyber threats in Colombia and Latin America. The research is grounded in risk management theory, which serves as the main analytical framework to understand how organizations identify, assess, and respond to evolving cyber risks. The findings reveal that corporate security has shifted from an operational function to a strategic component of organizational governance, requiring active involvement from top management. However, significant gaps persist in the region, including limited cybersecurity capabilities, regulatory fragmentation, and insufficient integration between security and corporate strategy. Additionally, human factors and organizational culture remain critical vulnerabilities.

Keywords: Corporate security governance; Cybersecurity; Risk management; Digital transformation; Organizational resilience; Latin America.

Cómo citar este trabajo: Carrascal Jacome, Manuel Guillermo. (2026). Gobernanza de la seguridad corporativa en la era digital. Desafíos estratégicos y ciberamenazas en Colombia y América Latina. *Cuadernos de RES PUBLICA en derecho y criminología, (8), 01–14.* https://doi.org/10.46661/respublica.13640.

Recepción: 14.06.2026 **Aceptación:** 18.06.2026 **Publicación:** 23.06.2026

1. Introducción

En el contexto de la transformación digital global, la seguridad corporativa ha evolucionado desde un enfoque tradicional centrado en la protección física hacia una concepción integral que incorpora dimensiones tecnológicas, informacionales y estratégicas. La creciente dependencia de infraestructuras digitales ha ampliado el espectro de riesgos, posicionando la ciberseguridad como un componente esencial de la gobernanza organizacional (Baldwin & Henkel, 2015; World Economic Forum, 2023).En este escenario, la gobernanza de la seguridad corporativa emerge como un campo clave para la toma de decisiones estratégicas, en tanto articula políticas, procesos y estructuras destinadas a gestionar riesgos complejos y dinámicos. La digitalización ha redefinido los marcos de control, requiriendo enfoques adaptativos que integren tecnología, regulación y gestión del riesgo (Von Solms & Van Niekerk, 2013; ISACA, 2020).

América Latina, y particularmente Colombia, enfrentan desafíos específicos en este ámbito debido a factores estructurales como la brecha digital, la debilidad institucional en algunos sectores y la creciente sofisticación de las ciberamenazas. Estos elementos generan un entorno de alta vulnerabilidad para las organizaciones, tanto públicas como privadas (CEPAL, 2022; BID, 2021).En términos generales, el incremento de ataques cibernéticos, como el ransomware, el phishing y las amenazas persistentes avanzadas (APT), evidencia la necesidad de fortalecer los modelos de gobernanza corporativa en seguridad. Las organizaciones ya no solo deben reaccionar ante incidentes, sino anticiparse mediante estrategias proactivas basadas en inteligencia y resiliencia (ENISA, 2023; Kshetri, 2021).

Desde una perspectiva teórica, la gobernanza de la seguridad corporativa se ha abordado desde distintos enfoques, incluyendo la teoría de la agencia, la gestión del riesgo y la gobernanza corporativa. Estos marcos permiten analizar cómo las organizaciones estructuran mecanismos de control y supervisión para proteger sus activos críticos (Jensen & Meckling, 1976; Power, 2007). El estado del arte evidencia un creciente interés en la integración de la ciberseguridad dentro de la gobernanza corporativa. Estudios recientes destacan la importancia del rol de la alta dirección y los consejos de administración en la supervisión de riesgos digitales, así como la necesidad de alinear la seguridad con la estrategia organizacional (Turel et al., 2017; Gordon et al., 2015).

Asimismo, investigaciones en el contexto latinoamericano han señalado limitaciones en la adopción de marcos internacionales de seguridad, debido a factores culturales, económicos y regulatorios. Esto sugiere la necesidad de enfoques contextualizados que respondan a las particularidades regionales (Gallego & Bueno, 2020; OAS, 2022). A nivel conceptual, la literatura coincide en la necesidad de abordar la seguridad corporativa desde una perspectiva multidimensional. En este sentido, el presente artículo se estructura a partir de tres categorías de análisis: (i) gobernanza de la seguridad corporativa, entendida como el conjunto de estructuras y procesos de dirección y control; (ii) ciberamenazas, como manifestaciones de riesgo en entornos digitales; y (iii) desafíos estratégicos, relacionados con la capacidad organizacional para responder y adaptarse a dichos riesgos (Von Solms & Van Niekerk, 2013; Kshetri, 2021).

Estas categorías permiten articular un análisis integral que vincula la dimensión normativa, tecnológica y estratégica de la seguridad corporativa. De esta manera, se supera una visión fragmentada del riesgo y se promueve un enfoque sistémico que integra gobernanza, gestión y resiliencia organizacional (World Economic Forum, 2023). No obstante, persiste una brecha significativa entre los avances teóricos y su implementación práctica en las organizaciones de Colombia y América Latina. Esta situación plantea interrogantes sobre la

efectividad de los modelos actuales de gobernanza frente a un entorno digital caracterizado por la incertidumbre y la complejidad.

En este contexto, la problemática central que orienta este estudio se expresa en la siguiente pregunta de investigación: ¿cómo se configura la gobernanza de la seguridad corporativa en la era digital frente a los desafíos estratégicos y las ciberamenazas en Colombia y América Latina? Como supuesto teórico, se plantea que una gobernanza de la seguridad corporativa basada en enfoques integrales y estratégicos fortalece la capacidad organizacional para anticipar, mitigar y responder a las ciberamenazas en entornos digitales complejos.

Para abordar esta problemática, el artículo se estructura en tres partes. En primer lugar, se desarrolla un análisis conceptual de la gobernanza de la seguridad corporativa en la era digital. En segundo lugar, se examinan las principales ciberamenazas y desafíos estratégicos en el contexto de Colombia y América Latina. Finalmente, se presentan reflexiones críticas y propuestas orientadas al fortalecimiento de la gobernanza de la seguridad en organizaciones de la región.

2. Marco Teórico

La seguridad corporativa se define como el conjunto de políticas, procedimientos, tecnologías y recursos humanos destinados a proteger los activos estratégicos de una organización, incluyendo tanto infraestructuras físicas como sistemas de información y procesos críticos. En este sentido, su evolución conceptual ha transitado desde enfoques reactivos hacia modelos integrales orientados a la gestión del riesgo y la resiliencia organizacional.

Desde una perspectiva contemporánea, la seguridad corporativa se articula con la gobernanza organizacional, en tanto implica procesos de dirección, control y toma de decisiones orientados a mitigar amenazas en entornos complejos. Este enfoque reconoce que los riesgos no son únicamente operativos, sino también estratégicos, lo que exige su incorporación en los niveles más altos de la organización (Power, 2007; ISACA, 2020). Es así, que para el desarrollo de este artículo, se adopta como marco analítico principal la teoría de la gestión del riesgo (*risk management theory*), la cual sostiene que las organizaciones deben identificar, evaluar y mitigar riesgos de manera sistemática para garantizar su sostenibilidad. Esta teoría permite comprender la seguridad corporativa como un proceso dinámico de anticipación y respuesta frente a amenazas, especialmente en entornos digitales caracterizados por la incertidumbre (Power, 2007).

La selección de la teoría de la gestión del riesgo se justifica en su capacidad para integrar dimensiones estratégicas, operativas y tecnológicas dentro de un mismo marco analítico. A diferencia de otros enfoques más limitados, esta teoría permite analizar la seguridad corporativa no solo como un sistema de control, sino como un elemento central de la gobernanza organizacional y la toma de decisiones estratégicas (Baldwin & Henkel, 2015).

En el desarrollo del análisis, esta teoría se aplicará mediante la identificación de las principales ciberamenazas, la evaluación de vulnerabilidades organizacionales y el análisis de las estrategias de gobernanza adoptadas por las organizaciones en Colombia y América Latina. De este modo, se busca evidenciar cómo la gestión del riesgo se traduce en prácticas concretas de seguridad corporativa en contextos digitales.

Diversos autores han abordado la teoría de la gestión del riesgo desde perspectivas complementarias. Power (2007) plantea que las organizaciones modernas operan en un entorno de “incertidumbre organizada”, donde la gestión del riesgo se convierte en un mecanismo fundamental de control y legitimidad institucional. Por su parte, ISO (2018) establece marcos estandarizados que orientan la implementación de sistemas de gestión del riesgo a nivel organizacional.

En el ámbito de la ciberseguridad, autores como Kshetri (2021) y Von Solms y Van Niekerk (2013) destacan que la gestión del riesgo es esencial para enfrentar amenazas digitales emergentes, dado que permite priorizar recursos y diseñar estrategias de protección basadas en el impacto y la probabilidadقوع de incidentes. Asimismo, Gordon et al. (2015) subrayan la importancia de vincular la gestión del riesgo con la gobernanza corporativa, especialmente en lo relacionado con la supervisión por parte de la alta dirección.

En conjunto, la literatura evidencia que la teoría de la gestión del riesgo constituye un marco amplio y robusto para analizar la gobernanza de la seguridad corporativa en la era digital. Su aplicación permite no solo comprender la naturaleza de las ciberamenazas, sino también evaluar la capacidad de las organizaciones para responder de manera estratégica y resiliente, lo cual es de vital importancia en contextos como el colombiano y latinoamericano, donde los desafíos estructurales amplifican los riesgos digitales.

3. MÉTODO

El presente artículo se enmarca en un enfoque cualitativo, dado que busca comprender e interpretar los fenómenos asociados a la gobernanza de la seguridad corporativa en la era digital, particularmente en relación con los desafíos estratégicos y las ciberamenazas en Colombia y América Latina. Este enfoque permite un análisis profundo de las dinámicas organizacionales y conceptuales, superando aproximaciones meramente cuantitativas centradas en la medición de variables.

Desde el punto de vista epistemológico, la investigación se sustenta en un paradigma interpretativo, el cual concibe la realidad social como una construcción compleja que debe ser analizada a partir de los significados, discursos y prácticas que emergen en contextos específicos. En este sentido, la seguridad corporativa es abordada como un fenómeno multidimensional que requiere ser comprendido desde su interacción con factores tecnológicos, estratégicos y organizacionales.

El método utilizado corresponde al análisis documental y teórico, basado en la revisión sistemática de literatura académica, informes institucionales y marcos normativos relacionados con la gobernanza de la seguridad y la ciberseguridad. La recolección de datos se realizó a partir de fuentes secundarias especializadas, incluyendo artículos científicos indexados, reportes de organismos internacionales y estándares reconocidos en la materia, lo que permitió construir un corpus teórico robusto y actualizado.

Para la interpretación de la información se empleó la hermenéutica como enfoque analítico, entendida como un proceso de comprensión e interpretación de textos que permite identificar significados, relaciones conceptuales y tendencias en la literatura. A través de este enfoque, se analizaron los discursos académicos sobre gobernanza, gestión del riesgo y ciberseguridad, permitiendo una lectura crítica y contextualizada de los aportes teóricos existentes.

Asimismo, el estudio incorpora un proceso de triangulación teórica basado en las categorías de análisis definidas: gobernanza de la seguridad corporativa, ciber amenazas y desafíos estratégicos. Esta triangulación permitió contrastar diferentes perspectivas teóricas y empíricas, fortaleciendo la validez del análisis mediante la convergencia de enfoques provenientes de la gestión del riesgo, la gobernanza corporativa y la ciberseguridad.

Finalmente, la articulación entre el enfoque cualitativo, el análisis hermenéutico y la triangulación de categorías posibilita una comprensión integral del fenómeno estudiado. Este diseño metodológico permite no solo describir las dinámicas de la seguridad corporativa en la era digital, sino también generar interpretaciones críticas y propuestas analíticas que contribuyan al fortalecimiento

de la gobernanza de la seguridad en el contexto latinoamericano.

4. Resultados

4.1. Análisis conceptual de la gobernanza de la seguridad corporativa en la era digital

La gobernanza de la seguridad corporativa en la era digital se configura como un campo de análisis emergente que articula principios de gobernanza organizacional, gestión del riesgo y ciberseguridad, en respuesta a la creciente complejidad de los entornos digitales. Este concepto supera la visión tradicional de la seguridad como una función operativa aislada, para posicionarla como un componente estratégico que incide directamente en la sostenibilidad organizacional. En este sentido, la literatura contemporánea destaca que la seguridad debe integrarse en los niveles más altos de toma de decisiones, particularmente en contextos caracterizados por la incertidumbre y la exposición constante a amenazas digitales (Power, 2007; World Economic Forum, 2023).

Desde una perspectiva conceptual, la gobernanza se entiende como el conjunto de estructuras, procesos y mecanismos mediante los cuales las organizaciones son dirigidas, supervisadas y controladas. Aplicada al ámbito de la seguridad corporativa, esta noción implica la formulación de políticas, la asignación de responsabilidades y la implementación de controles orientados a proteger los activos críticos. En este marco, la gobernanza de la seguridad no solo se limita a la gestión técnica de riesgos, sino que también abarca dimensiones estratégicas, éticas y regulatorias, lo que refuerza su carácter transversal dentro de la organización (Baldwin & Henkel, 2015; ISACA, 2020).

La transformación digital ha generado un cambio estructural en el entorno organizacional, incrementando la interdependencia entre sistemas tecnológicos y procesos de negocio. Este fenómeno ha ampliado significativamente la superficie de ataque, exponiendo a las organizaciones a ciberamenazas cada vez más sofisticadas y difíciles de detectar. En consecuencia, la gobernanza de la seguridad corporativa debe evolucionar hacia modelos más flexibles y adaptativos, capaces de responder a un entorno dinámico y altamente complejo (ENISA, 2023; Kshetri, 2021).

En este contexto, la seguridad corporativa adquiere un carácter transversal que impacta todas las áreas de la organización, desde la gestión operativa hasta la planificación estratégica. Esta transversalidad exige una articulación efectiva entre diferentes niveles organizacionales, especialmente entre la alta dirección, los responsables de tecnología y las áreas de gestión del riesgo. La literatura enfatiza que la falta de integración entre estas áreas puede generar brechas de seguridad significativas, aumentando la vulnerabilidad organizacional frente a incidentes cibernéticos (Gordon et al., 2015).

La adopción de un enfoque basado en la gestión del riesgo se consolida como un elemento central en la gobernanza de la seguridad corporativa. Este enfoque implica la identificación sistemática de amenazas, la evaluación de vulnerabilidades y la implementación de estrategias de mitigación orientadas a reducir el impacto de los incidentes. De acuerdo con diversos autores, la gestión del riesgo permite transformar la seguridad en un proceso continuo de anticipación y adaptación, en lugar de una respuesta reactiva a eventos adversos ; (Power, 2007).

La integración de la gestión del riesgo dentro de la gobernanza de la seguridad facilita la toma de decisiones informadas, al permitir priorizar recursos en función del nivel de exposición a amenazas. Este enfoque resulta particularmente relevante en entornos digitales, donde la velocidad de cambio y la aparición constante de nuevas vulnerabilidades requieren una capacidad organizacional de respuesta ágil y estratégica. En este sentido, la seguridad se convierte en un proceso dinámico que evoluciona en función de los riesgos emergentes (ISO, 2018; Kshetri, 2021).

Un aspecto fundamental de la gobernanza de la seguridad corporativa es el rol de la alta dirección y los órganos de gobierno. La literatura especializada coincide en que la participación activa de estos actores es determinante para garantizar la alineación entre las políticas de seguridad y los objetivos estratégicos de la organización. Esta participación no solo implica la aprobación de políticas, sino también la supervisión continua de los programas de seguridad y la asignación de recursos adecuados ; (Turel et al., 2017).

Asimismo, la gobernanza de la seguridad requiere la definición clara de roles y responsabilidades, lo que contribuye a una gestión más efectiva de los riesgos. La ambigüedad en las responsabilidades puede generar vacíos de control y dificultar la respuesta ante incidentes de seguridad. Por ello, los marcos de gobernanza recomiendan establecer estructuras organizacionales que faciliten la coordinación y la rendición de cuentas en materia de seguridad (ISACA, 2020).

En la era digital, la gobernanza de la seguridad corporativa también debe considerar el cumplimiento de marcos regulatorios y normativos. La proliferación de estándares internacionales, como ISO 27001, evidencia la necesidad de adoptar buenas prácticas que orienten la gestión de la seguridad de la información. Sin embargo, la implementación de estos estándares debe adaptarse a las características específicas de cada organización, evitando enfoques rígidos que limiten la capacidad de respuesta (ISO, 2018).

No obstante, diversos estudios advierten que la adopción de estándares internacionales no garantiza por sí misma una gobernanza efectiva. Es necesario que las organizaciones desarrollen capacidades internas que les permitan interpretar y aplicar estos marcos de manera contextualizada. En este sentido, la gobernanza de la seguridad debe entenderse como un proceso de aprendizaje organizacional continuo, más que como una simple adopción de normas (Baldwin & Henkel, 2015).

Desde una perspectiva sistémica, la gobernanza de la seguridad corporativa puede concebirse como un sistema socio-técnico que integra personas, procesos y tecnologías. Este enfoque reconoce que la seguridad no depende exclusivamente de soluciones tecnológicas, sino también de factores organizacionales y humanos que influyen en la gestión del riesgo (Von Solms & Van Niekerk, 2013).

La dimensión tecnológica de la seguridad es especialmente relevante en la era digital, dado que las infraestructuras críticas dependen cada vez más de sistemas interconectados. Sin embargo, la literatura enfatiza que la tecnología debe ser complementada con políticas organizacionales y prácticas de gestión adecuadas, para garantizar una protección efectiva frente a las ciberamenazas (ENISA, 2023).

En este contexto, la cultura organizacional se posiciona como un elemento clave en la gobernanza de la seguridad. La concienciación de los empleados y la formación continua en prácticas de seguridad contribuyen significativamente a la reducción de riesgos asociados al factor humano. Diversos estudios han demostrado que una cultura de seguridad sólida puede disminuir la probabilidad de incidentes relacionados con errores humanos (Kshetri, 2021).

Por otra parte, la gobernanza de la seguridad corporativa debe incorporar el concepto de resiliencia organizacional, entendido como la capacidad de anticipar, resistir y recuperarse de eventos adversos. Este enfoque resulta esencial en entornos digitales, donde las amenazas son inevitables y la capacidad de recuperación se convierte en un factor crítico de éxito (World Economic Forum, 2023). La resiliencia implica no solo la implementación de controles preventivos, sino también el desarrollo de capacidades de respuesta y recuperación. En este sentido, la gobernanza debe incluir planes de continuidad del negocio, gestión de incidentes y mecanismos de aprendizaje organizacional que permitan

mejorar continuamente las prácticas de seguridad (ISO, 2018).En el contexto de Colombia y América Latina, la gobernanza de la seguridad corporativa enfrenta desafíos particulares relacionados con limitaciones estructurales, como la escasez de recursos, la falta de talento especializado y las brechas regulatorias. Estos factores condicionan la capacidad de las organizaciones para implementar modelos robustos de gobernanza (CEPAL, 2022; OEA, 2022).

A pesar de estas limitaciones, la región también presenta oportunidades para fortalecer la gobernanza de la seguridad, especialmente a través de la adopción de buenas prácticas internacionales y el fortalecimiento de capacidades institucionales. La cooperación regional y el intercambio de conocimiento se configuran como estrategias clave para enfrentar las ciberamenazas de manera conjunta (BID, 2021).

En síntesis, la gobernanza de la seguridad corporativa en la era digital debe entenderse como un proceso dinámico, estratégico y multidimensional que integra la gestión del riesgo, la tecnología y la toma de decisiones organizacionales. Su fortalecimiento resulta fundamental para enfrentar los desafíos actuales y futuros en materia de ciberseguridad, particularmente en contextos emergentes donde los riesgos digitales se intensifican y diversifican (Power, 2007; World Economic Forum, 2023).

4.2. Ciberamenazas y desafíos estratégicos en Colombia y América Latina

En la era digital, las ciberamenazas se han consolidado como uno de los principales riesgos para las organizaciones, afectando tanto su operatividad como su reputación y sostenibilidad. Estas amenazas se caracterizan por su constante evolución, sofisticación y capacidad de adaptación, lo que dificulta su identificación y mitigación. En este contexto, la ciberseguridad deja de ser un problema técnico para convertirse en un desafío estratégico que requiere la intervención de los niveles más altos de la organización (ENISA, 2023; World Economic Forum, 2023).

Las ciberamenazas pueden definirse como acciones maliciosas dirigidas a comprometer la confidencialidad, integridad y disponibilidad de la información y los sistemas. Entre las más relevantes se encuentran el ransomware, el phishing, los ataques de denegación de servicio (DDoS) y las amenazas persistentes avanzadas (APT). Estas formas de ataque evidencian la creciente profesionalización del cibercrimen y su impacto en distintos sectores económicos (Kshetri, 2021).

En América Latina, el incremento de las ciberamenazas ha sido particularmente significativo en los últimos años, impulsado por la rápida digitalización de servicios y la expansión del comercio electrónico. Sin embargo, este crecimiento no ha sido acompañado por un fortalecimiento proporcional de las capacidades de ciberseguridad, lo que ha generado un entorno de alta vulnerabilidad para las organizaciones (BID, 2021; OEA, 2022).

Colombia, como parte de este contexto regional, enfrenta desafíos específicos relacionados con la protección de infraestructuras críticas y la gestión de riesgos digitales. La creciente adopción de tecnologías como la computación en la nube, el Internet de las cosas (IoT) y la inteligencia artificial ha ampliado la superficie de ataque, incrementando la exposición a amenazas cibernéticas (CEPAL, 2022).

Uno de los principales desafíos estratégicos radica en la falta de integración entre la ciberseguridad y la gobernanza organizacional. En muchas organizaciones, la seguridad continúa siendo percibida como una función técnica, lo que limita su capacidad de influir en la toma de decisiones estratégicas. Esta desconexión puede generar brechas significativas en la gestión del riesgo (Gordon et al., 2015).

Asimismo, la escasez de talento especializado en ciberseguridad constituye un obstáculo

importante para el fortalecimiento de las capacidades organizacionales. La demanda de profesionales capacitados supera ampliamente la oferta disponible, lo que dificulta la implementación de estrategias efectivas de protección y respuesta ante incidentes (World Economic Forum, 2023).

Otro desafío relevante es la falta de cultura organizacional en materia de seguridad. Diversos estudios han demostrado que el factor humano es uno de los principales vectores de riesgo, especialmente en ataques de ingeniería social como el phishing. La ausencia de programas de concienciación y capacitación incrementa la probabilidad de incidentes (Kshetri, 2021).

En este contexto, la gestión del riesgo se posiciona como un enfoque clave para abordar las ciberamenazas. Este enfoque permite identificar, evaluar y priorizar riesgos en función de su impacto potencial, facilitando la toma de decisiones estratégicas. Como se ha señalado, la seguridad corporativa moderna requiere un enfoque integral basado en la gestión del riesgo .La naturaleza transnacional de las ciberamenazas representa otro desafío significativo para los países de América Latina. Los ataques cibernéticos no reconocen fronteras, lo que dificulta su regulación y control a nivel nacional. Esto hace necesario fortalecer la cooperación internacional y los mecanismos de gobernanza global en materia de ciberseguridad (OEA, 2022).

Desde una perspectiva estratégica, las organizaciones deben adoptar enfoques proactivos que les permitan anticiparse a las amenazas, en lugar de limitarse a reaccionar ante incidentes. Esto implica el uso de inteligencia de amenazas, análisis predictivo y tecnologías avanzadas para la detección temprana de riesgos (ENISA, 2023). La inversión en ciberseguridad también constituye un desafío estratégico, especialmente en contextos donde los recursos son limitados. Las organizaciones deben tomar decisiones sobre la asignación de recursos en función de prioridades estratégicas, lo que requiere una adecuada evaluación del riesgo y del costo-beneficio de las medidas de seguridad (Gordon et al., 2015).

En América Latina, las brechas regulatorias representan un obstáculo adicional para el fortalecimiento de la ciberseguridad. Aunque algunos países han avanzado en la implementación de marcos normativos, aún persisten diferencias significativas en términos de regulación, lo que dificulta la armonización de prácticas a nivel regional (CEPAL, 2022). La adopción de estándares internacionales puede contribuir a reducir estas brechas, proporcionando un marco de referencia para la gestión de la seguridad. Sin embargo, su implementación debe adaptarse a las particularidades del contexto regional, evitando enfoques homogéneos que no consideren las diferencias estructurales entre países (ISO, 2018)

Otro aspecto relevante es la protección de infraestructuras críticas, como sistemas financieros, energéticos y de telecomunicaciones. Estos sectores son especialmente vulnerables a ataques cibernéticos debido a su alta dependencia tecnológica y su impacto en la estabilidad económica y social (BID, 2021). La resiliencia organizacional emerge como un elemento clave para enfrentar las ciberamenazas. Más allá de prevenir ataques, las organizaciones deben desarrollar capacidades para responder y recuperarse de manera efectiva, minimizando el impacto de los incidentes y garantizando la continuidad del negocio (World Economic Forum, 2023).

En el caso colombiano, se han realizado avances importantes en la formulación de políticas de ciberseguridad, pero aún existen desafíos en su implementación efectiva. La coordinación entre el sector público y privado, así como el fortalecimiento de capacidades institucionales, son elementos clave para mejorar la gestión de las ciberamenazas (OEA, 2022). La cooperación regional se configura como una estrategia fundamental para enfrentar los desafíos de la ciberseguridad. El

intercambio de información, la adopción de buenas prácticas y la coordinación de políticas pueden contribuir a fortalecer la capacidad de respuesta frente a amenazas comunes (BID, 2021).

En síntesis, las ciberamenazas y los desafíos estratégicos en Colombia y América Latina evidencian la necesidad de fortalecer la gobernanza de la seguridad corporativa desde un enfoque integral y contextualizado. La articulación entre gestión del riesgo, capacidades organizacionales y cooperación regional resulta esencial para enfrentar un entorno digital cada vez más complejo y desafiante (ENISA, 2023; World Economic Forum, 2023).

4.3. Propuestas, reflexiones y aportes para el fortalecimiento de la gobernanza de la seguridad

El fortalecimiento de la gobernanza de la seguridad corporativa en la era digital requiere una reconfiguración profunda de los enfoques tradicionales, orientada hacia modelos integrales que articulen la gestión del riesgo, la estrategia organizacional y la transformación digital. En este sentido, se propone avanzar hacia esquemas de gobernanza que integren la seguridad como un elemento central en la toma de decisiones, superando su tratamiento como una función técnica aislada. Esta integración resulta fundamental en contextos caracterizados por la incertidumbre y la creciente complejidad de las ciberamenazas (Power, 2007; World Economic Forum, 2023).

Una de las principales propuestas del presente estudio consiste en promover la incorporación de la ciberseguridad en los niveles más altos de la gobernanza organizacional, particularmente en los consejos de administración y la alta dirección. La evidencia sugiere que las organizaciones que integran la seguridad en su agenda estratégica presentan mayores niveles de resiliencia frente a incidentes cibernéticos. En este sentido, la participación activa de la alta dirección permite alinear las políticas de seguridad con los objetivos corporativos y fortalecer la asignación de recursos (Turel et al., 2017; Gordon et al., 2015).

Asimismo, se plantea la necesidad de adoptar un enfoque de gestión del riesgo como eje articulador de la gobernanza de la seguridad. Este enfoque permite priorizar amenazas, optimizar recursos y desarrollar estrategias de mitigación basadas en evidencia. Tal como se ha señalado, la seguridad corporativa moderna requiere identificar amenazas, evaluar vulnerabilidades y diseñar respuestas estratégicas de manera sistemática ; (ISO, 2018).

Otra propuesta relevante consiste en fortalecer la cultura organizacional en materia de seguridad. La evidencia demuestra que el factor humano continúa siendo uno de los principales vectores de riesgo, lo que hace indispensable implementar programas de formación, concienciación y gestión del cambio. Una cultura de seguridad sólida no solo reduce la probabilidad de incidentes, sino que también fortalece la capacidad de respuesta organizacional frente a eventos adversos (Kshetri, 2021).

En el ámbito tecnológico, se propone la adopción de soluciones avanzadas de ciberseguridad basadas en inteligencia artificial, análisis predictivo y automatización de procesos. Estas herramientas permiten mejorar la detección temprana de amenazas y optimizar la gestión de incidentes, contribuyendo a una gobernanza más efectiva. No obstante, su implementación debe estar acompañada de marcos de gobernanza que aseguren su uso adecuado y alineado con los objetivos organizacionales (ENISA, 2023).

Desde una perspectiva regional, es fundamental promover la cooperación entre países de América Latina para enfrentar las ciberamenazas de manera conjunta. La naturaleza transnacional de estas amenazas requiere mecanismos de coordinación que faciliten el intercambio de información, la armonización de políticas y el desarrollo de capacidades compartidas. En este sentido, la cooperación regional se configura como un

elemento estratégico para fortalecer la seguridad en la región (OEA, 2022; BID, 2021).

En el caso específico de Colombia, se propone fortalecer la articulación entre el sector público y privado en materia de ciberseguridad. La colaboración entre estos sectores permite aprovechar sinergias, compartir conocimientos y desarrollar estrategias más efectivas para la gestión de riesgos. Esta articulación es particularmente relevante en la protección de infraestructuras críticas y servicios esenciales (CEPAL, 2022).

Otra línea de acción consiste en el fortalecimiento de los marcos regulatorios y normativos en materia de ciberseguridad. Aunque se han logrado avances en la región, aún persisten brechas que limitan la efectividad de las políticas públicas. En este sentido, se propone avanzar hacia marcos regulatorios más robustos, coherentes y adaptados a las dinámicas del entorno digital (CEPAL, 2022).

En relación con la implementación de estándares internacionales, se sugiere adoptar un enfoque flexible que permita su adaptación a los contextos locales. Si bien estándares como ISO 27001 ofrecen marcos de referencia valiosos, su aplicación debe considerar las características específicas de cada organización y entorno. Esta adaptación es clave para garantizar su efectividad (ISO, 2018).

Desde una perspectiva estratégica, se propone incorporar el concepto de resiliencia organizacional como eje central de la gobernanza de la seguridad. La resiliencia implica no solo prevenir ataques, sino también desarrollar capacidades para responder y recuperarse de manera efectiva. Este enfoque resulta esencial en un entorno donde las amenazas son inevitables (World Economic Forum, 2023).

Asimismo, se plantea la necesidad de integrar la gestión de la seguridad en los procesos de transformación digital. La adopción de nuevas tecnologías debe ir acompañada de evaluaciones de riesgo y estrategias de seguridad que garanticen su implementación segura. Esta integración permite evitar vulnerabilidades asociadas a la digitalización acelerada (ENISA, 2023).

Otra reflexión importante se relaciona con la necesidad de desarrollar capacidades analíticas dentro de las organizaciones. La toma de decisiones en materia de seguridad requiere el uso de datos, indicadores y herramientas de análisis que permitan evaluar riesgos y medir la efectividad de las estrategias implementadas (Gordon et al., 2015).

En el ámbito académico, este estudio aporta a la consolidación de la gobernanza de la seguridad corporativa como un campo de investigación relevante, especialmente en contextos latinoamericanos. La integración de enfoques teóricos como la gestión del riesgo y la gobernanza corporativa permite avanzar en la comprensión de este fenómeno desde una perspectiva interdisciplinaria (Power, 2007).

Asimismo, el artículo contribuye a la literatura al proponer un marco analítico basado en tres categorías: gobernanza, ciberamenazas y desafíos estratégicos. Esta articulación permite un análisis integral del fenómeno, superando enfoques fragmentados que abordan la seguridad de manera aislada. Desde una perspectiva práctica, los resultados del estudio ofrecen orientaciones para la toma de decisiones en organizaciones públicas y privadas. Las propuestas planteadas pueden servir como base para el diseño de políticas, estrategias y programas de seguridad adaptados a las necesidades del contexto regional.

No obstante, es importante reconocer las limitaciones del estudio, especialmente en relación con el uso de fuentes secundarias y el enfoque teórico. Futuras investigaciones podrían complementar estos hallazgos mediante estudios empíricos que permitan validar las propuestas en contextos organizacionales específicos. En términos de investigación futura, se sugiere profundizar en el análisis de casos de estudio en Colombia y América Latina, así como explorar el impacto

de nuevas tecnologías en la gobernanza de la seguridad. Estas líneas de investigación pueden contribuir a enriquecer el conocimiento en este campo.

En conclusión, el fortalecimiento de la gobernanza de la seguridad corporativa en la era digital requiere un enfoque integral, estratégico y contextualizado. La articulación entre gestión del riesgo, cultura organizacional, tecnología y cooperación regional se configura como un elemento clave para enfrentar los desafíos actuales y futuros en materia de ciberseguridad (World Economic Forum, 2023; ENISA, 2023).

5. Discusión

Los resultados del presente estudio evidencian que la gobernanza de la seguridad corporativa en la era digital ha evolucionado desde un enfoque operativo hacia una dimensión estratégica, lo cual coincide con lo planteado por Power (2007) y el World Economic Forum (2023). Esta transformación responde a la creciente complejidad de las ciberamenazas y a la necesidad de integrar la gestión del riesgo en los niveles más altos de la organización. En este sentido, la seguridad deja de ser un asunto técnico para convertirse en un elemento clave de la sostenibilidad organizacional, lo que refuerza la pertinencia del enfoque adoptado en este artículo.

En relación con la teoría de la gestión del riesgo, los hallazgos confirman su relevancia como marco analítico para comprender la gobernanza de la seguridad corporativa. Tal como se ha señalado, este enfoque permite articular la identificación de amenazas, la evaluación de vulnerabilidades y la toma de decisiones estratégicas ; (ISO, 2018). Sin embargo, la discusión también revela que su implementación en contextos latinoamericanos enfrenta limitaciones estructurales, lo que sugiere la necesidad de adaptaciones contextuales.

Un aspecto relevante que emerge del análisis es la persistente brecha entre los avances teóricos y su aplicación práctica en las organizaciones. Aunque la literatura destaca la importancia de integrar la seguridad en la gobernanza corporativa, en muchos casos esta integración es limitada o inexistente. Este hallazgo coincide con Gordon et al. (2015), quienes señalan que la falta de participación de la alta dirección reduce la efectividad de las estrategias de ciberseguridad.

Asimismo, la discusión pone de manifiesto que la cultura organizacional constituye un factor crítico en la gestión de la seguridad. A pesar de los avances tecnológicos, el factor humano continúa siendo una de las principales fuentes de vulnerabilidad, lo que refuerza la necesidad de desarrollar programas de formación y concienciación. Este resultado es consistente con lo planteado por Kshetri (2021), quien destaca la importancia de la dimensión humana en la ciberseguridad.

En el contexto de Colombia y América Latina, los hallazgos evidencian que las ciberamenazas se ven amplificadas por factores estructurales como la brecha digital, la escasez de talento especializado y las debilidades regulatorias. Estos elementos limitan la capacidad de las organizaciones para implementar modelos efectivos de gobernanza de la seguridad, lo que coincide con los análisis de CEPAL (2022) y la OEA (2022).

Por otra parte, la discusión resalta la importancia de la cooperación regional como estrategia para enfrentar las ciberamenazas. Dado el carácter transnacional de estas amenazas, los esfuerzos aislados resultan insuficientes, lo que hace necesario fortalecer mecanismos de colaboración entre países. Este planteamiento se alinea con lo propuesto por el BID (2021), que enfatiza la necesidad de enfoques regionales en materia de ciberseguridad.

Un hallazgo significativo del estudio es la necesidad de adoptar enfoques proactivos en la gestión de la seguridad, basados en la anticipación de riesgos y el uso de inteligencia de amenazas. Este enfoque contrasta con prácticas tradicionales de carácter reactivo, que resultan insuficientes en entornos

digitales dinámicos. En este sentido, los resultados refuerzan las recomendaciones de ENISA (2023) sobre la importancia de la detección temprana y la prevención.

La discusión también permite identificar la relevancia de la resiliencia organizacional como complemento de la gestión del riesgo. En un entorno donde las amenazas son inevitables, la capacidad de respuesta y recuperación se convierte en un elemento crítico de la gobernanza de la seguridad. Este enfoque es consistente con las propuestas del World Economic Forum (2023), que destacan la resiliencia como un componente esencial de la ciberseguridad.

Desde una perspectiva teórica, el estudio contribuye a la integración de enfoques como la gobernanza corporativa, la gestión del riesgo y la ciberseguridad, ofreciendo un marco analítico que permite comprender la seguridad como un fenómeno multidimensional. Esta integración responde a la necesidad de superar enfoques fragmentados y avanzar hacia modelos más holísticos de análisis (Von Solms & Van Niekerk, 2013).

En síntesis, la discusión evidencia que la gobernanza de la seguridad corporativa en la era digital requiere un enfoque integral, estratégico y contextualizado. Si bien existen avances significativos en la literatura, persisten desafíos importantes en su implementación, especialmente en contextos latinoamericanos.

En este sentido, el estudio reafirma la importancia de fortalecer la articulación entre teoría y práctica, así como de desarrollar capacidades organizacionales que permitan enfrentar de manera efectiva las ciberamenazas (Power, 2007; World Economic Forum, 2023).

6. Conclusiones

La seguridad corporativa se ha consolidado como un componente esencial de la gobernanza organizacional en el entorno digital contemporáneo, en la medida en que las organizaciones dependen cada vez más de infraestructuras tecnológicas para su operación y sostenibilidad. Este estudio permitió evidenciar que la seguridad ya no puede ser concebida como una función técnica aislada, sino como un eje estratégico que atraviesa la toma de decisiones en todos los niveles organizacionales. En este sentido, su integración en la gobernanza corporativa resulta indispensable para enfrentar los riesgos emergentes asociados a la digitalización.

En el contexto de América Latina y particularmente en Colombia, el fortalecimiento de la gobernanza de la seguridad corporativa se configura como una prioridad estratégica para enfrentar los desafíos derivados de la transformación digital. Los hallazgos evidencian que, si bien se han logrado avances en la adopción de tecnologías y marcos normativos, persisten brechas estructurales que limitan la capacidad de respuesta frente a las ciberamenazas.

Estas limitaciones están asociadas a factores como la escasez de talento especializado, la fragmentación institucional y la insuficiente articulación entre actores públicos y privados.

El análisis desarrollado permitió confirmar la pertinencia de la teoría de la gestión del riesgo como marco analítico para comprender la gobernanza de la seguridad corporativa en la era digital.

Este enfoque facilita la identificación, evaluación y priorización de riesgos, permitiendo a las organizaciones adoptar decisiones estratégicas basadas en evidencia. No obstante, también se evidenció que su aplicación en contextos latinoamericanos requiere adaptaciones que consideren las particularidades económicas, culturales y regulatorias de la región.

Asimismo, el estudio destaca la importancia de la participación activa de la alta dirección en la gestión de la seguridad corporativa. La evidencia sugiere que las organizaciones que incorporan la ciberseguridad en sus estructuras de gobernanza presentan mayores niveles de resiliencia frente a

incidentes. En este sentido, la alineación entre seguridad y estrategia organizacional se configura como un elemento clave para fortalecer la capacidad de respuesta ante amenazas complejas.

Otro hallazgo relevante es la necesidad de fortalecer la cultura organizacional en materia de seguridad. El factor humano continúa siendo uno de los principales vectores de riesgo, lo que hace indispensable implementar estrategias de formación y concienciación que promuevan prácticas seguras dentro de las organizaciones. En este contexto, la gobernanza de la seguridad debe incorporar dimensiones culturales que complementen las soluciones tecnológicas.

Desde una perspectiva estratégica, el estudio resalta la importancia de adoptar enfoques proactivos y resilientes en la gestión de la seguridad corporativa. La capacidad de anticipar, resistir y recuperarse de eventos adversos se configura como un elemento central en entornos digitales caracterizados por la incertidumbre. En este sentido, la resiliencia organizacional emerge como un componente fundamental de la gobernanza de la seguridad.

Adicionalmente, se evidencia que la cooperación regional constituye un elemento clave para enfrentar las ciberamenazas en América Latina. La naturaleza transnacional de estos riesgos exige la articulación de esfuerzos entre países, así como el intercambio de información y buenas prácticas. En este contexto, el fortalecimiento de mecanismos de colaboración regional puede contribuir significativamente a mejorar la capacidad de respuesta frente a amenazas comunes.

La gobernanza de la seguridad corporativa en la era digital requiere un enfoque integral, estratégico y contextualizado que articule la gestión del riesgo, la cultura organizacional, la tecnología y la cooperación institucional. El fortalecimiento de estos elementos resulta esencial para enfrentar los desafíos actuales y futuros en materia de ciberseguridad, especialmente en contextos emergentes como el colombiano y latinoamericano, donde los riesgos digitales continúan en expansión y complejidad.

Referencias

BALDWIN, Robert., & HENKEL, Mary. (2015). Regulatory governance in a changing world. Oxford University Press.

Banco Interamericano de Desarrollo (BID). (2021). Ciberseguridad en América Latina y el Caribe: Riesgos, avances y el camino a seguir. https://www.iadb.org

CANO CUEVAS, Diego Fernando., VELANDIA PARDO, Elmers Freddy., CARRASCAL JACOME, Manuel Guillermo., & MOURE BLANCO, David. (2026). Human Firewall: Privacy Paradigms in the Face of the Technological Revolution. AI Influence on Governance and Law in the Digital Age https://doi.org/10.4018/979-8-3373-4480-5.ch006

Comisión Económica para América Latina y el Caribe (CEPAL). (2022). Transformación digital en América Latina: Desafíos y oportunidades. Naciones Unidas. https://www.cepal.org

DELGADO MORAN Juan. José. (2023). Perspectivas Criminológicas aplicadas a las Políticas de Seguridad Pública, en Caruso Fontán/ Macías Caro (dirs.), Nuevas tendencias y modernos peligros de la política criminal. Pp. 117-153. Tirant lo Blanch.

ENISA. (2023). ENISA Threat Landscape 2023. European Union Agency for Cybersecurity. https://www.enisa.europa.eu

FERNÁNDEZ OSORIO, Andrés. Eduardo., VILLALBA-GARCÍA, Luisa. Fernanda., & VELANDIA PARDO, Elmers. Freddy. (2024). Gobernanza policéntrica, big data e inteligencia artificial: herramientas para la seguridad ciudadana en Colombia. Revista Criminalidad, 66(3), 11-25. https://doi.org/10.47741/17943108.658

GORDON, Lawrence. A., LOEB, Martin. P., & ZHOU, Lei. (2015). The impact of information security breaches: Has there

been a downward shift in costs? Journal of Accounting and Public Policy, 34(5), 429–444. https://doi.org/10.3233/JCS-2009-0398

ISACA. (2020). COBIT 2019 framework: Governance and management objectives. ISACA. https://www.isaca.org

ISO. (2018). ISO 31000: Risk management – Guidelines. International Organization for Standardization.

ISO. (2022). ISO/IEC 27001: Information security, cybersecurity and privacy protection – Information security management systems. International Organization for Standardization.

JENSEN, Michael. C., & MECKLING, William. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of Financial Economics, 3(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

KSHETRI, Nir. (2021). Cybersecurity management: An organizational and strategic approach. Springer. https://doi.org/10.3138/9781487531249

MARTINO, Luigi. (2018). La quinta dimensione della conflittualità. L'ascesa del cyberspazio ei suoi effetti sulla politica internazionale. Politica e Società, [online] 1, pp.61–76. doi:https://doi.org/10.4476/89790.

MARTINO, Luigi. (2024). International Law, State Sovereignty and Competition in the Digital Age. *Rivista di filosofia del diritto internazionale e della politica globale*, Vol. 21, Nº. 2, 2024. https://dialnet.unirioja.es/descarga/articulo/10098952.pdf

MAZURIER, Pablo. Andrés, & PAYÁ SANTOS, Claudio. Augusto. (2018). *Amenazas híbridas: teoría de la hibridez y nuevo orden internacional.* Thomson Reuters Aranzadi.

NIST. (2020). Framework for improving critical infrastructure cybersecurity (Version 1.1). National Institute of Standards and Technology. https://www.nist.gov

Organización de los Estados Americanos (OEA). (2022). Informe de ciberseguridad en América Latina y el Caribe. https://www.oas.org

PAYÁ SANTOS, Claudio Augusto., MARTINO, Luigi., SANZ GONZÁLEZ, Roger., & DELGADO MORÁN, Juan José. (2026). Technological Gaps and Security: Challenges for Law Enforcement and Public Safety." AI Influence on Governance and Law in the Digital Age *(pp. 169-192). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-4480-5.ch007*

PAYÁ SANTOS, Claudio. Augusto; DELGADO MORÁN, Juan. José; MARTINO, Luigi; GARCÍA SEGURA, Luis, A.; DIZ CASAL, Javier, & FERNÁNDEZ RODRÍGUEZ, Juan, Carlos. (2023). Fuzzy Logic analysis for managing Uncertain Situations. Review of Contemporary Philosophy Vol 22 (1), 2023 pp. 6780 -6797. https://doi.org/10.52783/rcp.1132

PELTIER, Thomas. R. (2016). Information security policies, procedures, and standards: Guidelines for effective information security management. Auerbach Publications. https://doi.org/10.1201/9780849390326

PORTER, Michael. E., & HEPPELMANN, James. E. (2014). How smart, connected products are transforming competition. Harvard Business Review, 92(11), 64–88.

TAPIAS DIAZ, Fernando, y DELGADO MORAN Juan. José. (2017) "Lucha de realidad en Colombia" en Análisis de la seguridad internacional desde perspectivas académicas. Thomson Reuters Aranzadi.

TORRES GUARNIZO, Mauricio. Antonio., & VELANDIA-PARDO, Elmers. Freddy. (2022). The interrelationship of human rights and the environment from the human security perspective. *Revista Científica General José María Córdova*, *20*(37), 111–128. https://doi.org/10.21830/19006586.803