REVISTA MULTIDISCIPLINAR EPISTEMOLOGÍA DE LAS CIENCIAS

Volumen 3, Número 3
Julio-Septiembre 2026

Edición Trimestral

CROSSREF PREFIX DOI: 10.71112

ISSN: 3061-7812, www.omniscens.com

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 3
julio-septiembre 2026

Publicación trimestral
Hecho en México

La Revista Multidisciplinar Epistemología de las Ciencias acepta publicaciones de cualquier área del conocimiento, promoviendo una plataforma inclusiva para la discusión y análisis de los fundamentos epistemológicos en diversas disciplinas. La revista invita a investigadores y profesionales de campos como las ciencias naturales, sociales, humanísticas, tecnológicas y de la salud, entre otros, a contribuir con artículos originales, revisiones, estudios de caso y ensayos teóricos. Con su enfoque multidisciplinario, busca fomentar el diálogo y la reflexión sobre las metodologías, teorías y prácticas que sustentan el avance del conocimiento científico en todas las áreas.

Contacto principal: admin@omniscens.com

9773061781003

Cintillo legal

Revista Multidisciplinar Epistemología de las Ciencias Vol. 3, Núm. 3, julio-septiembre 2026, es una publicación trimestral editada por el Dr. Moises Ake Uc, C. 51 #221 x 16B , Las Brisas, Mérida, Yucatán, México, C.P. 97144 , Tel. 9993556027, Web: https://www.omniscens.com, admin@omniscens.com, Editor responsable: Dr. Moises Ake Uc. Reserva de Derechos al Uso Exclusivo No. 04-2024-121717181700-102, ISSN: 3061-7812, ambos otorgados por el Instituto Nacional del Derecho de Autor (INDAUTOR). Responsable de la última actualización de este número, Dr. Moises Ake Uc, fecha de última modificación, 1 julio 2026.

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 3, 2026, julio-septiembre

DOI: https://doi.org/10.71112/zjpvzb70

CIBERSEGURIDAD: PILAR ESTRATÉGICO CLAVE PARA LA RESILIENCIA, GOBERNANZA Y TRANSFORMACIÓN DIGITAL DE LA ORGANIZACIÓN EMPRESARIAL

CYBERSECURITY: KEY STRATEGIC PILLAR FOR RESILIENCE, GOVERNANCE AND DIGITAL TRANSFORMATION OF THE BUSINESS ORGANIZATION

Antonia del Carmen Madrid George

Panamá

DOI: https://doi.org/10.71112/zjpvzb70

Ciberseguridad: pilar estratégico clave para la resiliencia, gobernanza y transformación digital de la organización empresarial

Cybersecurity: key strategic pillar for resilience, governance and digital transformation of the business organization

Antonia del Carmen Madrid George[a,*]

amadridgeorge@gmail.com

https://orcid.org/0009-0005-7477-5954

[*]Autor de correspondencia: amadridgeorge@gmail.com, [a]Facultad de Administración de Empresas y Contabilidad Universidad de Panamá, Panamá

RESUMEN

La ciberseguridad, que se considera que es cada vez más importante para mantener la privacidad y la seguridad de los servicios de TI, ha sido reconocida por haber evolucionado desde una función técnica hasta un elemento estratégico clave en las organizaciones empresariales modernas, y en este caso se centra la atención en el papel en la transformación digital acelerada. Este documento pretende ser un análisis de la ciberseguridad como pilar estratégico total, explorando cómo representa un catalizador para la resiliencia de la organización, la gobernanza de la empresa y el aseguramiento de la transformación digital en un espacio de amenazas cibernéticas alta.

Metodológicamente, se lleva a cabo una revisión de literatura analítica-crítica que se apoya en la literatura académica indexada y que contribuye a vislumbrar las principales corrientes teóricas, las convergencias conceptuales y los vacíos en torno al fenómeno. Este análisis determina que la ciberseguridad es susceptible de ser analizada desde diferentes perspectivas

DOI: https://doi.org/10.71112/zjpvzb70

-recurso estratégico, capacidad dinámica, mecanismo de control, habilitador tecnológico- en las que se observa una fragmentación que dificulta el análisis holístico.

Los hallazgos indican que la ciberseguridad desempeña un importante papel en la resiliencia organizacional hasta el punto de influir positivamente en las capacidades de prevención, respuesta y recuperación ante incidentes; en la gobernanza corporativa, desde que se establece como responsabilidad estratégica de los altos directivos; y en la transformación digital, al ser un prerrequisito para la implementación segura de tecnologías emergentes. Aunque hay que hacer notar que también se vislumbran los enfoques simplistas que la limitan a función técnica o cumplimiento normativo. En este sentido, la principal contribución de la investigación es plantear una nueva conceptualización de ciberseguridad entendida como una capacidad organizacional transversal integradora que articula estrategia, riesgo e innovación. En resumen, la ciberseguridad se posiciona como un pilar estructural fundamental para la continuidad operativamente, la competitividad y la capacidad de cambio y adaptación de las organizaciones en la era digital.

Palabras clave: Ciberseguridad; resiliencia organizacional; gobernanza corporativa; transformación digital; gestión del riesgo.

ABSTRACT

Cybersecurity, which is considered as being more important to maintain the privacy and security of IT services, has been recognized by its evolution from a technical function that is a key strategic element in modern business organizations, and in this case it is central to it. Pay attention to the paper as it undergoes accelerated digital transformation. "This paper aims to analyze an analysis of cyber security as a total strategic pillar, exploring as it represents a catalyst for the resilience of the organization, the governance of the company and the assurance of the digital transformation into a space of high cyber security developments.

DOI: https://doi.org/10.71112/zjpvzb70

Methodologically, there is a review of analytical-critical literature that is based on indexed academic literature and that contributes to the visualization of the main theoretical corridors, conceptual convergences and gaps surrounding the phenomenon. This analysis determines that cyber security is likely to be analyzed from different perspectives - strategic recourse, dynamic capacity, control mechanism, technological enabler - and observes a fragment that makes holistic analysis difficult.

The findings indicate that cybersecurity plays a crucial role in organizational resilience to have a positive influence on the capabilities of prevention, response and recovery before incidents; in corporate governance, from which this is established as the strategic responsibility of our directing authorities; y in digital transformation, it will be a prerequisite for the secure implementation of emerging technologies. Please note that you can also see the simple fact that the limit has a technical or normative function. In this sense, the main contribution of the investigation is to plant a new conceptualization of cybersecurity intended as a transversal integrative organizational capacity that articulates strategy, performance and innovation.

In summary, cyber security is positioned as a fundamental structural pillar for operational continuity, competitiveness and change capacity and adaptation of organizations in the digital era.

Keywords: Ciberseguridad; organizational resilience; corporate governance; digital transformation; management of the riesgo.

Recibido: 2 septiembre 2026 | Aceptado: 17 septiembre 2026 | Publicado: 18 septiembre 2026

DOI: https://doi.org/10.71112/zjpvzb70

INTRODUCCIÓN

En la actualidad, en el contexto de una economía más y más digitalizada, la ciberseguridad ha dejado de ser un problema técnico relacionado únicamente con tecnologías informáticas para convertirse en un elemento estructural que determina la posibilidad de sobrevivir, desarrollarse y ser competitivo para las empresas. La rápida transformación digital, la incorporación masiva de tecnologías como la inteligencia artificial, la computación en nube y el Internet de las Cosas ha elevado de manera exponencial la superficie de exposición organizacional, aumentando la complejidad y frecuencia de riesgos cibernéticos.

En esa línea, los ciberataques no son ya eventos aislados, sino fenómenos sistemáticos que ponen en riesgo directamente la continuidad operativa, la reputación corporativa y la confianza de los stakeholders. Las entidades no solo sufren pérdidas económicas significativas, sino también impactos regulatorios y estratégicos que amenazan su posición en el mercado. Como resultado, la ciberseguridad aparece como una condición necesaria para la supervivencia organizacional, y no como un elemento accesorio o de soporte.

Sin embargo, a pesar de su cada vez más importancia, la literatura académica y la práctica empresarial muestran que existe una importante laguna conceptual. De hecho, muchas veces desde el análisis de la protección tecnológica o el cumplimiento regulatorio, percibiendo a la ciberseguridad como un fenómeno organizacional integral, se limita la comprensión de la misma. Esta dispersión teórica dificulta ver a ésta como la articuladora en conjunto con la resiliencia organizacional, la gobernanza corporativa y la transformación digital.

miras a la teoría, varios enfoques han contribuido en la explicación de modelos y elementos importantes para su comprensión. La importancia estratégica de la Teoría de Recursos y Capacidades, el carácter adaptativo de las capacidades dinámicas, la responsabilidad en la alta dirección considerada desde la gobernanza corporativa, y la consideración como facilitador de la innovación de los enfoques de transformación digital. No

obstante, tales contribuciones siguen siendo fragmentadas, sin conformar un cuerpo teórico que dé cuenta de la esencia del fenómeno en el contexto de las organizaciones actuales.

En tal contexto, el artículo pretende estudiar cómo la ciberseguridad puede ser considerada un pilar estratégico integrador de toda la estructura organizacional, en función de su aporte a la resiliencia operativa, a la gobernanza corporativa y a la habilitación segura de la transformación digital en ambientes de alto riesgo cibernético. Con ese fin, se utiliza un enfoque de revisión de la literatura crítico y analítico, para mapear las convergencias, tensiones y vacíos en la literatura.

La importancia de esta investigación reside en la urgencia de avanzar hacia una reconceptualización de la ciberseguridad que le permita superar su reducción técnica para posicionarse como una capacidad organizacional transversa. Desde este lugar, el artículo plantea una lectura abductiva que integre tanto la protección derivada de la ciberseguridad como la estructuración de una lógica en torno a la estrategia empresarial con la que pueda sostener estabilidad, control e innovación en un mundo de incertidumbre y complejidad informática.

Esta investigación tiene como objetivo aportar a la evolución de la teoría de la organización empresarial en las particulares de la era digital, proponiendo un marco desde el cual se pueda entender la ciberseguridad como un elemento clave en la conformación de organizaciones resilientes, con buena gobernanza y con capacidad para transformarse con seguridad.

Objetivo general:

Analizar la ciberseguridad como un pilar estratégico integral en la organización empresarial y evaluar su contribución esencial a la resiliencia operativa, la gobernanza corporativa eficaz y la habilitación segura de la transformación digital en entornos de alto riesgo cibernético.

Objetivos específicos:

Estudiar el potencial de la ciberseguridad para construir y mejorar la resiliencia organizacional, analizando el desempeño de los mecanismos identificados de prevención, detección, respuesta y recuperación ante incidentes cibernéticos que garantizan la continuidad del negocio.

Evaluar cómo se ha incorporado la ciberseguridad a los marcos de gobernanza corporativa, su alineación con la alta dirección, el consejo de administración y las políticas de gestión de riesgos para convertirse en una prioridad estratégica a nivel ejecutivo.

Identificar y evaluar cómo la ciberseguridad actúa como facilitadora y protectora clave de la transformación digital, permitiendo la adopción segura de tecnologías emergentes (IA, nube, IoT) sin poner en peligro la confidencialidad, la integridad y la disponibilidad de los activos críticos de una organización.

Justificación

En el actual escenario (2025-2026), la seguridad cibernética está pasando de ser una función técnica reactiva a un elemento fundamental de la estrategia empresarial. El vertiginoso avance de la transformación digital, la masiva adopción de inteligencia artificial, computación en la nube, Internet de las Cosas ha llevado a un crecimiento exponencial de la superficie de ataque, al tiempo que las amenazas cibernéticas siendo cada vez más sofisticadas, automatizadas con IA, atacando identidades y cadenas de suministros son una certeza estadística más que una posibilidad remota.

Los ciberataques provocan efectos catastróficos como pérdidas financieras millonarias, impacto reputacional a largo plazo, interrupción de operaciones críticas, multas regulatorias (GDPR, NIS2, leyes locales de protección de datos), y pérdida de confianza de clientes e inversores. Una variedad de informes y análisis recientes convergen en que las organizaciones que no hacen de la ciberseguridad un pilar estratégico están en riesgo de no sobrevivir o de un

severo crecimiento limitado en la era digital. Por tales razones, el presente artículo de revisión se torna oportuno y necesario ya que ayuda a evidenciar y fundamentar teóricamente el cambio de paradigma necesario de proteger la tecnología a gobernar el riesgo digital como ventaja competitiva, proponiendo un marco conceptual actualizado que sirva de apoyo a directivos, académicos y profesionales en las decisiones que deberán tomar para diseñar y moldear organizaciones resilientes, bien gobernadas y que puedan innovar con seguridad en un mundo de amenazas constantes y aumentativas.

Dimensión	Enfoque Teórico	Objetivo en la Organización
Resiliencia	Teoría de Sistemas Adaptativos	Garantizar la supervivencia ante ataques disruptivos.
Gobernanza	Agencia y Stakeholders	Asegurar la rendición de cuentas y el cumplimiento normativo.
Transformación	Agilidad Organizacional	Habilitar nuevos modelos de negocio (IA, Cloud) sin riesgos críticos.

Fuente: elaboración propia

Marco teórico

La ciberseguridad en la organización empresarial: fundamento conceptual y evolución estratégica

Se ha pasado en ciberseguridad de una idea técnico-operativa a una de una categoría estratégica en las empresas hoy. Aunque tradicionalmente se había asociado con la protección de infraestructuras informáticas, hoy día se entiende que es parte integral de la matriz organizacional, puesto que salvaguarda activos digitales que pueden ser críticos para la competitividad y la continuidad del negocio (Von Solms & Van Niekerk, 2013).

En cuanto a la estrategia, el ciber se puede ver a través de la lente de la RCV, que argumenta que las ventajas competitivas sostenibles provienen de recursos que son valiosos, escasos, difíciles de imitar y explotables organizacionalmente (Barney, 1991). De acuerdo con esto, las competencias superiores en ciberseguridad se consideran recursos estratégicos que

disminuyen las vulnerabilidades sistémicas y proveen a las empresas con una ventaja competitiva en el ciberespacio.

Sin embargo, sería insuficiente a nivel epistémico considerar que la seguridad informática se agota en una racionalidad instrumental. La transformación digital ha expandido la superficie de la vulnerabilidad de la organización y ha hecho que el riesgo cibernético se convierta en un riesgo corporativo estratégico (Bharadwaj et al., 2013). Así, la ciberseguridad se reafirma como una capacidad organizacional transversal, integrada en la arquitectura estratégica empresarial.

Ciberseguridad y resiliencia organizacional: capacidades dinámicas frente a la disrupción digital

La resiliencia del sistema se conceptualiza como la habilidad de predecir, absorber, adaptarse y recuperarse de perturbaciones (Lengnick-Hall et al., 2011). En el ámbito digital, los ciberataques son perturbaciones altamente sofisticadas que comprometen procesos críticos, reputación y el valor de la organización.

Desde la perspectiva de las capacidades dinámicas, la resiliencia se relaciona con la capacidad de la firma para reconfigurar recursos en respuesta a cambios en el ambiente externo (Teece, 2007). En este sentido, la ciberseguridad no sólo es preventiva, sino también adaptativa, al reforzar los mecanismos de detección, respuesta y aprendizaje organizacional.

La literatura reciente sugiere que las organizaciones con estrategias de ciberseguridad cohesionadas son más resilientes a los incidentes, atenuando los impactos financieros y de reputación (Boin & van Eeten, 2013). Sin embargo, una respuesta estrictamente reactiva limita la resiliencia a la recuperación del estado anterior. Fundamentalmente, la resiliencia digital debe entenderse como un proceso evolutivo en el que la vulnerabilidad se transforma en aprendizaje estratégico.

Por lo tanto, la ciberseguridad sirve como infraestructura organizacional que permite la continuidad operativa y la adaptación estratégica en un entorno de riesgo sistémico.

Ciberseguridad y gobernanza corporativa: del control técnico a la responsabilidad fiduciaria

La gobernanza corporativa es el sistema a través del que se dirigen y controlan las organizaciones (Shleifer & Vishny, 1997). En la era de la economía digital, el riesgo cibernético ahora reside como un tema de nivel ejecutivo, llevando la ciberseguridad desde la sala de servidores hasta la sala de juntas.

literatura en Gestión del Riesgo Empresarial (ERM) postula que los riesgos para la estrategia deben ser gestionados de forma integrada y alineados con la toma de decisiones corporativa (Power, 2007). A este respecto, la ciberseguridad no puede seguir siendo un área fragmentada dentro del departamento de TI, sino que tiene que formar una parte del sistema de gobernanza de la organización.

Recientes estudios indican que la supervisión activa del consejo en la ciberseguridad se relaciona con menores pérdidas asociadas a incidentes digitales (Li et al., 2018). No obstante, se mantiene una laguna conceptual entre responsabilidad formal y entendimiento estratégico del riesgo digital.

Críticamente, la falta de una gobernanza digital madura introduce una desconexión entre la estrategia corporativa y la superficie expuesta tecnológica, que erosiona la estructura organizacional. En consecuencia, la ciberseguridad tiene que ser considerada una responsabilidad fiduciaria estratégica, estrechamente relacionada con la sostenibilidad y legitimidad del negocio.

Ciberseguridad como habilitador estratégico de la transformación digital

La digitalización transforma modelos de negocio, estructuras organizativas y dinámicas de competencia (Vial, 2019). La adopción de tecnologías tales como inteligencia artificial,

computación en nube e Internet de las Cosas (IoT, por sus siglas en inglés) proporciona más oportunidades para innovar, al mismo tiempo que incrementa la complejidad del riesgo en el ciberespacio.

Desde la perspectiva de la estrategia digital, la adopción de tecnologías informa la necesidad de que capacidades tecnológicas se alineen con objetivos organizativos (Bharadwaj et al., 2013). Sin embargo, una arquitectura sólida de seguridad cibernética puede ayudar a que la digitalización no se convierta en una fuente de fragilidad estructural.

Los estudios empíricos indican que las organizaciones más maduras en ciberseguridad experimentan menores exposiciones a incidentes críticos al realizar procesos de transformación digital (Westerman et al., 2014). Esto implica que establecer la ciberseguridad como una disciplina no es un freno a la innovación, sino una condición para que esta pueda sostenerse.

En clave crítica, la tensión entre velocidad e innovación y profundidad en el control pide una gobernanza balanceada. Seguridad cibernética estratégica funciona como un mecanismo de equilibrio dinámico, asegurando la confidencialidad, integridad y disponibilidad de los activos críticos sin impedir la evolución digital.

Integración teórica: ciberseguridad como capacidad organizacional estructural

La combinación de los ejes resiliencia, gobernanza y transformación digital, es la que permite visibilizar la ciberseguridad como una capacidad estructural integradora de la arquitectura organizacional. A partir de la teoría de sistemas abiertos (Katz & Kahn, 1978), la organización mantiene una interacción constante con su ambiente. En la era digital, este ambiente esta influenciado por amenazas cibernéticas constantes. Entonces, la ciberseguridad opera como un mecanismo de regulación, que estabiliza al sistema organizacional ante la perturbación proveniente del medio.

En síntesis, la literatura converge en que:

Hay un consenso generalizado en la ciberseguridad el cual es de importancia estratégica para las organizaciones (Rauscher, 2017). De acuerdo con la Teoría de los Recursos y Capacidades, la ciberseguridad es un recurso estratégico que protege activos significativos y que tiene el potencial de formar una ventaja competitiva sostenible (Barney, 1991). No obstante, esta idea se queda corta si no se añade una dimensión dinámica que explique su adaptación a mediaciones digitales en transformación. En aquella línea, desde la perspectiva de las capacidades dinámicas actúa como una capacidad organizacional que se encuentra en constante evolución para hacer frente a amenazas emergentes (Teece, 2007).

Al mismo tiempo, la disciplina de la gobernanza corporativa ha ido incorporando a la seguridad cibernética como un factor crítico en la gestión y supervisión organizacional, implicando que el riesgo cibernético afecta fundamentalmente el valor de la firma y la confianza de los stakeholders (Shleifer & Vishny, 1997). Tal sincronización confirma que la ciberseguridad debe ser relegada desde los técnicos hacia la alta dirección, como un asunto estratégico. También, las investigaciones de transformación digital han indicado que ciberseguridad no únicamente protege, sino también habilita la innovación a través de dar las condiciones para la segura adopción de tecnologías emergentes (Vial, 2019). Sin una robusta arquitectura de seguridad, se puede decir que el proceso de digitalización es enterrado en una estructura insegura y que pone en duda su sustentabilidad.

Sin embargo, a pesar de estos avances teóricos, sigue habiendo un relevante huso epistemológico: la ciberseguridad sigue siendo tratada de manera fragmentaria y, en el mejor de los casos, como una función técnica o un requerimiento de cumplimiento. Esta limitación impide su desarrollo como una categoría de centralidad dentro de la teoría organizacional contemporánea. Por lo tanto, es necesario un movimiento hacia una conceptualización integradora que construya a la ciberseguridad como una capacidad organizacional transversal,

que articule estrategia, gobernanza y transformación digital en ambientes de altísima complejidad y riesgo.

Cuadro comparativo de teorías

Ciberseguridad, resiliencia, gobernanza y transformación digital

Teoría	Postulado central	Aplicación a la ciberseguridad	Aporte al estudio	Limitaciones críticas
Teoría de Recursos y Capacidades (RBV) (Barney, 1991)	Las ventajas competitivas provienen de recursos valiosos, raros, inimitables y organizables	La ciberseguridad se concibe como un recurso estratégico que protege activos críticos y genera ventaja competitiva	Permite posicionar la ciberseguridad como activo intangible clave en la organización	Tiende a ser estática; no explica adecuadamente entornos dinámicos de amenazas cibernéticas
Capacidades Dinámicas (Teece, 2007)	La empresa debe integrar, construir y reconfigurar capacidades frente a cambios del entorno	La ciberseguridad se interpreta como capacidad adaptativa (detección, respuesta, aprendizaje)	Explica la resiliencia organizacional frente a ciberataques	Difícil operacionalización empírica; ambigüedad conceptual
Teoría de Sistemas (Katz & Kahn, 1978)	La organización es un sistema abierto en interacción constante con su entorno	La ciberseguridad actúa como mecanismo regulador frente a perturbaciones externas (amenazas digitales)	Permite entender la ciberseguridad como componente estructural del sistema organizacional	Puede resultar demasiado abstracta; limitada capacidad explicativa para decisiones estratégicas
Gobernanza Corporativa	La empresa debe ser dirigida y controlada para	La ciberseguridad se integra como responsabilidad	Eleva la ciberseguridad a	Enfoque tradicional no contempla plenamente

(Shleifer & Vishny, 1997)	proteger intereses de stakeholders	del consejo y alta dirección	nivel estratégico y fiduciario	riesgos digitales emergentes
Gestión del Riesgo Empresarial (ERM) (Power, 2007)	Los riesgos deben gestionarse de forma integral y alineada a la estrategia	El riesgo cibernético se incorpora como riesgo estratégico dentro del sistema ERM	Facilita la integración de la ciberseguridad en la toma de decisiones organizacionales	Enfoque muchas veces formalista (compliance), no necesariamente efectivo en la práctica
Resiliencia Organizacional (Lengnick-Hall et al., 2011)	Capacidad de anticipar, resistir y adaptarse a disrupciones	La ciberseguridad fortalece la continuidad del negocio ante incidentes cibernéticos	Conecta ciberseguridad con sostenibilidad operativa	Puede enfocarse excesivamente en recuperación y no en transformación post-crisis
Estrategia Digital (Bharadwaj et al., 2013)	La estrategia empresarial se redefine a partir de la integración tecnológica	La ciberseguridad habilita la transformación digital segura	Integra tecnología, estrategia y riesgo en un mismo marco	Subestima la complejidad del riesgo cibernético en contextos reales
Transformación Digital (Vial, 2019)	Uso de tecnologías digitales para generar cambios organizacionales profundos	La ciberseguridad protege procesos, datos y modelos digitales emergentes	Permite analizar la relación entre innovación y seguridad	Suele tratar la ciberseguridad como elemento secundario
Teoría Institucional (DiMaggio & Powell, 1983)	Las organizaciones adoptan prácticas por presión normativa, mimética y coercitiva	La adopción de ciberseguridad responde a regulaciones, estándares y presión del entorno	Explica la difusión de prácticas de ciberseguridad en sectores empresariales	Puede reducir la ciberseguridad a cumplimiento, no a estrategia

Fuente: elaboración propia

DOI: https://doi.org/10.71112/zjpvzb70

Análisis del cuadro

El contraste de teorías muestra que la ciberseguridad, no es un planteamiento homogéneo, sino que se ha analizado bajo diferentes marcos teóricos que permiten ver aspectos el fenómeno de forma parcial. Esta multifocalidad conceptual representa, al mismo tiempo, una limitante y una ventaja: limita su conocimiento pleno, pero también propicia en la formación de una lectura crítica que la posiciona nuevamente como una capacidad organizacional ontológica.

Desde la perspectiva de la teoría de los recursos y capacidades (RBV) (Barney, 1991), la ciberseguridad puede considerarse como un recurso estratégico que protege activos críticos y que contribuye a la generación de ventajas competitivas sostenibles. No obstante, esta perspectiva posee un límite: su aproximación relativamente estática le resta capacidad explicativa frente a la naturaleza dinámica y evolutiva de las amenazas cibernéticas. En este sentido, la teoría de las capacidades dinámicas (Teece, 2007) incorpora en el análisis a la ciberseguridad como capacidad adaptativa que puede reconfigurarse en entornos digitales altamente volátiles. Sin embargo, la debilidad de esta radica en la imprecisión conceptual y en la dificultad para su correcta aplicación práctica.

Por otro lado, la teoría de sistemas (Katz & Kahn, 1978) provee una mirada integral al colocar a la organización como un sistema abierto que se encuentra en interacción constante con un ambiente donde los riesgos cibernéticos están en aumento. En ese sentido, la ciberseguridad desde esa mirada es un mecanismo regulativo que posibilita sostener el equilibrio organizacional frente a perturbaciones exteriores. Aun así, su nivel de abstracción restringe su utilidad para comprender elecciones estratégicas específicas en escenarios empresariales.

En el campo de la gestión organizacional, el gobierno corporativo (Shleifer & Vishny, 1997) y la teoría de agentes (Jensen & Meckling, 1976) dan lugar para que la ciberseguridad

sea impulsada desde lo técnico hacia lo estratégico. Estas teorías respaldan la supervisión necesaria para el consejo de administración y la alta dirección, ya que el riesgo cibernético impacta directamente en el valor organizacional y la confianza de los stakeholders. A manera de complemento, la gestión del riesgo empresarial (ERM) (Power, 2007) considera a la ciberseguridad bajo una visión de riesgos sistémica. Sin embargo, este enfoque muchas veces degenere en un formalismo en el cumplimiento, que no necesariamente mejora las capacidades de protección tangible

La teoría institucional (DiMaggio & Powell, 1983) provee una explicación adicional para la implementación de la práctica de ciberseguridad resultante de presiones normativas, coercitivas y miméticas. Esta perspectiva permite entender mejor la propagación de normas y regulaciones, pero tiene la tendencia a reducir la ciberseguridad a una práctica de legitimación externa más que a una integración genuina y estratégica.

En cuanto a la innovación organizativa, y bajo el punto de vista de la estrategia digital (Bharadwaj et al., 2013) e innovación digital (Vial, 2019), la ciberseguridad es un facilitador para la adopción tecnológica. Estas teorías muestran que la digitalización sin una célula robusta de ciberseguridad hace que la vulnerabilidad organizacional aumente. Sin embargo, la ciberseguridad es vista como un aspecto secundario que debe ser (re)considerado desde la lógica de innovación, sin reconocer plenamente su carácter estructural.

La vinculación entre la ciberseguridad y la protección de datos personales en el ámbito empresarial con la resiliencia organizacional (Lengnick-Hall et al., 2011) se evidencia en la capacidad de la empresa para prever, resistir y recuperarse ante interrupciones. Si esta mirada es necesaria para entender la continuidad del negocio, se corre el riesgo de observar a la recuperación como un fin, y no develar qué ocurre con la organización luego de la crisis.
Este análisis permite establecer un punto de vista crítico: la literatura hasta el momento no ha conseguido articular un marco teórico común que diera explicación a la ciberseguridad en su

totalidad. Existe una visión dividida, cada teoría configura una parte del asunto los recursos, las capacidades, el control, el riesgo, la innovación o la legitimidad, no obstante, ninguna teoría ha incorporado el fenómeno.

En contraposición, el presente estudio aboga por derribar esta fragmentación conceptual, considerando la ciberseguridad como una capacidad organizacional estratégica, tangencial y habilitadora, que balancea operacionalmente entre la resiliencia operativa con la gobernanza corporativa y con la transformación digital. En este sentido, la ciberseguridad pasa de ser un soporte técnico, o un requisito regulatorio, a convertirse en un pilar estratégico estructural, sin el cual no puede sostenerse la competitividad ni la rentabilidad económica de la organización empresarial en escenarios de alta incertidumbre cibernética.

METODOLOGÍA

Este estudio se enmarca en una perspectiva cualitativa, la cual se basa en una revisión bibliográfica de tipo analítica y crítica, dirigida a no sólo reunir información existente sino a problematizar, resignificar y articular los principales aportes teóricos a favor de la ciberseguridad en la empresa. Esta selección metodológica está en consonancia con la naturaleza del objeto de estudio: un fenómeno conceptual complejo que ha sido tratado fragmentariamente en diferentes corrientes, lo que demanda un abordaje integrador y no sólo descriptivo.

ello, la revisión no se basa en un resumen narrativo habitual, sino que está guiada por criterios de sistematicidad en la búsqueda y en la selección de fuentes, con el fin de lograr rigor académico, además de conservar un punto de vista crítico que posibilite la detección de vacíos epistemológicos y tensiones conceptuales en la literatura.

Se estructuró la estrategia de búsqueda, consultando bases de datos académicas de alta repercusión, tales como Scopus, Web of Science, ScienceDirect y Google Scholar que

garantiza el captar literatura de relevancia sustentada en la comunidad científica. La elección de estas fuentes no es aleatoria, sino que obedece a la necesidad de sustentar el análisis en investigaciones que posean estándares de calidad y visibilidad internacional.

Para la detección de estudios se emplearon combinaciones con los términos en inglés y en español cybersecurity, corporate governance, organizational resilience, digital transformation y sus respectivos términos en español unidos por operadores booleanos. Con esta táctica se logró acotar el contexto del estudio y evitar una dispersión temática que hiciera difuminar el objetivo de investigación.

El proceso de selección estuvo regido por criterios de inclusión y exclusión explícitos. Se seleccionaron principalmente artículos científicos publicados en revistas indizadas, correspondientes principalmente al período enero de 2010 a diciembre de 2024, cuando la ciberseguridad fue adquiriendo relevancia estratégica en el marco de transformación digital. Sin embargo, se incluyeron autores clásicos cuando estos fueran necesarios para fundamentar el marco teórico. Se descartaron aquellos estudios de carácter técnico, pues no contribuían a la comprensión organizacional del fenómeno, así como documentos no arbitrados académicamente o con baja calidad metodológica. Esta limitación es una decisión epistemológica, poner foco en la ciberseguridad como categoría organizacional y no como un problema tecnológico aislado.

El análisis informacional consistió en la lectura crítica y categorización temática. Se llevó a cabo una revisión inicial exploratoria para evaluar la idoneidad de los textos a partir de títulos y resúmenes. Después, se realizó una lectura profunda para extraer las teorías, los conceptos principales y la dinámica de las variables centrales del estudio: resiliencia, gobernanza y transformación digital. Finalmente, los resultados se organizaron en categorías analíticas que sostuvieron la construcción de una síntesis integradora.

Cabe la importante advertencia de que el análisis no se centra únicamente en identificar convergencias en la literatura, sino también en mostrar carencias. En este sentido, el estudio toma distancia para afirmar que la mayoría de los análisis revisados se aproximan a la ciberseguridad a partir de enfoques fragmentarios en torno al cumplimiento normativo, a la gestión del riesgo, a la protección tecnológica, sin que logren instalarla como una categoría nodal en el pensamiento organizacional. Esta afirmación hace necesaria una relectura en la que dichas dimensiones queden articuladas en una interpretación más amplia.

Los criterios de selección, el uso de fuentes académicas de alta calidad y la triangulación de marcos teóricos garantizan la calidad metodológica y están explícitamente referidos en la investigación. Sin embargo, se contempla como limitación la dependencia de fuentes secundarias y la naturaleza interpretativa del análisis, lo que conlleva a que los hallazgos se ven influenciados por la óptica del investigador. Esta condición no sólo no invalida el estudio sino es coherente con el enfoque cualitativo que se adoptó y con las intenciones de producir una lectura crítica del campo. En resumen, la metodología utilizada permite no sólo hacer una revisión del marco teórico, sino también realizar una re conceptualización de la ciberseguridad moviendo desde una focalización técnica para verla como una capacidad organizacional estratégica, en consistencia con la finalidad general del estudio.

DISCUSIÓN

Los resultados de la revisión de literatura pueden concluir que la ciberseguridad ha evolucionado conceptualmente, pasando de ser una función técnica dependiente del área de tecnologías de la información a ser una capacidad estratégica de primer nivel en la organización de negocios. Sin embargo, esta transformación no se ha traducido en una homogeneización teórica que muestre que existen diferencias en la forma en la que el fenómeno es tratado en la literatura.

En el marco de la Teoría de Recursos y Capacidades (Barney, 1991), la ciberseguridad se define como un recurso estratégico que salvaguarda activos críticos y apoya sustancialmente la sustentabilidad de la ventaja competitiva. Esta conceptualización, no obstante, resulta insuficiente para abarcar la dinámica de la ciber amenaza. Aquí es donde entra en escena la teoría de las capacidades dinámicas (Teece, 2007), que amplía el debate para considerar la ciberseguridad como una capacidad dinámica que permite a las organizaciones adaptarse a entornos digitales cambiantes. La sinergia entre estas dos perspectivas implica que la ciberseguridad, no sólo debería ser acumulada como recurso, sino ser desarrollada como capacidad dinámica.

No cabe duda que los resultados apoyan que la ciberseguridad es un elemento estructural en la continuidad del negocio en cuanto a resiliencia organizacional. Sin embargo, se nota una inclinación en la literatura a favorecer perspectivas reactivas de recuperación post incidente que reducen la atención en las transformaciones resilientes. Esta laguna reduce la inteligencia de la ciberseguridad como un proceso de aprendizaje organizacional para fortalecer la estrategia de adaptación luego de eventos disruptivos.

Por el contrario, el análisis muestra una evolución respecto a la integración de la ciberseguridad en la gobernanza corporativa, especialmente en cuanto a su consideración como riesgo estratégico. La integración del asunto en la agenda del consejo de administración y su conexión a la gestión de riesgos global es un paso adelante. Sin embargo, aún existe una diferencia entre la aprobación de políticas y la escaza implementación, lo que demuestra que, en definitiva, en muchos casos la ciberseguridad sigue siendo vista más como un requisito normativo que como un factor relevante para la toma de decisiones estratégicas o del negocio.

En relación a la digitalización, los autores coinciden en señalar que la ciberseguridad es un facilitador clave de la innovación. La implementación de tecnologías emergentes sin la debida seguridad expone a la organización a riesgos sistémicos que pueden poner en peligro la

sostenibilidad de su digitalización. No obstante, se aprecia cierta tendencia a subordinar la ciberseguridad a la lógica de innovación sin tener en cuenta su naturaleza estructural, lo que se podría traducir en una estrategia poco equilibrada.

En conjunto, estos hallazgos permiten sostener que la principal limitación del campo radica en su fragmentación teórica. La ciberseguridad es abordada desde múltiples enfoques recurso, capacidad, riesgo, cumplimiento o habilitador tecnológico sin una integración conceptual que capture su complejidad. Esta dispersión impide su consolidación como una categoría central dentro de la teoría de la organización empresarial.

Frente a esta limitación, el presente estudio propone una reinterpretación de la ciberseguridad como una capacidad organizacional transversal e integradora, que articula simultáneamente resiliencia, gobernanza y transformación digital. Esta perspectiva permite superar los enfoques reduccionistas y avanzar hacia una comprensión más completa del fenómeno en contextos de alta incertidumbre cibernética.

CONCLUSIONES

El objetivo del presente estudio era examinar la ciberseguridad como pilar estratégico de la organización empresarial y sus aportaciones a la resiliencia operacional, a la gobernanza corporativa y a la transformación digital. De las revisiones bibliográficas realizadas se tienen, lo siguiente:

Primer se concluye que la ciberseguridad es un recurso estratégico y se constituye como una capacidad organizacional dinámica, que va más allá de la protección tecnológica para impactar en la sustentabilidad y la competitividad del negocio empresarial. Además, al gestionar de manera efectiva el riesgo se fortalecen las fortalezas de la organización en un entorno digital complejo.

En segundo lugar, se demuestra que la ciberseguridad es la base clave para asegurarse de que las organizaciones puedan anticipar, responder y recuperarse de los incidentes cibernéticos. Sin embargo, su potencial de transformación sólo llega a la práctica cuando se articula en procesos de aprendizaje organizacional, más allá de estrategias puras de recuperación operativa.

En tercer lugar, la investigación demuestra que la ciberseguridad debe establecerse como un área de la gobernanza corporativa enderezando a la alta dirección y al consejo de administración a empatarlos de manera directa. Su integración en los sistemas de gestión de riesgos y decisiones estratégicas es crucial para mantener la estabilidad y legitimidad organizacional.

Cuarto, se concluye que la ciberseguridad es un habilitador clave de la transformación digital, ya que es responsable de establecer los requisitos mínimos para la adopción segura de tecnologías emergentes. En este sentido, no es una barrera para la innovación, es un elemento estructural que la sostiene.

Teóricamente, la principal contribución del estudio se encuentra en la conceptualización integrada de la ciberseguridad como una capacidad organizacional transversal, evitando una oferta dispersa tratada desde la literatura. Esta reconceptualización aporta a la construcción de la teoría de organización de la empresa en contexto digital.

Por último, se plantea una agenda de futuras investigaciones que permita validar el modelo propuesto y profundizar en la relación entre ciberseguridad, cultura organizacional y desempeño empresarial. También se recomienda investigar mecanismos de gobernanza que permitan acercar la brecha en la toma de decisiones estratégicas y la ejecución efectiva en ciberseguridad.

La ciberseguridad se establece no sólo como un requisito operativo, sino como un pilar estructural de la organización empresarial actual que precisa para su resiliencia, gobernanza y transformación digital en ambientes de complejidad creciente y riesgo cibernético.

Declaración de conflicto de interés

Declaro no tener ningún conflicto de interés relacionado con esta investigación.

Declaración de contribución a la autoría

Declaración de contribución a la autoría Antonia del C. Madrid George: metodología, conceptualización, redacción del borrador original, revisión y edición de la redacción.

Declaración de uso de inteligencia artificial

La autora declara que utilizo la Inteligencia Artificial como apoyo para este artículo, y que esta herramienta no sustituyó de ninguna manera la tarea o proceso intelectual, manifiesta y reconoce que este trabajo fue producto de un trabajo intelectual propio, que no ha sido publicado en ninguna plataforma electrónica de inteligencia artificial.

REFERENCIAS

Barney, J. (1991). Firm resources and sustained competitive advantage. Journal of Management, 17(1), 99–120. https://doi.org/10.1177/014920639101700108

Bharadwaj, A., El Sawy, O., Pavlou, P., & Venkatraman, N. (2013). Digital business strategy: Toward a next generation of insights. MIS Quarterly, 37(2), 471–482.

Boin, A., & van Eeten, M. (2013). The resilient organization. Public Management Review, 15(3), 429–445.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American Sociological Review, 48(2), 147–160. https://doi.org/10.2307/2095101

Jensen, M. C., & Meckling, W. 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

Katz, D., & Kahn, R. (1978). The social psychology of organizations (2nd ed.). Wiley.

Lengnick-Hall, C., Beck, T., & Lengnick-Hall, M. (2011). Developing a capacity for organizational resilience. Human Resource Management Review, 21(3), 243–255.

Li, T., No, W., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. International Journal of Accounting Information Systems, 30, 40–55.

Power, M. (2007). Organized uncertainty: Designing a world of risk management. Oxford University Press.

Rauscher, H. (2017). Cybersecurity: The strategic imperative for business and government. Routledge.

Shleifer, A., & Vishny, R. (1997). A survey of corporate governance. Journal of Finance, 52(2), 737–783.

Teece, D. (2007). Explicating dynamic capabilities. Strategic Management Journal, 28(13), 1319–1350.

Vial, G. (2019). Understanding digital transformation. Journal of Strategic Information Systems, 28(2), 118–144.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers & Security, 38, 97–102.

Westerman, G., Bonnet, D., & McAfee, A. (2014). Leading digital. Harvard Business Review Press.