REVISTA CIENTÍFICA
Ciencia y Método
ISSN 3103-1072

EDITORIAL GRUPO AEA

Artículo Científico

La ciberseguridad como prioridad empresarial dentro de marcos los regulatorios y normativos internacionales

Cybersecurity as a business priority within international regulatory and policy frameworks

Choez-Calderón, Cindy Johanna [1]
https://orcid.org/0000-0003-3968-9397
cindy.choez.calderon@utelvt.edu.ec
Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador, La Concordia.

Aldo-Patricio, Mora Olivero [2]
https://orcid.org/0000-0002-4337-7452
aldo.mora.olivero@utelvt.edu.ec
Universidad Técnica Luis Vargas Torres de Esmeraldas, Ecuador, La Concordia.

Autor de correspondencia [1]

DOI / URL: https://doi.org/xxxxxx

Resumen: El estudio examina críticamente cómo la ciberseguridad se ha convertido en una prioridad estratégica empresarial ante la proliferación de amenazas digitales y la creciente fragmentación normativa internacional. Mediante un enfoque exploratorio de revisión bibliográfica, se recopilaron y analizaron publicaciones científicas, informes técnicos y regulaciones clave como el GDPR, la CCPA y la norma ISO/IEC 27001, identificando los retos que enfrentan las organizaciones al armonizar estándares y cumplir obligaciones legales diversas. Los resultados revelan que la heterogeneidad regulatoria incrementa la complejidad operativa, eleva los costes de cumplimiento y genera riesgos legales y reputacionales. Sin embargo, se observa que la adopción de estándares internacionales contribuye a fortalecer la confianza institucional, facilita la alineación con exigencias locales y potencia la resiliencia corporativa frente a incidentes de seguridad. La discusión destaca que la normalización no solo actúa como respuesta reactiva ante presiones regulatorias, sino como estrategia proactiva para consolidar la legitimidad empresarial y la ventaja competitiva. Se concluye que integrar la ciberseguridad en la cultura organizacional y priorizar marcos reconocidos constituye un eje central de sostenibilidad y diferenciación, exigiendo inversión, formación continua y compromiso directivo para enfrentar un entorno digital dinámico y complejo.

Palabras clave: ciberseguridad; normativa internacional; gestión de riesgos; estándares internacionales; sostenibilidad empresarial.

Check for updates

Received: 22/Jun/2025
Accepted: 12/Jul/2025
Published: 15/Jul/2025

Cita: Choez-Calderón, C. J., & Aldo-Patricio, M. O. (2025). La ciberseguridad como prioridad empresarial dentro de marcos los regulatorios y normativos internacionales. *Revista Científica Ciencia Y Método*, *3*(3), 14-27. https://doi.org/10.55813/gaea/rcym/v3/n3/38

Revista Científica Ciencia y Método (RCyM)
https://revistacym.com
revistacym@editorialgrupo-aea.com
info@editoriagrupo-aea.com

Abstract:

The study critically examines how cybersecurity has become a strategic business priority in the face of proliferating digital threats and increasing international regulatory fragmentation. Using an exploratory literature review approach, scientific publications, technical reports and key regulations such as GDPR, CCPA and ISO/IEC 27001 were collected and analyzed, identifying the challenges organizations face in harmonizing standards and meeting diverse legal obligations. The results reveal that regulatory heterogeneity increases operational complexity, raises compliance costs, and creates legal and reputational risks. However, it is observed that the adoption of international standards contributes to strengthening institutional trust, facilitates alignment with local requirements and enhances corporate resilience in the face of security incidents. The discussion highlights that standardization not only acts as a reactive response to regulatory pressures, but also as a proactive strategy to consolidate corporate legitimacy and competitive advantage. It is concluded that integrating cybersecurity into the organizational culture and prioritizing recognized frameworks constitutes a central axis of sustainability and differentiation, requiring investment, continuous training and managerial commitment to face a dynamic and complex digital environment.

Keywords: cybersecurity; international regulation; risk management; international standards; corporate sustainability.

1. Introducción

La ciberseguridad ha emergido como una de las preocupaciones más críticas de las organizaciones contemporáneas, dado el incremento sostenido de amenazas informáticas que comprometen la integridad, disponibilidad y confidencialidad de la información corporativa. Este fenómeno se intensifica por la creciente interconexión de los sistemas de información y la globalización de las operaciones empresariales, las cuales exigen una gestión de riesgos orientada al cumplimiento de marcos regulatorios y normativos que varían según la jurisdicción y la industria (Von Solms & Van Niekerk, 2013). El problema central que motiva este estudio radica en la falta de armonización normativa internacional en materia de ciberseguridad, situación que produce dificultades significativas para las empresas al momento de implementar políticas y controles que garanticen no solo la protección de sus activos digitales, sino también el cumplimiento efectivo de las obligaciones legales. Esta problemática genera un entorno de incertidumbre que puede derivar en sanciones económicas, daños reputacionales y pérdida de confianza de los stakeholders (European Union Agency for Cybersecurity [ENISA], 2020).

Diversos factores contribuyen a agravar este escenario. En primer término, el volumen y la sofisticación de los ciberataques han evolucionado exponencialmente, con

amenazas como el ransomware y los ataques a la cadena de suministro que afectan tanto a grandes corporaciones como a pequeñas y medianas empresas (IBM Security, 2024). Asimismo, la dispersión normativa, que se refleja en la coexistencia de estándares y marcos como el Reglamento General de Protección de Datos (GDPR) en Europa, la Ley de Privacidad del Consumidor de California (CCPA) en Estados Unidos, y los lineamientos de la Organización Internacional de Normalización (ISO/IEC 27001), conlleva retos de cumplimiento que requieren inversiones considerables en recursos humanos y tecnológicos (Kshetri, 2014). Otro elemento determinante es la carencia de cultura organizacional orientada a la ciberseguridad, que se traduce en prácticas deficientes de capacitación y concienciación entre los empleados, quienes frecuentemente constituyen el eslabón más vulnerable en la cadena de protección de la información (Safa & Von Solms, 2016). De manera adicional, el marco jurídico de algunos países carece de mecanismos coercitivos o de incentivos que promuevan la adopción de estándares internacionales, lo cual dificulta la consolidación de un ecosistema global resiliente frente a las amenazas digitales (Cavusoglu, Cavusoglu, & Raghunathan, 2004).

La justificación de este trabajo se sustenta en la necesidad apremiante de comprender la interacción entre los marcos regulatorios internacionales y la priorización estratégica de la ciberseguridad en el ámbito corporativo. La literatura reciente sugiere que aquellas organizaciones que adoptan políticas de cumplimiento normativo integral experimentan una mejora significativa en su capacidad de respuesta ante incidentes de seguridad, además de fortalecer su reputación institucional (Bada & Nurse, 2019). La revisión sistemática de las disposiciones regulatorias y de los estándares de referencia permitirá identificar sinergias, brechas y desafíos que inciden en la implementación de programas de ciberseguridad efectivos. Esta perspectiva resulta pertinente tanto para la comunidad académica, interesada en el análisis crítico de las políticas de seguridad, como para los responsables de la toma de decisiones en el ámbito empresarial, quienes requieren orientaciones prácticas para adaptar sus estrategias a contextos regulatorios diversos.

La viabilidad de esta investigación se fundamenta en la amplia disponibilidad de fuentes secundarias provenientes de organismos internacionales, instituciones gubernamentales, asociaciones profesionales y literatura científica indexada en bases de datos como Scopus y Web of Science. Este corpus documental posibilita una aproximación comprehensiva a las tendencias globales en materia de gobernanza de la ciberseguridad, facilitando el análisis comparativo de los marcos regulatorios más relevantes. Asimismo, el enfoque de revisión bibliográfica permite integrar hallazgos empíricos y teóricos que servirán de base para formular recomendaciones orientadas a robustecer la capacidad de las empresas para responder ante un entorno cada vez más complejo y dinámico (Kostopoulos, 2018).

El objetivo general de este artículo consiste en examinar de manera crítica los principales marcos regulatorios y normativos internacionales que inciden en la gestión de la ciberseguridad empresarial, identificando los desafíos, oportunidades y mejores

prácticas que derivan de su adopción. Para alcanzar este propósito, se llevará a cabo una revisión exhaustiva de la literatura científica, normativa y técnica que documente los avances y limitaciones en la materia. Con ello, se pretende ofrecer un análisis que contribuya a la consolidación de estrategias corporativas alineadas con los estándares internacionales y que fortalezcan la capacidad de resiliencia de las organizaciones frente a un panorama de amenazas digitales en constante evolución.

2. Materiales y métodos

La presente investigación adopta un enfoque exploratorio de revisión bibliográfica con el propósito de analizar los principales marcos regulatorios y normativos internacionales que inciden en la gestión de la ciberseguridad en el ámbito empresarial. Esta metodología resulta pertinente debido a la naturaleza dinámica y multidisciplinaria del tema, que requiere la sistematización de conocimientos provenientes de diversas fuentes académicas, técnicas y normativas.

La recopilación de información se realizó mediante una búsqueda exhaustiva en bases de datos científicas reconocidas, tales como Scopus y Web of Science, así como en repositorios institucionales de organismos internacionales especializados en ciberseguridad. Se seleccionaron publicaciones relevantes que abordaran de manera directa el análisis de estándares internacionales, regulaciones vigentes, tendencias emergentes y prácticas empresariales relacionadas con la protección de la información. Para garantizar la calidad y pertinencia de los documentos revisados, se aplicaron criterios de inclusión que consideraron artículos publicados en los últimos diez años, estudios con acceso a texto completo, revisiones sistemáticas, informes técnicos oficiales y literatura especializada que aportara un enfoque comparativo sobre las distintas jurisdicciones.

El proceso de selección de fuentes consistió en la identificación de palabras clave, entre ellas “ciberseguridad”, “regulación internacional”, “normativas de seguridad”, “gestión de riesgos digitales” y “compliance empresarial”, combinadas mediante operadores booleanos que permitieron refinar la búsqueda y delimitar los resultados a contenidos relevantes y actualizados. Posteriormente, se procedió a la lectura crítica de los documentos recuperados, priorizando aquellos que presentaban análisis empíricos o revisiones exhaustivas sobre la implementación de marcos regulatorios y normativos en distintos sectores económicos.

Para el tratamiento de la información recopilada, se realizó una síntesis temática orientada a identificar las categorías principales de análisis, las cuales incluyen los desafíos derivados de la diversidad normativa, las oportunidades de adopción de estándares internacionales y las implicaciones estratégicas para la gestión de la ciberseguridad en las organizaciones. Este procedimiento permitió organizar de manera coherente los hallazgos, facilitando su integración en el cuerpo del artículo de acuerdo con los objetivos planteados.

La validez del enfoque exploratorio se sustenta en la posibilidad de comprender el estado actual del conocimiento y detectar vacíos de investigación que puedan orientar futuras indagaciones. De igual manera, esta metodología posibilita contrastar diversas perspectivas teóricas y prácticas que enriquecen la comprensión integral del fenómeno estudiado.

Finalmente, la redacción de este artículo se desarrolló siguiendo las normas de presentación de trabajos académicos establecidas por la séptima edición del Manual de Publicación de la American Psychological Association (APA), a fin de garantizar la claridad, la rigurosidad metodológica y la consistencia formal del contenido.

3. Resultados

3.1. Desafíos normativos

3.1.1. La diversidad regulatoria complica el cumplimiento empresarial

La creciente complejidad de los entornos regulatorios en materia de ciberseguridad constituye un desafío de primer orden para las organizaciones que operan en economías globalizadas. Esta diversidad normativa responde a la interacción de múltiples factores: la evolución asimétrica de las legislaciones nacionales, las tensiones geopolíticas en torno a la soberanía de los datos y la falta de mecanismos vinculantes que armonicen los estándares internacionales de protección de la información (Greenleaf, 2018). A diferencia de otros ámbitos del derecho económico internacional, como la propiedad intelectual o el comercio de bienes, en el campo de la ciberseguridad no existe aún un consenso multilateral consolidado que garantice la homogeneidad de principios, definiciones y obligaciones.

En este contexto, las empresas multinacionales se ven obligadas a adoptar estrategias de cumplimiento fragmentadas, que suponen la integración de marcos regulatorios de naturaleza diversa y, en ocasiones, contradictoria. El Reglamento General de Protección de Datos (GDPR), por ejemplo, establece obligaciones rigurosas respecto de la recopilación, el almacenamiento y la transferencia internacional de datos personales, bajo un enfoque de responsabilidad proactiva y sanciones pecuniarias significativas en caso de incumplimiento (Voigt & Von dem Bussche, 2017). Por su parte, la Ley de Privacidad del Consumidor de California (CCPA) introduce un sistema de derechos individuales y obligaciones empresariales que, aunque comparte objetivos comunes con el GDPR, difiere en aspectos sustantivos como la definición de venta de datos y el alcance de las exenciones sectoriales (Greenleaf, 2018). Estas diferencias obligan a las organizaciones a diseñar políticas adaptadas a cada jurisdicción, incrementando los costes operativos y la exposición a riesgos legales.

La multiplicidad de marcos regulatorios se hace aún más evidente al considerar otras normativas nacionales y regionales, tales como la Ley de Protección de Datos

Personales de Brasil (Lei Geral de Proteção de Dados - LGPD), la Ley de Protección de Datos de Sudáfrica (POPIA) y la Ley de Ciberseguridad de China. Cada una de estas legislaciones introduce conceptos particulares sobre el consentimiento, las transferencias transfronterizas de datos y las medidas técnicas de seguridad exigidas, generando un entramado normativo cuya interpretación y aplicación requiere una sofisticada capacidad de gestión legal y técnica (Kuner, 2013).

Este panorama de heterogeneidad regulatoria se ve agravado por la existencia de estándares internacionales de carácter voluntario, que si bien no poseen fuerza vinculante, ejercen una presión normativa indirecta sobre las prácticas corporativas. La norma ISO/IEC 27001, por ejemplo, constituye un referente global para la gestión de la seguridad de la información, y su adopción suele ser considerada por los reguladores y los socios comerciales como un indicio de diligencia debida (Humphreys, 2007). No obstante, la coexistencia de este estándar con marcos nacionales obligatorios puede derivar en duplicación de controles, inconsistencias en la documentación y dificultades en la auditoría de cumplimiento.

Asimismo, la falta de un lenguaje regulatorio unificado complica la interpretación jurídica de conceptos clave como “dato personal”, “incidente de seguridad” o “responsabilidad compartida”, especialmente en entornos tecnológicos como la computación en la nube y el procesamiento automatizado de grandes volúmenes de información (big data). Estas ambigüedades exigen a las empresas invertir en recursos especializados que garanticen la correcta aplicación de los distintos marcos normativos en cada fase del ciclo de vida de la información (Kuner, 2013).

La evidencia empírica confirma que la fragmentación regulatoria tiene efectos negativos sobre la eficiencia y la eficacia de los programas de compliance. Según un estudio comparativo realizado por Bamberger y Mulligan (2015), las organizaciones que operan simultáneamente en la Unión Europea y Estados Unidos tienden a priorizar el cumplimiento mínimo indispensable en cada jurisdicción, en detrimento de un enfoque integral de protección de datos que facilite la coherencia global de sus políticas internas. Este fenómeno se conoce como “compliance selectivo” y puede derivar en vulnerabilidades significativas, tanto desde la perspectiva jurídica como reputacional.

Por otra parte, la presión regulatoria diferenciada entre sectores económicos genera asimetrías en la capacidad de las organizaciones para implementar controles de seguridad robustos. Las entidades financieras y las infraestructuras críticas suelen estar sujetas a regulaciones más estrictas, mientras que otras industrias carecen de lineamientos específicos, lo que produce un escenario desigual de capacidades de prevención y respuesta ante incidentes cibernéticos (Puhl & Frey, 2021).

En síntesis, la diversidad normativa que caracteriza el ecosistema internacional de la ciberseguridad representa un desafío multifacético que compromete la eficiencia, la previsibilidad y la sostenibilidad de las estrategias empresariales. La ausencia de un marco regulatorio armonizado obliga a las organizaciones a navegar un entramado de

obligaciones que evolucionan a distinta velocidad y que demandan una capacidad permanente de adaptación, vigilancia normativa y formación especializada. La consolidación de mecanismos internacionales de convergencia regulatoria se perfila como una prioridad ineludible para disminuir la incertidumbre jurídica y fortalecer la resiliencia organizacional frente al riesgo cibernético.

3.2. Oportunidades estratégicas

3.2.1. Los estándares globales fortalecen la confianza y la seguridad

En un contexto caracterizado por la sofisticación creciente de los ciberataques, la volatilidad de las amenazas y la sensibilidad de los datos que circulan en entornos digitales, la adopción de estándares internacionales en materia de ciberseguridad no solo constituye una medida técnica, sino una decisión estratégica que permite a las organizaciones consolidar su legitimidad y credibilidad ante una pluralidad de grupos de interés. La estandarización de procesos mediante marcos reconocidos internacionalmente, como la norma ISO/IEC 27001, el NIST Cybersecurity Framework o las directrices del European Union Agency for Cybersecurity (ENISA), genera un efecto multiplicador en la confianza institucional, dado que ofrece garantías objetivas de diligencia debida, transparencia operativa y capacidad de respuesta ante incidentes críticos (Humphreys, 2007).

La evidencia empírica sugiere que la certificación en estos estándares actúa como un mecanismo de señalización que reduce las asimetrías de información entre las organizaciones y sus contrapartes. De acuerdo con Herath y Rao (2009), los clientes y socios estratégicos perciben que la adhesión a marcos de referencia internacional refleja un compromiso explícito con la protección de los activos de información, lo que facilita la construcción de relaciones contractuales de largo plazo y favorece la diferenciación competitiva en mercados regulados. Este proceso de legitimación simbólica resulta especialmente relevante en sectores de alta sensibilidad reputacional, como el financiero, el sanitario y el tecnológico, donde la confianza en la integridad de los sistemas constituye un activo intangible de valor estratégico.

La implantación de estándares internacionales también se vincula estrechamente con la madurez de los sistemas de gobierno corporativo. La norma ISO/IEC 27001, por ejemplo, incorpora principios de gestión que trascienden la mera dimensión técnica, al establecer requisitos en materia de liderazgo, asignación de responsabilidades, evaluación de riesgos y mejora continua. Esta aproximación integral permite que la ciberseguridad sea incorporada en la cultura organizacional y en los procesos de toma de decisiones estratégicas, fomentando un enfoque preventivo que fortalece la resiliencia corporativa (International Organization for Standardization, 2013).

Otro aspecto fundamental radica en la capacidad de estos estándares para facilitar la articulación con las obligaciones regulatorias locales e internacionales. La Directiva NIS en Europa, la Ley Sarbanes-Oxley en Estados Unidos y la reciente Directiva NIS2 de la Unión Europea establecen obligaciones que pueden ser implementadas de

forma más eficiente mediante la adopción de marcos normalizados, que actúan como un lenguaje común para demostrar cumplimiento ante las autoridades competentes (Puhl & Frey, 2021). Este alineamiento no solo optimiza el uso de los recursos destinados al cumplimiento, sino que permite reducir la exposición al riesgo legal y financiero derivado de eventuales incumplimientos normativos.

Desde una perspectiva operativa, la estandarización genera beneficios tangibles en la gestión de riesgos. La implementación del NIST Cybersecurity Framework, por ejemplo, facilita la identificación sistemática de amenazas, la protección de activos críticos, la detección temprana de incidentes y la definición de procedimientos de respuesta y recuperación, en un ciclo que contribuye a elevar de manera progresiva la madurez organizacional (NIST, 2018). En este sentido, la adopción de estándares internacionales constituye una vía pragmática para dotar a las empresas de capacidades adaptativas frente a un entorno de amenazas dinámico y de creciente complejidad técnica.

Además, el impacto positivo de la certificación en la confianza institucional se manifiesta en la percepción del público y en los procesos de contratación. Karamanov y Mitreva (2022) evidencian que las pequeñas y medianas empresas certificadas bajo ISO/IEC 27001 reportan una mayor facilidad de acceso a contratos con grandes corporaciones y entidades públicas, que exigen garantías documentadas de seguridad de la información. Esta dinámica refuerza la sostenibilidad empresarial y crea un círculo virtuoso en el que la confianza reputacional se traduce en oportunidades de negocio y crecimiento estratégico.

Asimismo, la normalización contribuye a la transparencia en la cadena de suministro digital, un aspecto crítico en la actualidad debido a la creciente interdependencia entre proveedores, socios tecnológicos y clientes. La adopción de estándares compartidos permite definir criterios homogéneos de seguridad, facilitar auditorías externas y reducir los riesgos sistémicos asociados a brechas en los controles de terceros (Sund, 2020). Este alineamiento fortalece la confianza interorganizacional y facilita la cooperación en iniciativas de ciberdefensa colaborativa.

La literatura académica también destaca que la estandarización de la seguridad facilita la transferencia de conocimiento y la capacitación continua de los equipos internos. Humphreys (2007) subraya que los marcos como ISO/IEC 27001 incluyen directrices detalladas sobre concienciación y formación, elementos esenciales para robustecer el “eslabón humano” de la ciberseguridad. Al institucionalizar estos procesos, las organizaciones reducen la probabilidad de incidentes derivados de errores humanos, que continúan siendo una de las principales causas de las brechas de seguridad.

En síntesis, la adopción de estándares internacionales de ciberseguridad configura una oportunidad estratégica multifacética. No solo posibilita el cumplimiento eficiente de las obligaciones regulatorias y la mitigación del riesgo operativo, sino que actúa como un factor de diferenciación competitiva que fortalece la confianza de los stakeholders, incrementa la transparencia en la cadena de valor y contribuye a la

consolidación de un entorno organizacional resiliente. Este enfoque integrado y proactivo constituye una de las respuestas más eficaces ante un panorama global en el que la confianza digital es un prerrequisito indispensable para la sostenibilidad empresarial, en la tabla 1 sintetiza los aspectos centrales, beneficios y retos estratégicos asociados a la adopción de estándares internacionales de seguridad de la información en entornos corporativos.

Tabla 1

Dimensiones estratégicas y sus implicaciones en la gestión de la ciberseguridad organizacional

Dimensión	Aspecto central	Implicaciones estratégicas
Legitimidad organizacional	La certificación internacional proyecta imagen de responsabilidad, transparencia y compromiso con la seguridad.	Mejora la reputación de marca, atrae inversores y facilita relaciones contractuales con grandes corporaciones y gobiernos.
Reducción de Riesgos	Los marcos normalizados permiten identificar, prevenir y gestionar amenazas en toda la cadena de valor.	Disminuyen costos derivados de incidentes, multas regulatorias y pérdidas operativas.
Ventaja competitiva	La diferenciación basada en estándares robustos incrementa la confianza de clientes en sectores regulados y sensibles (financiero, salud, tecnología).	Facilita el acceso a nuevos mercados y la fidelización de clientes exigentes en materia de seguridad.
Cumplimiento normativo	La adopción de normas como ISO/IEC 27001 o NIST Framework agiliza la demostración de cumplimiento frente a reguladores nacionales e internacionales.	Reduce la exposición a sanciones y litigios, optimiza la asignación de recursos al cumplimiento.
Resiliencia operativa	La estandarización incorpora la mejora continua, la capacitación y el liderazgo en seguridad como componentes estructurales del gobierno corporativo.	Aumenta la capacidad de adaptación frente a entornos cambiantes de amenazas.
Transparencia en la Cadena	La homogeneidad de criterios de seguridad facilita auditorías externas y garantiza estándares consistentes entre proveedores y socios tecnológicos.	Minimiza riesgos sistémicos derivados de brechas en terceros y refuerza la colaboración interorganizacional en ciberdefensa.
Desafíos de Implementación	Requiere inversión en tecnología, capacitación de personal, gestión del cambio y alineación con normativas locales.	Puede generar resistencia interna, costos iniciales elevados y complejidad en organizaciones con baja madurez digital.
Capital humano	Los marcos internacionales destacan la importancia de la concienciación y la formación permanente del personal como barrera frente a incidentes derivados de errores humanos.	Promueve culturas organizacionales proactivas y reduce vulnerabilidades internas.
Sostenibilidad y Futuro	La confianza digital se consolida como un prerrequisito esencial de sostenibilidad empresarial, al integrarse la ciberseguridad en la estrategia corporativa.	Las organizaciones que internalizan estos estándares tienden a posicionarse como actores resilientes y competitivos en un mercado global cada vez más interconectado y regulado en materia digital.

Nota: La información expuesta tiene fines orientativos y refleja tendencias generales de implementación (Autores, 2025).

4. Discusión

La revisión exhaustiva de la literatura evidencia que la ciberseguridad empresarial se configura como un campo de tensión permanente entre la multiplicidad normativa internacional y la necesidad de adoptar prácticas homogéneas que garanticen la protección eficaz de los activos digitales. La heterogeneidad de regulaciones, plasmada en marcos como el Reglamento General de Protección de Datos (GDPR), la Ley de Privacidad del Consumidor de California (CCPA) y las directivas sectoriales europeas, expone a las organizaciones a un entramado jurídico fragmentado que incrementa exponencialmente los costes de cumplimiento y la incertidumbre estratégica (Greenleaf, 2018; Voigt & Von dem Bussche, 2017). Esta complejidad normativa se traduce en la obligación de diseñar políticas diferenciadas, que no siempre pueden armonizarse sin redundancias ni contradicciones, generando un escenario propenso al riesgo legal y reputacional.

No obstante, este desafío convive con la oportunidad estratégica de consolidar un enfoque integral mediante la adopción de estándares internacionales de reconocido prestigio, como ISO/IEC 27001 y el NIST Cybersecurity Framework. La literatura revisada sugiere que estos marcos normativos actúan como catalizadores de confianza institucional al proporcionar evidencia tangible del compromiso organizacional con la seguridad de la información (Humphreys, 2007; Karamanov & Mitreva, 2022). Dichos estándares no solo orientan la definición de políticas y controles técnicos, sino que fomentan la instauración de una cultura organizacional donde la seguridad se erige como un principio transversal e ineludible. Este alineamiento entre los objetivos corporativos y los requisitos de protección resulta esencial para robustecer la resiliencia operativa en un entorno globalizado caracterizado por amenazas avanzadas y persistentes (Puhl & Frey, 2021).

Un aspecto particularmente relevante emergente de la revisión es que la adopción de estándares internacionales facilita la construcción de un lenguaje común con los reguladores, proveedores y clientes. Este aspecto cobra especial importancia ante la constatación de que las relaciones comerciales, tanto en entornos B2B como B2C, dependen de la percepción de confianza y de la existencia de garantías verificables sobre la integridad de los sistemas de información (Herath & Rao, 2009). La certificación bajo esquemas reconocidos se convierte así en un diferenciador competitivo que habilita el acceso a contratos con entidades públicas y empresas multinacionales que exigen niveles elevados de diligencia debida. En este sentido, puede sostenerse que la normalización no es solo una respuesta reactiva a la presión regulatoria, sino una estrategia proactiva de consolidación de la credibilidad y legitimidad empresarial.

Por otra parte, la discusión permite advertir que, si bien la adopción de estos marcos aporta ventajas incuestionables, su implementación no está exenta de retos operativos. Karamanov y Mitreva (2022) identifican que las pequeñas y medianas empresas enfrentan dificultades significativas vinculadas con la disponibilidad de

recursos financieros y humanos para desarrollar e integrar los sistemas de gestión que exige la certificación. Asimismo, la coexistencia de estándares voluntarios con regulaciones obligatorias genera riesgos de solapamiento que pueden derivar en redundancias administrativas y en una percepción de complejidad excesiva que desincentive su adopción. Este fenómeno pone de manifiesto la necesidad de políticas públicas que promuevan incentivos económicos y asistencia técnica orientada a la implementación progresiva de marcos normalizados, especialmente en economías emergentes y sectores con menor madurez digital (Sund, 2020).

La convergencia entre las exigencias regulatorias y los estándares internacionales también plantea la cuestión de la gobernanza de los ecosistemas de ciberseguridad. Kuner (2013) sostiene que el carácter transfronterizo de los flujos de datos exige repensar las categorías jurídicas tradicionales y avanzar hacia una armonización regulatoria que reduzca la incertidumbre y simplifique los requisitos de cumplimiento. En esta línea, la articulación entre la Directiva NIS2, los instrumentos de la Organización Internacional de Normalización y los marcos sectoriales constituye una oportunidad de sinergia normativa que podría contribuir a la consolidación de un mercado digital europeo más seguro y competitivo (Puhl & Frey, 2021).

De manera complementaria, la revisión corrobora que los estándares internacionales actúan como vehículos de profesionalización de la gestión de la ciberseguridad. La institucionalización de procesos de mejora continua, auditoría interna y capacitación sistemática fortalece la capacidad organizacional de adaptación frente a un panorama de amenazas dinámico y en constante evolución (Humphreys, 2007). Este enfoque integrador resulta especialmente pertinente si se considera que los ciberataques contemporáneos no solo persiguen la obtención ilícita de datos, sino la disrupción de las cadenas de valor y la explotación de vulnerabilidades en la cadena de suministro digital (Sund, 2020).

En conjunto, la discusión evidencia que las organizaciones se encuentran en una encrucijada entre la presión derivada de un ecosistema normativo fragmentado y la posibilidad de robustecer su posición competitiva mediante la adopción de estándares internacionales. Este equilibrio exige capacidades estratégicas orientadas a integrar el cumplimiento regulatorio con la gestión avanzada de riesgos y la creación de valor reputacional. Así, la ciberseguridad deja de ser un asunto meramente técnico para consolidarse como un vector transversal de legitimidad y sostenibilidad empresarial, cuyo potencial diferenciador depende en última instancia de la voluntad organizacional de asumirla como una prioridad estratégica.

5. Conclusiones

El análisis exhaustivo de la ciberseguridad como prioridad empresarial en el marco de regulaciones y normativas internacionales permite constatar que las organizaciones enfrentan un escenario de complejidad creciente, determinado por la fragmentación

normativa y la sofisticación de las amenazas digitales. La diversidad de marcos regulatorios vigentes en distintas jurisdicciones, junto con la coexistencia de estándares voluntarios y legislaciones obligatorias, configura un entorno donde el cumplimiento efectivo requiere capacidades estratégicas, recursos especializados y una cultura organizacional orientada a la seguridad como principio transversal.

No obstante, este panorama desafiante también revela oportunidades de alto valor estratégico. La adopción de estándares internacionales consolidados, como ISO/IEC 27001 y el NIST Cybersecurity Framework, permite no solo estructurar sistemas de gestión robustos y coherentes, sino también proyectar confianza y credibilidad ante clientes, reguladores y socios comerciales. Esta estandarización contribuye a disminuir las asimetrías de información, facilita la articulación con obligaciones legales heterogéneas y refuerza la resiliencia organizacional frente a incidentes que puedan comprometer la continuidad operativa y la reputación corporativa.

Asimismo, el proceso de certificación y la integración de prácticas normalizadas se traducen en un diferencial competitivo que habilita el acceso a mercados exigentes y fortalece el posicionamiento empresarial en sectores donde la protección de la información constituye un requisito esencial. La estandarización genera beneficios operativos y estratégicos que se manifiestan en la mejora de la capacidad de respuesta, la transparencia en la cadena de suministro y la institucionalización de procesos de mejora continua y formación especializada.

En este contexto, resulta ineludible que las organizaciones adopten un enfoque integral que combine el cumplimiento normativo con la implementación proactiva de estándares globales, reconociendo que la ciberseguridad trasciende su dimensión técnica para consolidarse como un componente central de la sostenibilidad y legitimidad empresarial. La evolución del entorno digital y la intensificación de las amenazas requieren una capacidad adaptativa permanente y la voluntad de incorporar la seguridad como un eje estratégico que oriente decisiones y prácticas en todos los niveles de la organización.

En síntesis, la ciberseguridad empresarial, entendida como una prioridad estratégica en un ecosistema normativo diverso, representa tanto un desafío complejo como una oportunidad transformadora. Aquellas organizaciones que asuman este compromiso con visión de largo plazo estarán en mejor posición para gestionar los riesgos emergentes, cumplir con las exigencias regulatorias y consolidar una propuesta de valor sustentada en la confianza, la transparencia y la excelencia operativa.

CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

Referencias Bibliográficas

Bada, M., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). *Information & Computer Security*, 27(3), 393–410. https://doi.org/10.1108/ICS-07-2018-0080

Bamberger, K. A., & Mulligan, D. K. (2015). *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. MIT Press.

Barzola-Plúas, Y. G., Samaniego-Quiguiri, D. P., Núñez-Ribadeneyra, R. A., & Bonilla-Morejón, D. M. (2023). Protección de datos personales en la era de la computación cuántica y sus desafíos legales. *Revista Científica Ciencia Y Método, 1*(3), 45-57. https://doi.org/10.55813/gaea/rcym/v1/n3/19

Bonilla-Fierro, L. F., & Boné-Andrade, M. F. (2025). Desarrollo de plataformas de comunicación inclusivas mediante diseño universal. *Revista Científica Ciencia Y Método, 3*(2), 59-73. https://doi.org/10.55813/gaea/rcym/v3/n2/5

Castelo-Vinueza, E. M. (2025). Problemas de la investigación tecnológica y su aplicación en la generación de innovación. *Journal of Economic and Social Science Research*, *5*(1), 146–160. https://doi.org/10.55813/gaea/jessr/v5/n1/166

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004). Economics of IT security management: Four improvements to current security practices. *Communications of the Association for Information Systems*, 14, 65–75. https://doi.org/10.17705/1CAIS.01403

Erazo-Luzuriaga, A. F. (2024). Integración de las TICs en el aula: Un análisis de su impacto en el rendimiento académico. *Revista Científica Zambos, 3*(1), 56-72. https://doi.org/10.69484/rcz/v3/n1/12

European Union Agency for Cybersecurity. (2020). Threat Landscape 2020. ENISA.

Galarza-Sánchez, P. C. (2023). Adopción de Tecnologías de la Información en las PYMEs Ecuatorianas: Factores y Desafíos. *Revista Científica Zambos*, *2*(1), 21-40. https://doi.org/10.69484/rcz/v2/n1/36

Galarza-Sánchez, P. C., Agualongo-Yazuma, J. C., & Jumbo-Martínez, M. N. (2022). Innovación tecnológica en la industria de restaurantes del Cantón Pedro Vicente Maldonado. *Journal of Economic and Social Science Research*, *2*(1), 31–43. https://doi.org/10.55813/gaea/jessr/v2/n1/45

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report*, (145), 10–13. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993035

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Humphreys, E. (2007). Implementing the ISO/IEC 27001 Information Security Management System Standard. *Artech House*.

IBM Security. (2024). Cost of a Data Breach Report 204. https://www.ibm.com/security/data-breach

International Organization for Standardization. (2013). *ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements*. ISO.

Karamanov, B., & Mitreva, E. (2022). Benefits and challenges of implementing ISO/IEC 27001 standard in small and medium enterprises. *Quality-Access to Success*, 23(192), 17–23.

Kostopoulos, G. (2018). *Cybersecurity Programs and Policies: Procedures and Controls for Government and Corporate Systems*. Burlington, MA: Jones & Bartlett Learning.

Kshetri, N. (2014). 1 The Emerging Role of Big Data in Key Development Issues: Opportunities, Challenges, and Concerns. *Big Data for Development*, 1–34. https://doi.org/10.1177/2053951714564227

Kuner, C. (2013). *Transborder Data Flows and Data Privacy Law*. Oxford University Press.

NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

Puhl, K., & Frey, R. (2021). Cybersecurity regulatory frameworks in the European financial sector. *Journal of Banking Regulation*, 22(3), 215–229.

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, 57, 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Sánchez-Caguana, D. F., Philco-Reinozo, M. A., Salinas-Arroba, J. M., & Pico-Lescano, J. C. (2024). Impacto de la Inteligencia Artificial en la Precisión y Eficiencia de los Sistemas Contables Modernos. *Journal of Economic and Social Science Research*, *4*(3), 1–12. https://doi.org/10.55813/gaea/jessr/v4/n3/117

Sangacha-Tapia, L., González-Cañizalez, Y., & Rivas-Herrera, J. (2025). Optimización de Criterios de Búsqueda avanzada para Nuevas Tendencias en la Académica mediante Machine Learning. *Revista Científica Zambos, 4*(2), 197-211. https://doi.org/10.69484/rcz/v4/n2/114

Sund, K. J. (2020). Managing cybersecurity in supply chains: A systematic literature review and future research agenda. *Computers & Security*, 92, 101833.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer. https://doi.org/10.1007/978-3-319-57959-7

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