Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), marzo-abril 2026,
Volumen 10, Número 2.

https://doi.org/10.37811/cl_rcm.v10i2

CYBERSECURITY FRAMEWORK (NIST) COMO ESTÁNDAR INTERNACIONAL DE PROTECCIÓN

CYBERSECURITY FRAMEWORK (NIST) AS AN INTERNATIONAL PROTECTION STANDARD

Maria Teodolinda Ortega Ovalle
Universidad de Panamá - Panamá

DOI: https://doi.org/10.37811/cl_rcm.v10i2.23653

Cybersecurity Framework (NIST) como estándar internacional de protección

Maria Teodolinda Ortega Ovalle[1]
maria.ortegao@up.ac.pa
https://orcid.org/0009-0000-3629-9751
Universidad de Panamá
Panamá

RESUMEN

El presente artículo analiza el Cybersecurity Framework desarrollado por el National Institute of Standards and Technology (NIST) como un estándar internacional de referencia para la gestión de riesgos de ciberseguridad. El objetivo principal es evaluar su relevancia en la protección de infraestructuras digitales y su aplicabilidad en organizaciones de distintos sectores y tamaños. La metodología utilizada corresponde a un enfoque cualitativo y documental, basado en la revisión de literatura académica, normativa y estudios de caso. Los resultados evidencian que el NIST Cybersecurity Framework ofrece un modelo flexible y adaptable, estructurado en cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar. Entre los hallazgos más relevantes se destaca su capacidad para mejorar la resiliencia organizacional, estandarizar procesos de seguridad y fortalecer la confianza en el ecosistema digital. No obstante, se identifican desafíos relacionados con los costos de implementación, la necesidad de capacitación especializada y la adaptación en pequeñas y medianas empresas. En conclusión, el NIST Cybersecurity Framework constituye una herramienta fundamental para enfrentar las amenazas digitales contemporáneas, consolidándose como un estándar internacional que promueve la seguridad, la sostenibilidad y la cooperación global en materia de ciberseguridad.

***Palabras clave*:** NIST Cybersecurity Framework, ciberseguridad, gestión de riesgos, protección digital, resiliencia organizacional, estándares internacionales

[1] Autor Principal
Correspondencia: maria.ortegao@up.ac.pa

Cybersecurity Framework (NIST) as an international protection standard

ABSTRACT

This article examines the Cybersecurity Framework developed by the National Institute of Standards and Technology (NIST) as an international reference standard for cybersecurity risk management. The main objective is to assess its relevance in protecting digital infrastructures and its applicability across organizations of different sectors and sizes. The methodology employed follows a qualitative and documentary approach, based on the review of academic literature, regulatory frameworks, and case studies. The findings reveal that the NIST Cybersecurity Framework provides a flexible and adaptable model structured around five core functions: identify, protect, detect, respond, and recover. Among the most significant results is its ability to enhance organizational resilience, standardize security processes, and strengthen trust in the digital ecosystem. However, challenges were identified regarding implementation costs, the need for specialized training, and adaptation in small and medium-sized enterprises. In conclusion, the NIST Cybersecurity Framework represents a fundamental tool to address contemporary digital threats, consolidating itself as an international standard that promotes security, sustainability, and global cooperation in cybersecurity.

***Keywords*:** NIST Cybersecurity Framework, cybersecurity, risk management, digital protection, organizational resilience, international standards

Artículo recibido 20 marzo 2026
Aceptado para publicación: 15 abril 2026

INTRODUCCIÓN

La creciente digitalización de la sociedad contemporánea ha transformado radicalmente la manera en que individuos, organizaciones y gobiernos interactúan, gestionan información y desarrollan sus actividades cotidianas. El uso intensivo de tecnologías de la información y la comunicación ha generado un ecosistema digital interconectado que ofrece innumerables beneficios, pero que también expone a riesgos cada vez más complejos. Entre ellos destacan el cibercrimen, el robo de identidad, los ataques a infraestructuras críticas y la explotación indebida de datos personales. En este contexto, la ciberseguridad se ha convertido en un eje estratégico para garantizar la confianza en los servicios digitales y la sostenibilidad de la economía global.

El problema de investigación que se aborda en este artículo radica en comprender cómo el *Cybersecurity Framework* desarrollado por el National Institute of Standards and Technology (NIST) se ha consolidado como un estándar internacional de referencia para la gestión de riesgos de ciberseguridad. La relevancia de este estudio se justifica en la necesidad de contar con marcos normativos y técnicos que permitan enfrentar amenazas digitales en un entorno caracterizado por la constante innovación tecnológica y la globalización de los mercados. El NIST Cybersecurity Framework, publicado por primera vez en 2014 y actualizado en 2018, se presenta como una herramienta flexible y adaptable que busca fortalecer la resiliencia organizacional y promover la cooperación internacional en materia de seguridad digital.

Los antecedentes investigativos muestran que, antes de la creación del NIST Cybersecurity Framework, existía una diversidad de normas y estándares de seguridad, como la familia ISO/IEC 27000, que ofrecían lineamientos generales para la gestión de la seguridad de la información. Sin embargo, muchos de estos estándares resultaban complejos de implementar, especialmente en pequeñas y medianas empresas, y carecían de un enfoque integral que permitiera gestionar riesgos de manera dinámica. El NIST Cybersecurity Framework surge como respuesta a esta necesidad, ofreciendo un modelo estructurado en cinco funciones esenciales: identificar, proteger, detectar, responder y recuperar. Estas funciones permiten a las organizaciones diseñar estrategias de seguridad adaptadas a sus necesidades específicas, sin importar su tamaño o sector.

Desde una perspectiva teórica, el NIST Cybersecurity Framework se fundamenta en los principios de la gestión de riesgos y la seguridad de la información. La gestión de riesgos plantea que toda organización debe identificar las amenazas potenciales, evaluar su impacto y diseñar medidas de mitigación adecuadas. Por su parte, la seguridad de la información se basa en garantizar la confidencialidad, integridad y disponibilidad de los datos, principios que se encuentran directamente reflejados en las funciones del framework. Además, el NIST incorpora un enfoque constructivista, en el que las organizaciones son responsables de adaptar el modelo a su contexto particular, construyendo soluciones que respondan a sus vulnerabilidades específicas.

El contexto internacional en el que se desarrolla esta investigación es el de una sociedad globalizada, en la que los ciberataques no reconocen fronteras y pueden afectar tanto a grandes corporaciones como a pequeñas empresas y gobiernos. La interdependencia digital hace que un incidente de seguridad en una organización pueda tener repercusiones en múltiples sectores y países. En este escenario, el NIST Cybersecurity Framework se presenta como un estándar que busca establecer un lenguaje común y una metodología compartida para enfrentar amenazas digitales, promoviendo la cooperación entre actores institucionales, empresariales y sociales.

La relevancia de abordar este tema radica en que la ciberseguridad no solo es un asunto técnico, sino también económico, político y social. La falta de protección adecuada puede generar consecuencias graves, como pérdidas financieras, daños reputacionales, interrupción de servicios esenciales y vulneración de derechos fundamentales. Además, la inseguridad digital disminuye la confianza de los usuarios en las plataformas tecnológicas, lo que limita el potencial de desarrollo de la economía digital y afecta la innovación. Por ello, analizar el NIST Cybersecurity Framework como estándar internacional permite comprender cómo este modelo contribuye a mitigar riesgos y a consolidar un ecosistema digital seguro y sostenible.

En cuanto a los objetivos de la investigación, se plantea como objetivo general analizar el NIST Cybersecurity Framework y evaluar su impacto como estándar internacional de protección en la gestión de riesgos de ciberseguridad. Los objetivos específicos incluyen: identificar los beneficios del framework en la resiliencia organizacional, examinar los desafíos que enfrentan las organizaciones en

su implementación y explorar las perspectivas futuras de su aplicación frente a nuevas tecnologías emergentes como la inteligencia artificial, el internet de las cosas y el big data.

Finalmente, este artículo se propone ofrecer una revisión crítica del NIST Cybersecurity Framework, destacando tanto sus aportes como sus limitaciones. La hipótesis que guía el estudio sostiene que, aunque el framework constituye una herramienta esencial para enfrentar amenazas digitales, su eficacia depende de la capacidad de las organizaciones para adaptarlo a sus necesidades específicas y de la cooperación internacional para establecer estándares globales de seguridad. Solo mediante un esfuerzo conjunto será posible consolidar un entorno digital seguro, confiable y sostenible, en el que la innovación tecnológica se desarrolle en armonía con la protección de los derechos y la resiliencia de las organizaciones.

METODOLOGÍA

La presente investigación se enmarca en un enfoque cualitativo, dado que busca comprender y analizar en profundidad el Cybersecurity Framework del NIST como estándar internacional de referencia en la gestión de riesgos de ciberseguridad. El estudio se clasifica como descriptivo y explicativo, ya que pretende describir las características principales del framework y explicar su impacto en la protección de infraestructuras digitales y en la resiliencia organizacional.

El diseño de investigación adoptado es de tipo documental y transversal, basado en la revisión crítica de fuentes académicas, normativas y estudios de caso. Se empleó un enfoque constructivista, en el que el análisis se orienta a la interpretación de los datos y a la construcción de significados sobre la relevancia del NIST Cybersecurity Framework en el contexto digital contemporáneo.

La población de estudio está constituida por documentos oficiales del NIST, literatura académica especializada en ciberseguridad y gestión de riesgos, informes técnicos de organismos internacionales y estudios de caso de empresas que han implementado el framework. La muestra se seleccionó mediante un muestreo intencional, priorizando fuentes actualizadas, pertinentes y de alta calidad académica y normativa, publicadas entre 2014 (año de la primera versión del framework) y 2025.

Las técnicas de recolección de datos incluyeron la revisión documental sistemática, apoyada en bases de datos académicas, repositorios institucionales y publicaciones oficiales. El instrumento de recolección consistió en una matriz de análisis que permitió clasificar la información en categorías

como: beneficios del framework, dificultades de implementación, impacto en organizaciones y perspectivas futuras.

En cuanto a las consideraciones éticas, se respetó la integridad de las fuentes consultadas, garantizando la correcta citación según las normas de la Asociación Americana de Psicología (APA, séptima edición). No se manipularon datos sensibles ni se involucraron participantes humanos, por lo que no se requirió consentimiento informado.

Los criterios de inclusión contemplaron documentos publicados entre 2014 y 2025, relacionados directamente con la aplicación del NIST Cybersecurity Framework en entornos digitales. Los criterios de exclusión descartaron fuentes no académicas, artículos de opinión sin respaldo científico y documentos anteriores a la promulgación del framework.

Finalmente, se reconocen como limitaciones la ausencia de datos empíricos propios, dado que el estudio se centra en la revisión documental, y la dificultad de abarcar la totalidad de casos de aplicación del framework en diferentes países y sectores. No obstante, estas limitaciones no afectan la validez del análisis, ya que el objetivo principal es ofrecer una visión crítica y fundamentada sobre la relevancia del NIST Cybersecurity Framework como estándar internacional de protección.

MARCO TEÓRICO

La ciberseguridad se ha convertido en un campo estratégico para la protección de infraestructuras críticas, la defensa de los derechos digitales y la sostenibilidad de la economía global. En este contexto, el Cybersecurity Framework desarrollado por el National Institute of Standards and Technology (NIST) constituye un referente internacional ampliamente reconocido. Su propósito es proporcionar un modelo flexible y adaptable que permita a las organizaciones gestionar riesgos de ciberseguridad de manera sistemática, independientemente de su tamaño, sector o nivel de madurez tecnológica.

Fundamentos conceptuales

El NIST Cybersecurity Framework se sustenta en los principios de la **gestión de riesgos**, entendida como el proceso de identificar, evaluar y mitigar amenazas que pueden afectar la seguridad de los sistemas de información. Este enfoque reconoce que la seguridad absoluta es imposible, pero que es posible reducir la probabilidad y el impacto de los incidentes mediante estrategias preventivas y correctivas.

Asimismo, el framework se relaciona con los principios de la **seguridad de la información**, que incluyen la confidencialidad, la integridad y la disponibilidad de los datos. Estos tres pilares, conocidos como la "tríada CIA", constituyen la base teórica de cualquier sistema de protección digital y se encuentran reflejados en las funciones del NIST.

Estructura del NIST Cybersecurity Framework

El modelo se organiza en cinco funciones esenciales que representan un ciclo continuo de gestión de riesgos:

1. **Identify (Identificar):** Consiste en reconocer los activos, sistemas, personas y procesos que requieren protección. Esta función se vincula con teorías de gestión de activos y gobernanza organizacional, ya que establece la necesidad de comprender el contexto empresarial antes de diseñar medidas de seguridad.
2. **Protect (Proteger):** Incluye la implementación de salvaguardas para garantizar la prestación de servicios críticos. Se relaciona con la teoría de controles internos y con la ética digital, al enfatizar la responsabilidad de las organizaciones en proteger la información de sus usuarios.
3. **Detect (Detectar):** Se centra en desarrollar mecanismos para identificar incidentes de seguridad en tiempo real. Este componente se fundamenta en teorías de vigilancia tecnológica y monitoreo continuo, que plantean la importancia de la detección temprana para minimizar daños.
4. **Respond (Responder):** Implica establecer planes de acción para contener y mitigar los efectos de un incidente. Se vincula con teorías de gestión de crisis y resiliencia organizacional, que destacan la capacidad de las instituciones para adaptarse y recuperarse frente a situaciones adversas.
5. **Recover (Recuperar):** Busca restaurar las capacidades afectadas y garantizar la continuidad de las operaciones. Este componente se relaciona con teorías de continuidad del negocio y sostenibilidad digital, que subrayan la importancia de aprender de los incidentes para fortalecer la seguridad futura.

Relación con otros estándares internacionales

El NIST Cybersecurity Framework no surge en aislamiento, sino que dialoga con otros marcos normativos y estándares internacionales. Entre ellos destacan la **ISO/IEC 27001**, que establece

requisitos para sistemas de gestión de seguridad de la información, y el **GDPR** de la Unión Europea, que regula la protección de datos personales. Mientras que la ISO/IEC 27001 ofrece un enfoque más formal y certificable, el NIST se caracteriza por su flexibilidad y adaptabilidad. Por su parte, el GDPR complementa al NIST al enfocarse en la privacidad y los derechos de los individuos, mientras que el framework se centra en la gestión integral de riesgos.

Antecedentes investigativos

Diversos estudios han demostrado que la adopción del NIST Cybersecurity Framework contribuye a mejorar la resiliencia organizacional y a estandarizar procesos de seguridad. Investigaciones comparativas señalan que las organizaciones que implementan el framework logran reducir significativamente el tiempo de respuesta ante incidentes y aumentar la confianza de sus clientes en los servicios digitales. Sin embargo, también se han identificado desafíos, como los costos de implementación, la necesidad de capacitación especializada y la dificultad de adaptación en pequeñas y medianas empresas.

Perspectivas teóricas y prospectivas

El marco teórico de este estudio reconoce que la ciberseguridad es un proceso dinámico que debe evolucionar constantemente frente a nuevas amenazas. El surgimiento de tecnologías emergentes como la inteligencia artificial, el internet de las cosas y el big data plantea retos inéditos que requieren ajustes normativos y técnicos. En este sentido, el NIST Cybersecurity Framework se presenta como una base sólida sobre la cual se pueden construir regulaciones complementarias que respondan a los cambios del entorno digital.

La hipótesis que guía este trabajo sostiene que, aunque el NIST Cybersecurity Framework constituye un estándar internacional esencial, su eficacia depende de la capacidad de las organizaciones para adaptarlo a sus necesidades específicas y de la cooperación internacional para establecer un lenguaje común en materia de ciberseguridad.

RESULTADOS

Los hallazgos de esta investigación, obtenidos a partir de la revisión documental y el análisis crítico de fuentes académicas, normativas y estudios de caso, permiten identificar tres grandes dimensiones en

torno a la aplicación del Cybersecurity Framework del NIST: **beneficios alcanzados**, **desafíos persistentes** y **perspectivas futuras**.

1. Beneficios del NIST Cybersecurity Framework

El análisis evidencia que el framework ha generado impactos positivos en la gestión de riesgos de ciberseguridad, consolidándose como un estándar internacional de referencia. Entre los beneficios más relevantes se encuentran:

Flexibilidad y adaptabilidad: El NIST Cybersecurity Framework puede ser implementado en organizaciones de distintos tamaños y sectores, desde grandes corporaciones hasta pequeñas y medianas empresas. Su carácter modular permite que cada institución seleccione las categorías y subcategorías más pertinentes a su contexto.

Resiliencia organizacional: La estructura del framework, basada en las funciones de identificar, proteger, detectar, responder y recuperar, fortalece la capacidad de las organizaciones para anticipar amenazas, contener incidentes y restaurar operaciones críticas.

Estandarización de procesos: Al proporcionar un lenguaje común y una metodología compartida, el framework facilita la comunicación entre diferentes actores institucionales y empresariales, promoviendo la cooperación y la interoperabilidad.

Confianza digital: La adopción del framework incrementa la credibilidad de los servicios electrónicos, al garantizar que las organizaciones cuentan con un modelo sistemático de protección. Esto se traduce en mayor confianza de los usuarios y clientes en el ecosistema digital.

Tabla 1. Beneficios del NIST Cybersecurity Framework

Beneficio	Descripción
Flexibilidad	Adaptable a organizaciones de distintos tamaños y sectores.
Resiliencia organizacional	Mejora la capacidad de recuperación frente a incidentes.
Estandarización	Facilita procesos comunes de seguridad en diferentes industrias.
Confianza digital	Incrementa la credibilidad de usuarios y clientes en servicios electrónicos.

Desafíos en la implementación

A pesar de sus ventajas, la investigación revela que existen obstáculos significativos en la aplicación práctica del framework:

Costos de implementación: Las PYMEs enfrentan dificultades financieras para adquirir tecnologías avanzadas y contratar personal especializado. Esto limita su capacidad de cumplir con las recomendaciones del framework.

Capacitación especializada: La falta de profesionales con conocimientos en gestión de riesgos y ciberseguridad constituye una barrera para la implementación efectiva.

Recursos humanos limitados: Muchas organizaciones carecen de equipos dedicados exclusivamente a la seguridad digital, lo que dificulta mantener un monitoreo constante y responder de manera eficaz a incidentes.

Adaptación tecnológica: Integrar el framework en sistemas heredados o infraestructuras obsoletas resulta complejo, lo que retrasa la adopción en ciertos sectores.

Tabla 2. Desafíos en la implementación del NIST Cybersecurity Framework

Desafío	Impacto
Costos de implementación	Limitaciones financieras en PYMEs.
Capacitación especializada	Necesidad de formar personal en gestión de riesgos y ciberseguridad.
Recursos humanos limitados	Dificultad para mantener monitoreo y respuesta constante.
Adaptación tecnológica	Complejidad en integrar el framework con sistemas heredados.

Perspectivas futuras

El estudio también identifica tendencias y retos que marcarán la evolución del framework en los próximos años:

Integración con nuevas tecnologías: La expansión de la inteligencia artificial, el internet de las cosas y el big data exige que el framework incorpore lineamientos específicos para enfrentar riesgos emergentes.

Cooperación internacional: Dado que los ciberataques no reconocen fronteras, se requiere un esfuerzo global para armonizar estándares y promover la colaboración entre países y sectores.

Evolución normativa: El framework debe actualizarse periódicamente para responder a amenazas inéditas y garantizar su vigencia en un entorno digital dinámico.

Sinergia con otros estándares: La complementariedad con normas como ISO/IEC 27001 y regulaciones como el GDPR permitirá fortalecer la protección integral de datos y sistemas.

Tabla 3. Perspectivas futuras del NIST Cybersecurity Framework

Perspectiva	Implicación
Integración con nuevas tecnologías	Regulación frente a IA, IoT y Big Data.
Cooperación internacional	Establecimiento de estándares globales de ciberseguridad.
Evolución normativa	Ajustes continuos para enfrentar amenazas emergentes.
Sinergia con otros estándares	Complementariedad con ISO/IEC 27001 y GDPR.

En conjunto, los hallazgos muestran que el NIST Cybersecurity Framework constituye un estándar internacional esencial para la protección digital. Su flexibilidad y enfoque integral lo convierten en una herramienta valiosa para fortalecer la resiliencia organizacional y la confianza en el ecosistema digital. No obstante, su eficacia depende de la capacidad de las organizaciones para superar los desafíos de implementación y de la cooperación global para enfrentar amenazas emergentes.

DISCUSIÓN

La interpretación de los resultados obtenidos permite establecer conexiones entre los hallazgos de este estudio, las teorías de gestión de riesgos, la seguridad de la información y los antecedentes investigativos revisados. En primer lugar, los beneficios identificados del NIST Cybersecurity Framework confirman su relevancia como estándar internacional de protección. La flexibilidad y adaptabilidad del modelo se alinean con la teoría de la gestión de riesgos, que plantea que las organizaciones deben diseñar estrategias específicas según su contexto y vulnerabilidades. El hecho de que el framework pueda aplicarse tanto en grandes corporaciones como en pequeñas empresas refuerza su carácter inclusivo, aunque la práctica demuestra que las PYMEs enfrentan mayores dificultades de implementación.

La resiliencia organizacional, otro de los beneficios destacados, se relaciona directamente con la teoría de la continuidad del negocio y con los principios de la seguridad de la información. La capacidad de anticipar amenazas, responder a incidentes y recuperar operaciones críticas refleja un enfoque integral que va más allá de la mera prevención. En este sentido, el NIST Cybersecurity Framework se diferencia de otros estándares como ISO/IEC 27001, que tienden a centrarse en la certificación de procesos, mientras que el NIST enfatiza la construcción de capacidades dinámicas y adaptativas.

No obstante, los desafíos identificados contrastan con la visión optimista de algunos estudios que consideran al framework como un modelo de fácil implementación. La evidencia muestra que los costos de adaptación tecnológica y la necesidad de capacitación especializada constituyen barreras significativas, especialmente para las PYMEs. Este hallazgo plantea un problema de equidad en la protección digital, ya que no todas las organizaciones cuentan con los mismos recursos para garantizar la seguridad de sus sistemas. La discusión con antecedentes investigativos sugiere que, aunque el framework es técnicamente sólido, su eficacia depende de políticas de apoyo y programas de formación que permitan a las pequeñas empresas superar estas limitaciones.

La falta de recursos humanos especializados también se presenta como un obstáculo recurrente. La teoría de la resiliencia organizacional enfatiza que la capacidad de respuesta ante incidentes depende no solo de la tecnología, sino también del capital humano. En este sentido, el NIST Cybersecurity Framework requiere ser complementado con estrategias de capacitación y concienciación que fortalezcan la cultura de seguridad en las organizaciones. La discusión con la teoría de la ética digital refuerza esta idea, al señalar que la protección de datos no puede depender únicamente de sistemas automatizados, sino que requiere un compromiso ético y profesional por parte de quienes gestionan la información.

En cuanto a las perspectivas futuras, la discusión con la teoría de la seguridad dinámica sugiere que la ciberseguridad debe concebirse como un proceso evolutivo. El surgimiento de tecnologías emergentes como la inteligencia artificial, el internet de las cosas y el big data plantea retos inéditos que requieren ajustes normativos y técnicos. El NIST Cybersecurity Framework, al ser un modelo flexible, tiene la capacidad de adaptarse a estos cambios, pero necesita actualizarse periódicamente para mantener su vigencia. La cooperación internacional se presenta como un elemento clave, ya que los ciberataques no reconocen fronteras y pueden afectar a múltiples sectores y países de manera simultánea.

La sinergia con otros estándares, como ISO/IEC 27001 y el GDPR, constituye otra perspectiva relevante. Mientras que el NIST se centra en la gestión integral de riesgos, la ISO/IEC 27001 ofrece un enfoque certificable y el GDPR regula la protección de datos personales. La complementariedad entre estos marcos normativos permite construir un ecosistema digital más seguro y confiable. La discusión con antecedentes investigativos confirma que las organizaciones que integran múltiples estándares logran una protección más robusta y una mayor confianza por parte de sus clientes.

La novedad científica de este trabajo radica en la identificación de la brecha en la implementación del framework entre grandes corporaciones y PYMEs. Este hallazgo abre nuevas líneas de investigación sobre la equidad en la protección digital y la necesidad de soluciones diferenciadas según el tamaño y capacidad de las organizaciones. Asimismo, la discusión resalta la pertinencia del NIST Cybersecurity Framework en la consolidación de la confianza digital, aunque subraya la necesidad de políticas públicas y cooperación internacional para garantizar su eficacia.

En conclusión, la discusión confirma que el NIST Cybersecurity Framework constituye un instrumento esencial para enfrentar las amenazas digitales contemporáneas. Sus beneficios en términos de resiliencia, estandarización y confianza digital son indiscutibles, pero su eficacia depende de la capacidad de las organizaciones para superar los desafíos de implementación y de la actualización constante frente a nuevas tecnologías emergentes. La protección digital en la era contemporánea requiere un enfoque integral que combine regulación, tecnología, capital humano y cooperación internacional. Solo mediante este esfuerzo conjunto será posible consolidar un ecosistema digital seguro, confiable y sostenible.

CONCLUSIÓN

El análisis realizado sobre el Cybersecurity Framework del NIST permite afirmar que este modelo se ha consolidado como un estándar internacional de referencia en la gestión de riesgos de ciberseguridad. Sus cinco funciones esenciales identificar, proteger, detectar, responder y recuperar constituyen un ciclo integral que facilita a las organizaciones enfrentar amenazas digitales de manera sistemática y estructurada. La investigación confirma que el framework no solo aporta un lenguaje común y una metodología compartida, sino que también fortalece la resiliencia organizacional y la confianza en el ecosistema digital.

Uno de los principales aportes del NIST Cybersecurity Framework es su flexibilidad, que lo hace aplicable en organizaciones de distintos tamaños y sectores. A diferencia de otros estándares más rígidos, el NIST permite que cada institución adapte las categorías y subcategorías a su contexto particular, lo que lo convierte en una herramienta inclusiva y práctica. Este hallazgo es especialmente relevante en un mundo digital caracterizado por la diversidad de actores y por la interdependencia de sistemas, donde la seguridad de una organización puede impactar directamente en la de otras.

Sin embargo, la investigación también revela desafíos significativos que limitan la eficacia del framework en la práctica. Las pequeñas y medianas empresas enfrentan mayores dificultades para implementarlo, debido a los costos de adaptación tecnológica, la necesidad de capacitación especializada y la falta de recursos humanos dedicados exclusivamente a la seguridad digital. Esta brecha entre grandes corporaciones y PYMEs plantea un problema de equidad en la protección digital, ya que no todas las organizaciones cuentan con las mismas capacidades para garantizar la seguridad de sus sistemas. En este sentido, se hace evidente la necesidad de políticas públicas, programas de apoyo y estrategias de capacitación que permitan democratizar el acceso a la ciberseguridad.

La discusión también subraya que el NIST Cybersecurity Framework debe concebirse como un modelo dinámico y evolutivo, capaz de adaptarse a las transformaciones del entorno digital. El surgimiento de tecnologías emergentes como la inteligencia artificial, el internet de las cosas y el big data plantea retos inéditos que requieren ajustes normativos y técnicos. La cooperación internacional se presenta como un elemento clave para enfrentar estas amenazas, ya que los ciberataques no reconocen fronteras y pueden afectar a múltiples sectores y países de manera simultánea. En este sentido, el framework debe integrarse con otros estándares y regulaciones, como ISO/IEC 27001 y el GDPR, para construir un ecosistema digital más seguro y confiable.

La **novedad científica** de este trabajo radica en la identificación de la brecha en la implementación del framework entre grandes corporaciones y PYMEs. Este hallazgo abre nuevas líneas de investigación sobre la equidad en la protección digital y la necesidad de soluciones diferenciadas según el tamaño y capacidad de las organizaciones. Asimismo, se resalta la importancia de fortalecer la cultura de seguridad en las instituciones, reconociendo que la ciberseguridad no depende únicamente de la

tecnología, sino también del capital humano y del compromiso ético de quienes gestionan la información.

En conclusión, el NIST Cybersecurity Framework constituye un instrumento esencial para enfrentar las amenazas digitales contemporáneas. Sus beneficios en términos de resiliencia, estandarización y confianza digital son indiscutibles, pero su eficacia depende de la capacidad de las organizaciones para superar los desafíos de implementación y de la actualización constante frente a nuevas tecnologías emergentes. La protección digital en la era contemporánea requiere un enfoque integral que combine regulación, tecnología, capital humano y cooperación internacional.

Este estudio reafirma que invertir en ciberseguridad es invertir en el futuro de la sociedad digital. La confianza en los servicios electrónicos, el comercio en línea y las plataformas tecnológicas depende de la capacidad de garantizar que la información y los sistemas estén protegidos frente a riesgos cada vez más complejos. El NIST Cybersecurity Framework, aunque no exento de limitaciones, representa un paso decisivo hacia la construcción de un entorno digital en el que la innovación tecnológica se desarrolle en armonía con la defensa de los derechos fundamentales y la resiliencia de las organizaciones.

REFERENCIAS BIBLIOGRÁFICAS

Cebula, J. L., & Young, L. R. (2010). *A taxonomy of operational cyber security risks*. Carnegie Mellon University, Software Engineering Institute.

European Union Agency for Cybersecurity (ENISA). (2021). *Cybersecurity guidelines for SMEs*. ENISA Publications.

Greenleaf, G. (2018). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. *Privacy Laws & Business International Report, 145*(1), 10–13.

Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.

Kuner, C. (2020). *Transborder data flows and data privacy law*. Oxford University Press.

Kuner, C., Bygrave, L. A., & Docksey, C. (Eds.). (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

Mitrou, L. (2017). El Reglamento General de Protección de Datos: ¿Una ley para la era digital? En A. Savin & J. Trzaskowski (Eds.), *Derecho de Internet de la UE* (pp. 19–57). Springer. https://doi.org/10.1007/978-3-319-64955-9_2

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity (Version 1.1)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018

National Institute of Standards and Technology (NIST). (2023). *Cybersecurity Framework 2.0: Draft for public comment*. U.S. Department of Commerce. https://www.nist.gov/cyberframework

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020). *Protecting controlled unclassified information in nonfederal systems and organizations (NIST SP 800-171 Rev. 2)*. National Institute of Standards and Technology.

Voigt, P., & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Springer.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.