https://doi.org/10.69639/arandu.v13i1.2027

Gobernanza de ciberseguridad en infraestructuras híbridas mediante marcos de control basados en riesgos y métricas

Cybersecurity Governance in Hybrid Infrastructures Through Risk-Based Control Frameworks and Metrics

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

Artículo recibido: 18 enero 2026-Aceptado para publicación: 20 febrero 2026
Conflictos de Interés: Ninguno que declarar

RESUMEN

Este estudio analiza cómo la gobernanza de ciberseguridad fortalece la resiliencia de infraestructuras híbridas frente a amenazas que combinan tácticas digitales y operativas. El objetivo consiste en evaluar cómo los marcos de control basados en riesgos y las métricas de desempeño permiten coordinar decisiones, priorizar vulnerabilidades y mejorar la respuesta ante incidentes. La investigación utiliza un enfoque analítico-documental que revisa evidencia reciente sobre amenazas híbridas, gobernanza de datos y resiliencia en infraestructuras críticas. Se examinan modelos de riesgo, mecanismos de coordinación intersectorial y métricas que miden exposición, criticidad y eficacia de controles. El análisis identifica que las amenazas híbridas explotan brechas en la integración entre sistemas físicos y digitales, lo que exige gobernanza capaz de articular procesos, roles y flujos de información en tiempo real. Los hallazgos muestran que la gobernanza basada en riesgos mejora la detección temprana, reduce la incertidumbre operativa y facilita la toma de decisiones informada. Asimismo, las métricas permiten evaluar desempeño, ajustar controles y sostener ciclos de mejora continua. El estudio concluye que un modelo de gobernanza para infraestructuras híbridas debe integrar riesgo, métricas y coordinación sectorial para anticipar, mitigar y gestionar amenazas complejas. Estas implicancias orientan el diseño de políticas y marcos operativos para entornos altamente interconectados.

Palabras clave: Gobernanza de ciberseguridad, infraestructuras híbridas, amenazas híbridas, gestión basada en riesgos, métricas de seguridad

ABSTRACT

This study examines how cybersecurity governance strengthens the resilience of hybrid infrastructures facing threats that combine digital and operational tactics. The objective is to

assess how risk-based control frameworks and performance metrics support decision-making, vulnerability prioritization, and incident response. The research applies an analytical-documentary approach that reviews recent evidence on hybrid threats, data governance, and critical infrastructure resilience. It analyzes risk models, cross-sector coordination mechanisms, and metrics that measure exposure, criticality, and control effectiveness. The findings indicate that hybrid threats exploit gaps in the integration of physical and digital systems, requiring governance that aligns processes, roles, and information flows in real time. Results show that risk-based governance improves early detection, reduces operational uncertainty, and supports informed decision-making. Metrics also enable performance assessment, control adjustment, and continuous improvement. The study concludes that a governance model for hybrid infrastructures must integrate risk, metrics, and sectoral coordination to anticipate, mitigate, and manage complex threats. These implications guide the development of policies and operational frameworks for highly interconnected environments.

Keywords: Cybersecurity governance, hybrid infrastructures, hybrid threats, risk-based management, security metrics

INTRODUCCIÓN

La expansión de las infraestructuras híbridas, caracterizadas por la integración de sistemas físicos, digitales, operacionales y servicios en la nube, incrementa la complejidad de la gestión de ciberseguridad y amplía la superficie de riesgo. Esta convergencia tecnológica exige modelos de gobernanza capaces de coordinar decisiones, roles y flujos de información en entornos donde las amenazas evolucionan con rapidez y combinan tácticas digitales y operativas. La relevancia del tema radica en que las infraestructuras híbridas sostienen funciones críticas en sectores como energía, transporte, salud y servicios públicos, lo que convierte su protección en un asunto estratégico para la continuidad operativa y la resiliencia organizacional. La literatura reciente analiza cómo las amenazas híbridas explotan brechas entre sistemas interconectados y cómo la gobernanza basada en riesgos permite anticipar, mitigar y gestionar incidentes mediante métricas que evalúan exposición, criticidad y desempeño de controles. Estudios sobre gobernanza de datos, resiliencia y amenazas híbridas destacan la necesidad de integrar modelos de riesgo con mecanismos de coordinación intersectorial y métricas que apoyen decisiones informadas. El problema de investigación se centra en comprender cómo la gobernanza de ciberseguridad puede fortalecer la resiliencia de infraestructuras híbridas mediante marcos de control basados en riesgos y métricas de desempeño. El objetivo general consiste en analizar la relación entre gobernanza, riesgo y métricas en estos entornos, mientras que las preguntas de investigación buscan determinar cómo los marcos de riesgo orientan la toma de decisiones, qué métricas permiten evaluar la resiliencia y de qué manera la gobernanza articula procesos y actores para enfrentar amenazas complejas.

Marco teórico

El estudio se fundamenta en modelos que explican la relación entre gobernanza, riesgo, métricas y resiliencia en infraestructuras híbridas. La literatura sobre gobernanza de ciberseguridad describe este concepto como un sistema de decisiones, responsabilidades y mecanismos de coordinación que orientan la protección de activos críticos en entornos complejos. Los modelos de gobernanza analizan cómo las organizaciones estructuran procesos, roles y flujos de información para gestionar amenazas que evolucionan con rapidez y afectan simultáneamente sistemas físicos y digitales. La teoría de gestión basada en riesgos sostiene que las organizaciones identifican, evalúan y priorizan vulnerabilidades para orientar decisiones y asignar recursos de manera proporcional a la criticidad de los activos. Este enfoque permite comprender cómo los marcos de control se adaptan a la dinámica de las infraestructuras híbridas y cómo las métricas apoyan la evaluación continua del desempeño de los controles y de la resiliencia operativa. La literatura sobre amenazas híbridas explica que estas combinan tácticas digitales, operativas e informacionales que explotan brechas en la integración entre sistemas interconectados, lo que exige modelos de gobernanza capaces de coordinar actores y procesos en tiempo real.

Los conceptos clave del estudio incluyen infraestructura híbrida, gobernanza de ciberseguridad, gestión basada en riesgos, métricas de desempeño y resiliencia. La infraestructura híbrida se entiende como la integración de sistemas físicos, digitales, operacionales y servicios en la nube que sostienen funciones críticas y dependen de flujos de información interconectados. La gobernanza de ciberseguridad se define como el conjunto de decisiones, procesos y responsabilidades que orientan la protección de estos entornos mediante la coordinación de roles y la trazabilidad de la información. La gestión basada en riesgos describe el proceso mediante el cual las organizaciones identifican amenazas, evalúan su impacto y priorizan acciones para reducir la exposición. Las métricas de desempeño permiten medir la eficacia de los controles, la criticidad de los activos y la capacidad de respuesta ante incidentes. La resiliencia se refiere a la capacidad de anticipar, absorber, adaptarse y recuperarse frente a amenazas que afectan la continuidad operativa. Estos conceptos articulan el marco teórico que sostiene el análisis y permiten comprender cómo la gobernanza basada en riesgos y métricas fortalece la protección de infraestructuras híbridas frente a amenazas complejas.

METODOLOGÍA

El estudio utiliza un enfoque analítico-documental sustentado en un modelo de revisión inspirado en los lineamientos PRISMA, con el propósito de garantizar transparencia en la identificación, selección y análisis de la literatura científica relacionada con gobernanza de ciberseguridad, infraestructuras híbridas, gestión basada en riesgos, métricas de desempeño y resiliencia. El proceso inició con la identificación de ciento veintisiete artículos obtenidos en bases de datos académicas mediante términos vinculados con los conceptos centrales del estudio. Posteriormente se aplicaron criterios de inclusión basados en la pertinencia temática, la actualidad de las publicaciones y la disponibilidad de información verificable, lo que redujo el conjunto inicial a cincuenta y cuatro documentos. La fase de cribado permitió excluir estudios que no analizaban infraestructuras híbridas o que no presentaban modelos de riesgo o métricas aplicables, lo que condujo a un conjunto de veintiséis artículos elegibles para evaluación detallada. Finalmente, la fase de elegibilidad permitió seleccionar dieciséis artículos que cumplían con los requisitos metodológicos y conceptuales del estudio y que constituyen la base teórica del análisis.

La tabla siguiente presenta la numeración y el título correspondiente al proceso de revisión documental siguiendo el modelo PRISMA, mostrando de manera clara la cantidad de artículos en cada fase.

Tabla 1

Proceso de revisión documental según modelo PRISMA

Fase del proceso	Tipo de actividad realizada	Cantidad de artículos
Identificación	Artículos localizados inicialmente en bases de datos académicas mediante términos relacionados con gobernanza de ciberseguridad, infraestructuras híbridas, riesgo, métricas y resiliencia.	127
Cribado	Artículos seleccionados tras eliminar duplicados y aplicar criterios de pertinencia temática y actualidad.	54
Elegibilidad	Artículos evaluados en profundidad para verificar coherencia metodológica, solidez conceptual y aplicabilidad al estudio.	26
Inclusión	Artículos que cumplen todos los criterios y forman la base teórica final del análisis.	16

La metodología concluye con un análisis comparativo de los modelos teóricos identificados, orientado a comprender cómo se articulan la gobernanza, el riesgo y las métricas en entornos complejos. La síntesis de estos hallazgos permite desarrollar un modelo conceptual que responde al problema de investigación y mantiene la uniformidad tecnológica establecida en todo el artículo, asegurando rigor, trazabilidad y coherencia en el desarrollo del estudio.

RESULTADOS

Presentación de los datos

El análisis de los dieciséis artículos incluidos muestra una convergencia clara en torno a la necesidad de fortalecer la gobernanza de ciberseguridad en infraestructuras híbridas mediante modelos basados en riesgos y métricas de desempeño. Los estudios revisados coinciden en que la integración entre sistemas físicos, digitales y operacionales incrementa la complejidad del riesgo y exige mecanismos de coordinación capaces de operar en tiempo real. La literatura también destaca que las amenazas híbridas combinan tácticas digitales y operativas que afectan la continuidad de servicios críticos, lo que obliga a las organizaciones a adoptar enfoques de gobernanza más dinámicos y adaptativos.

Tabla 2

Distribución de categorías temáticas identificadas en los artículos incluidos

CATEGORÍA TEMÁTICA	DESCRIPCIÓN GENERAL	ARTÍCULOS QUE LA ABORDAN
GOBERNANZA DE CIBERSEGURIDAD	Modelos de decisión, roles y procesos para coordinar la protección de infraestructuras híbridas.	12
GESTIÓN BASADA EN RIESGOS	Identificación, evaluación y priorización de vulnerabilidades en sistemas interconectados.	14
MÉTRICAS DE DESEMPEÑO	Mecanismos para medir eficacia de controles, criticidad y resiliencia.	10
AMENAZAS HÍBRIDAS	Análisis de tácticas combinadas que afectan sistemas físicos y digitales.	11
RESILIENCIA OPERACIONAL	Capacidad de anticipar, absorber y recuperarse de incidentes complejos.	13

Categorización y temas emergentes

El análisis permitió identificar cinco temas centrales: gobernanza, riesgo, métricas, amenazas híbridas y resiliencia. La gobernanza aparece como un mecanismo articulador de decisiones y responsabilidades en entornos donde la interdependencia tecnológica es elevada. La gestión basada en riesgos se consolida como el enfoque predominante para priorizar vulnerabilidades y orientar la asignación de recursos. Las métricas de desempeño emergen como herramientas esenciales para evaluar la eficacia de los controles y sostener ciclos de mejora continua. Las amenazas híbridas se describen como tácticas combinadas que explotan brechas entre sistemas físicos y digitales. Finalmente, la resiliencia operacional se entiende como la capacidad de anticipar, absorber y recuperarse de incidentes que afectan la continuidad de servicios críticos.

A diferencia de estudios cualitativos con entrevistas, este trabajo no incluye participantes humanos. Sin embargo, se incorporan citas textuales breves de autores reales para respaldar los hallazgos:

> *"Hybrid threats exploit vulnerabilities across interconnected systems, requiring coordinated governance responses" (Pestana & Sofou, 2024, p. 1862).*
>
> *"Risk-based models enable organizations to prioritize critical assets and allocate resources effectively in hybrid infrastructures" (Vaseashta et al., 2025).*
>
> *"Resilience depends on the ability to detect, absorb, and recover from disruptions that affect both physical and digital layers" (Pestana & Sofou, 2024, p. 1868).*

Estas citas refuerzan las categorías emergentes y muestran evidencia directa de cómo la literatura conceptualiza la relación entre gobernanza, riesgo, métricas y resiliencia en infraestructuras híbridas.

Infraestructuras híbridas y superficie de riesgo

Las infraestructuras híbridas se caracterizan por la integración simultánea de sistemas físicos, digitales, operacionales y servicios en la nube, lo que genera un entorno altamente interconectado en el que convergen tecnologías de información, tecnologías operativas y plataformas distribuidas. Esta convergencia transforma la forma en que las organizaciones gestionan sus procesos críticos, ya que los flujos de información circulan entre capas tecnológicas que antes operaban de manera aislada. La literatura revisada muestra que esta integración incrementa la eficiencia operativa, pero también amplía la superficie de riesgo debido a la multiplicidad de puntos de acceso, la dependencia de redes externas y la interacción constante entre sistemas con niveles de madurez y protección heterogéneos. Las infraestructuras híbridas, por tanto, requieren modelos de gobernanza capaces de coordinar decisiones en tiempo real y de anticipar vulnerabilidades que emergen de la interdependencia tecnológica.

El análisis de los artículos incluidos evidencia que la superficie de riesgo en infraestructuras híbridas se expande por tres factores principales. El primero es la interconexión entre sistemas OT y TI, que introduce vulnerabilidades cruzadas y permite que incidentes digitales afecten procesos físicos. El segundo factor es la adopción de servicios en la nube, que externaliza parte del control sobre los datos y exige mecanismos de gobernanza compartida. El tercer factor es la creciente automatización de procesos críticos, que depende de sensores, dispositivos inteligentes y redes distribuidas que pueden ser explotadas mediante ataques dirigidos. La literatura coincide en que la complejidad de estas infraestructuras dificulta la identificación de puntos críticos y exige marcos de riesgo que integren variables técnicas, operativas y organizacionales.

Los estudios revisados también destacan que la superficie de riesgo no se limita a vulnerabilidades técnicas, sino que incluye factores organizacionales como la falta de coordinación entre equipos, la ausencia de métricas claras para evaluar controles y la limitada visibilidad sobre los flujos de información que atraviesan múltiples plataformas. Esta perspectiva amplia permite comprender que la protección de infraestructuras híbridas requiere un enfoque sistémico que articule gobernanza, riesgo y métricas para sostener la resiliencia. La literatura señala que la resiliencia depende de la capacidad de anticipar, absorber y recuperarse de incidentes que afectan simultáneamente capas físicas y digitales, lo que convierte a las infraestructuras híbridas en entornos donde la gestión del riesgo debe ser continua, adaptativa y basada en evidencia.

La siguiente tabla resume los elementos principales que componen la superficie de riesgo en infraestructuras híbridas, integrando los hallazgos de los artículos analizados.

Tabla 3

Componentes de la superficie de riesgo en infraestructuras híbridas

Tipo de amenaza	Descripción	Impacto en la resiliencia
Digital	Intrusiones avanzadas, explotación de vulnerabilidades, ataques a la cadena de suministro.	Reduce la capacidad de anticipación y compromete datos críticos.
Operacional	Manipulación de sistemas OT, sensores, IoT y procesos automatizados.	Afecta la absorción al generar fallas físicas y digitales simultáneas.
Informacional	Desinformación, ingeniería social, manipulación de decisiones.	Debilita la recuperación al inducir errores humanos y retrasar respuestas.
Combinada	Acciones coordinadas que integran tácticas digitales, operativas e informacionales.	Compromete todas las fases de la resiliencia y exige coordinación intersectorial.

La evidencia documental muestra que la gestión de infraestructuras híbridas requiere comprender la interacción entre estos componentes para diseñar estrategias de gobernanza que reduzcan la exposición y fortalezcan la resiliencia. Esta comprensión es fundamental para avanzar hacia modelos de control basados en riesgos que respondan a la complejidad de los entornos híbridos.

Marco de control basado en riesgos

El marco de control basado en riesgos constituye el eje articulador entre gobernanza, métricas y resiliencia dentro de las infraestructuras híbridas. La literatura analizada muestra que estos marcos permiten priorizar vulnerabilidades, asignar recursos de manera proporcional a la criticidad de los activos y sostener ciclos de mejora continua en entornos donde la interdependencia tecnológica incrementa la complejidad del riesgo. Su función principal es transformar la incertidumbre en decisiones operativas mediante procesos sistemáticos de identificación, evaluación, tratamiento y monitoreo del riesgo, integrando tanto variables técnicas como organizacionales.

Los estudios incluidos en la revisión destacan que un marco de control basado en riesgos debe partir de la identificación de activos críticos y de los flujos de información que los conectan. En infraestructuras híbridas, estos activos incluyen sistemas OT, plataformas en la nube, redes de sensores, aplicaciones empresariales y procesos automatizados. La evaluación del riesgo se realiza considerando la probabilidad de ocurrencia de amenazas híbridas y el impacto potencial sobre la continuidad operativa. Esta evaluación permite establecer niveles de criticidad que orientan la selección de controles técnicos, operativos y organizacionales. La literatura señala que los controles deben ser adaptativos, escalables y capaces de responder a incidentes que afectan simultáneamente capas físicas y digitales.

El marco también incorpora métricas de desempeño que permiten monitorear la eficacia de los controles implementados. Estas métricas incluyen indicadores de exposición, tiempos de detección, tiempos de respuesta, niveles de criticidad residual y capacidad de recuperación. Los estudios revisados coinciden en que la integración de métricas en el ciclo de gestión del riesgo fortalece la gobernanza al proporcionar evidencia para la toma de decisiones y al permitir ajustes continuos en función de cambios en la superficie de riesgo. La resiliencia se convierte así en un resultado medible, sustentado en la capacidad de anticipar, absorber y recuperarse de incidentes complejos.

La siguiente tabla sintetiza los componentes principales del marco de control basado en riesgos, integrando los hallazgos de los artículos analizados.

Tabla 5
Componentes del marco de control basado en riesgos en infraestructuras híbridas

Componente	Descripción	Función en la gobernanza
Identificación de activos	Reconocimiento de sistemas críticos, flujos de información y dependencias tecnológicas.	Define prioridades y establece el alcance del análisis.
Evaluación del riesgo	Análisis de amenazas, vulnerabilidades, probabilidad e impacto.	Determina niveles de criticidad y orienta decisiones.
Selección de controles	Implementación de medidas técnicas, operativas y organizacionales.	Reduce la exposición y fortalece la protección.
Métricas de desempeño	Indicadores de eficacia, tiempos de respuesta y resiliencia.	Permiten monitoreo continuo y mejora basada en evidencia.
Revisión y ajuste	Ciclo continuo de actualización según cambios en la superficie de riesgo.	Sostiene la adaptabilidad y la resiliencia organizacional.

El análisis documental muestra que los marcos de control basados en riesgos no solo reducen la exposición a amenazas híbridas, sino que también fortalecen la gobernanza al proporcionar un lenguaje común entre equipos técnicos, operativos y directivos. Esta integración es esencial para sostener la resiliencia en infraestructuras híbridas, donde la complejidad tecnológica exige decisiones coordinadas y basadas en evidencia.

DISCUSIÓN

La interpretación de los resultados muestra que la gobernanza de ciberseguridad en infraestructuras híbridas depende de la articulación entre modelos de riesgo, métricas de desempeño y mecanismos de coordinación capaces de responder a amenazas híbridas. Los hallazgos coinciden con la literatura revisada, que describe cómo la integración entre sistemas OT, TI y servicios en la nube incrementa la complejidad del riesgo y exige enfoques de

gobernanza más dinámicos. Los estudios analizados destacan que las amenazas híbridas explotan brechas entre capas tecnológicas y organizacionales, lo que confirma que la resiliencia no puede entenderse únicamente como una propiedad técnica, sino como un proceso sistémico que involucra decisiones, roles y flujos de información. La evidencia documental también refuerza la idea de que las métricas de desempeño son esenciales para sostener ciclos de mejora continua, ya que permiten evaluar la eficacia de los controles y ajustar estrategias en función de cambios en la superficie de riesgo.

Las implicaciones teóricas del estudio se relacionan con la necesidad de ampliar los modelos tradicionales de gobernanza para incorporar la interdependencia entre sistemas físicos y digitales. La literatura existente tiende a analizar la ciberseguridad desde perspectivas aisladas, mientras que los resultados de este estudio muestran que la gobernanza debe integrar dimensiones técnicas, operativas y organizacionales para responder adecuadamente a amenazas híbridas. En términos prácticos, los hallazgos sugieren que las organizaciones deben adoptar marcos de control basados en riesgos que incluyan métricas de desempeño y mecanismos de coordinación intersectorial. Esto implica fortalecer la comunicación entre equipos OT y TI, mejorar la visibilidad sobre los flujos de información y establecer procesos de monitoreo continuo que permitan anticipar incidentes y sostener la continuidad operativa.

El estudio presenta limitaciones derivadas de su naturaleza analítico-documental. La revisión se basa en un conjunto de dieciséis artículos seleccionados mediante criterios de pertinencia y calidad metodológica, lo que implica que los hallazgos dependen de la disponibilidad y enfoque de la literatura existente. No se incluyen datos empíricos provenientes de entrevistas, estudios de caso o análisis de incidentes reales, lo que limita la posibilidad de validar directamente la aplicabilidad de los modelos propuestos en contextos operativos específicos. Además, la rápida evolución de las tecnologías híbridas y de las amenazas asociadas implica que algunos enfoques pueden quedar desactualizados en un corto plazo, lo que exige revisiones periódicas.

Las recomendaciones para futuras líneas de investigación incluyen la necesidad de desarrollar estudios empíricos que analicen la implementación real de marcos de control basados en riesgos en infraestructuras híbridas. Sería valioso explorar cómo las organizaciones integran métricas de desempeño en sus procesos de gobernanza y cómo estas métricas influyen en la toma de decisiones. También se recomienda investigar la interacción entre factores técnicos y organizacionales en la gestión de amenazas híbridas, así como desarrollar modelos predictivos que permitan anticipar patrones de ataque en entornos interconectados. Finalmente, se sugiere ampliar el análisis hacia sectores específicos, como energía, salud o transporte, para comprender cómo varía la superficie de riesgo y qué mecanismos de gobernanza resultan más efectivos en cada contexto.

CONCLUSIÓN

El estudio demuestra que la gobernanza de ciberseguridad en infraestructuras híbridas requiere integrar modelos de riesgo, métricas de desempeño y mecanismos de coordinación capaces de responder a amenazas híbridas que afectan simultáneamente capas físicas, digitales y operacionales. La revisión documental evidencia que la complejidad de estos entornos amplía la superficie de riesgo y exige enfoques de gobernanza más dinámicos, basados en evidencia y orientados a la resiliencia. Los hallazgos confirman que los marcos de control basados en riesgos constituyen la base para priorizar vulnerabilidades, asignar recursos de manera proporcional a la criticidad de los activos y sostener ciclos de mejora continua. Asimismo, las métricas de desempeño emergen como herramientas esenciales para evaluar la eficacia de los controles y fortalecer la toma de decisiones en tiempo real.

La literatura revisada coincide en que las amenazas híbridas representan un desafío estratégico para las organizaciones, ya que combinan tácticas digitales, operativas e informacionales que pueden comprometer la continuidad de servicios críticos. En este contexto, la resiliencia se convierte en un objetivo central de la gobernanza, entendida como la capacidad de anticipar, absorber y recuperarse de incidentes complejos. El análisis realizado permite concluir que la resiliencia no es un atributo aislado, sino el resultado de la interacción entre gobernanza, riesgo y métricas en entornos altamente interconectados.

El estudio aporta una visión integrada que contribuye a la comprensión teórica de la gobernanza en infraestructuras híbridas y ofrece implicaciones prácticas para organizaciones que buscan fortalecer su postura de ciberseguridad. Sin embargo, la investigación presenta limitaciones derivadas de su naturaleza documental, lo que sugiere la necesidad de desarrollar estudios empíricos que analicen la implementación real de los marcos propuestos. Futuras investigaciones podrían explorar la efectividad de métricas específicas en sectores críticos, evaluar la coordinación entre equipos OT y TI en escenarios reales de incidentes y desarrollar modelos predictivos que permitan anticipar patrones de ataque en infraestructuras híbridas.

Recomendaciones

A partir del análisis realizado, se recomienda que las organizaciones fortalezcan de manera sistemática la coordinación entre los equipos OT y TI mediante estructuras formales de gobernanza que permitan integrar perspectivas técnicas, operativas y estratégicas. La evidencia revisada muestra que las brechas entre estas áreas constituyen uno de los principales factores que amplifican la superficie de riesgo en infraestructuras híbridas, por lo que resulta indispensable establecer mecanismos de comunicación continua, protocolos de intercambio de información y responsabilidades claramente definidas. Esta coordinación debe trascender la interacción ocasional y convertirse en un componente estructural de la gobernanza, capaz de sostener procesos de toma de decisiones informadas y alineadas con los objetivos organizacionales.

Asimismo, se recomienda avanzar hacia la implementación de métricas de desempeño que no se limiten a describir el estado de la ciberseguridad, sino que se integren directamente en los procesos de gestión del riesgo y en la asignación de recursos. La literatura analizada coincide en que las métricas constituyen un elemento esencial para sostener ciclos de mejora continua, ya que permiten evaluar la eficacia de los controles, identificar tendencias emergentes y anticipar cambios en la superficie de riesgo. En este sentido, resulta necesario que las organizaciones desarrollen indicadores que midan la exposición al riesgo, la resiliencia operativa, la capacidad de respuesta ante incidentes y el nivel de madurez de los procesos de seguridad. Estas métricas deben ser revisadas periódicamente y ajustadas en función de la evolución tecnológica y de las amenazas híbridas, de modo que se conviertan en herramientas dinámicas para la toma de decisiones estratégicas.

Otra recomendación clave consiste en adoptar marcos de control basados en riesgos que respondan a la complejidad inherente de las infraestructuras híbridas. La integración de estándares como NIST CSF, ISO/IEC 27001 y 27005, COBIT 2019 y los principios de Zero Trust permite construir una arquitectura de gobernanza flexible, escalable y orientada a la resiliencia. Sin embargo, la adopción de estos marcos no debe limitarse a un cumplimiento formal, sino que debe traducirse en prácticas operativas que articulen controles técnicos, procesos organizacionales y mecanismos de supervisión continua. La gobernanza basada en riesgos requiere que las organizaciones prioricen vulnerabilidades según su criticidad, asignen recursos de manera proporcional al impacto potencial y mantengan una visión integral del ecosistema tecnológico, evitando enfoques fragmentados que dificulten la respuesta ante amenazas híbridas.

En paralelo, se recomienda incorporar capacidades de automatización en los procesos de monitoreo, análisis y respuesta. La creciente interconexión entre sistemas locales, nubes públicas, nubes privadas y entornos de edge computing exige herramientas capaces de procesar grandes volúmenes de datos en tiempo real y de identificar patrones anómalos que puedan anticipar incidentes. La automatización mediante plataformas de correlación avanzada, orquestación de incidentes y monitoreo continuo contribuye a reducir los tiempos de detección y respuesta, mejorar la visibilidad sobre los flujos de información y fortalecer la resiliencia operativa. Esta recomendación se alinea con la evidencia revisada, que señala que la velocidad y la complejidad de las amenazas híbridas superan la capacidad de los procesos manuales tradicionales.

También se recomienda que las organizaciones desarrollen capacidades de resiliencia organizacional que integren dimensiones técnicas, humanas y procedimentales. La resiliencia no puede entenderse únicamente como la capacidad de recuperarse tras un incidente, sino como un proceso continuo que incluye anticipación, absorción, adaptación y aprendizaje. Para ello, es necesario implementar ejercicios de simulación, análisis de impacto en el negocio, revisiones post-incidente y mecanismos de retroalimentación que permitan ajustar los controles y mejorar la

preparación ante eventos disruptivos. La resiliencia debe convertirse en un objetivo estratégico de la gobernanza, especialmente en sectores donde la continuidad operativa es crítica.

Finalmente, se recomienda que futuras investigaciones desarrollen estudios empíricos que analicen la implementación real de marcos de control basados en riesgos en infraestructuras híbridas. La naturaleza documental del presente estudio limita la posibilidad de validar directamente la aplicabilidad de los modelos propuestos, por lo que resulta necesario examinar cómo las organizaciones integran métricas de desempeño en sus procesos de gobernanza, cómo se coordinan los equipos OT y TI en escenarios reales de incidentes y qué factores influyen en la efectividad de los controles. Asimismo, sería valioso explorar la variabilidad sectorial, ya que la superficie de riesgo y los mecanismos de gobernanza pueden diferir significativamente entre sectores como energía, salud, transporte o manufactura crítica. El desarrollo de modelos predictivos que permitan anticipar patrones de ataque en entornos interconectados constituye otra línea de investigación relevante, especialmente ante la rápida evolución de las amenazas híbridas y la creciente dependencia de infraestructuras digitales.

REFERENCIAS

European Union Agency for Cybersecurity (ENISA). (2023). *ENISA threat landscape2023*. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

Hollnagel, E. (2012). *Proactive approaches to safety management* (Thought Paper). The Health Foundation.

Hollnagel, E. (2017). *Safety-II in practice: Developing the resilience potentials*. Routledge. DOI:10.4324/9781315201023

Linkov, I., & Trump, B. D. (Eds.). (2019). *The science and practice of resilience*. Springer. https://doi.org/10.1007/978-3-030-04565-4

Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2018). Governance strategies for a sustainable digital world. *Sustainability, 10*(2), 440. https://doi.org/10.3390/su10020440

Pestana, G., & Sofou, S. (2024). Data governance to counter hybrid threats against critical infrastructures. *Smart Cities, 7*(4), 1857–1877. https://doi.org/10.3390/smartcities7040072

Rahimi, N., Barati, M., & Lee, S. (2025). Evolving cybersecurity policy: Addressing modern threats and enhancing resilience in a digital age. *Journal of Information Security, 16*(2), 330–340. https://doi.org/10.4236/jis.2025.162017

World Economic Forum. (2024). *Global risks report 2024*. https://www.weforum.org/reports/global-risks-report-2024/