Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México.
ISSN 2707-2207 / ISSN 2707-2215 (en línea), enero-febrero 2026,
Volumen 10, Número 1.

https://doi.org/10.37811/cl_rcm.v10i1

TRANSFORMACIÓN DIGITAL Y CIBERSEGURIDAD: EL RETO DE PUERTOS SEGUROS PARA UN DESARROLLO REGIONAL Y TECNOLÓGICO SOSTENIBLE

DIGITAL TRANSFORMATION AND CYBERSECURITY: THE CHALLENGE OF SAFE HARBORS FOR SUSTAINABLE REGIONAL AND TECHNOLOGICAL DEVELOPMENT

Ricardo Manuel Candanedo Yau
Facultad de Informática Electrónica y Comunicación

Oneida del Carmen Garay Menasho
Facultad de Administración de Empresas y Contabilidad

Ilka María Juliao Obregón
Facultad de Administración de Empresas y Contabilidad

Maricella Corpas
Facultad de Administración de Empresas y Contabilidad

DOI: https://doi.org/10.37811/cl_rcm.v10i1.22776

Transformación Digital y Ciberseguridad: El reto de puertos seguros para un desarrollo regional y tecnológico sostenible

Ricardo Manuel Candanedo Yau[1]
ricardo.candanedo@up.c.pa
https://orcid.org/0009-0002-5017-9830
Facultad de Informática Electrónica y Comunicación
Centro Regional Universitario de Panamá Este
Universidad de Panamá
Panamá, República de Panamá

Oneida del Carmen Garay Menasho
oneida.garay@up.c.pa
https://orcid.org/0009-0002-4412-5422
Facultad de Administración de Empresas y Contabilidad
Campus Octavio Méndez Pereira
Universidad de Panamá
Panamá, República de Panamá

Ilka María Juliao Obregón
ilkajuliao@gmail.com
https://orcid.org/0000-0001-7829-6110
Facultad de Administración de Empresas y Contabilidad
Campus Octavio Méndez Pereira
Universidad de Panamá
Panamá, República de Panamá

Maricella Corpas
maricella.corpas@up.c.pa
https://orcid.org/0000-0001-6430-4423
Facultad de Administración de Empresas y Contabilidad
Campus Octavio Méndez Pereira
Universidad de Panamá
Panamá, República de Panamá

RESUMEN

El presente artículo tiene como objetivo analizar la relación entre la transformación digital y la ciberseguridad en el contexto portuario, destacando su impacto en el desarrollo regional y tecnológico sostenible. La investigación se orienta a comprender cómo la adopción de tecnologías digitales en los puertos marítimos contribuye a la optimización de los procesos logísticos y administrativos, al tiempo que incrementa la exposición a riesgos cibernéticos que pueden comprometer la continuidad operativa y la seguridad de la información. Metodológicamente, se emplea un enfoque cualitativo de tipo descriptivo y analítico, basado en la revisión sistemática de literatura científica, informes técnicos internacionales y marcos normativos relacionados con la gestión portuaria, las tecnologías de la información y la seguridad informática. Los resultados evidencian que la digitalización portuaria, cuando se integra con estrategias sólidas de ciberseguridad, favorece la eficiencia operativa, la competitividad regional y la sostenibilidad, mientras que la ausencia de una gestión adecuada del riesgo digital incrementa la vulnerabilidad de las infraestructuras críticas. Se concluye que la ciberseguridad constituye un componente estratégico e indispensable para consolidar puertos seguros y resilientes en el marco del desarrollo sostenible.

Palabras Claves: desarrollo sostenible; gestión portuaria; puertos marítimos; seguridad informática; tecnologías de la información

[1] Autor Principal
Correspondencia: ricardo.candanedo@up.c.pa

Digital Transformation and Cybersecurity: The challenge of safe harbors for sustainable regional and technological development

ABSTRACT

This article aims to analyze the relationship between digital transformation and cybersecurity in the port context, highlighting its impact on regional and technological sustainable development. The study seeks to understand how the adoption of digital technologies in seaports contributes to the optimization of logistical and administrative processes while increasing exposure to cyber risks that may compromise operational continuity and information security. Methodologically, a qualitative descriptive and analytical approach is applied, based on a systematic review of scientific literature, international technical reports, and regulatory frameworks related to port management, information technology, and computer security. The findings show that port digitalization, when integrated with robust cybersecurity strategies, enhances operational efficiency, regional competitiveness, and sustainability, whereas the lack of adequate digital risk management increases the vulnerability of critical infrastructures. It is concluded that cybersecurity is a strategic and essential component for consolidating secure and resilient ports within the framework of sustainable development.

Keywords: Information technology; Computer security; Seaports; Sustainable development; Port management

Artículo recibido 10 diciembre 2025
Aceptado para publicación: 10 enero 2026

INTRODUCCIÓN

La transformación digital se posiciona como un fenómeno estructural que redefine los modelos de gestión, operación y gobernanza de los sistemas portuarios en el contexto de la economía global contemporánea. La incorporación progresiva de tecnologías de la información y la comunicación, sistemas de automatización, plataformas digitales, soluciones basadas en datos y redes inteligentes modifica sustancialmente la manera en que los puertos articulan los flujos de mercancías, información y servicios (Heilig et al., 2017; UNCTAD, 2019; Basulo-Ribeiro et al., 2024). Este proceso no solo impacta la eficiencia operativa y la competitividad logística, sino que también incide de forma directa en el desarrollo regional, la integración económica y la sostenibilidad tecnológica de los territorios donde los puertos se insertan (Banco Mundial, 2020; CEPAL, 2021).

En este escenario, los puertos evolucionan desde infraestructuras físicas tradicionales hacia ecosistemas digitales complejos, caracterizados por altos niveles de interconectividad entre sistemas administrativos, operativos y de control industrial. La digitalización portuaria favorece la optimización de procesos, la reducción de costos, la mejora en la trazabilidad y la toma de decisiones basada en información en tiempo real, elementos ampliamente documentados en la literatura sobre puertos inteligentes y logística digital (UNCTAD, 2022; Hawari et al., 2024; Schia, 2024). Sin embargo, esta creciente dependencia tecnológica genera un aumento significativo de la superficie de exposición a amenazas cibernéticas, lo que convierte a la ciberseguridad en un desafío estratégico para la gestión portuaria moderna (Grispos & Mahoney, 2022; Khan et al., 2023).

El problema de investigación que orienta este artículo se vincula con la brecha existente entre la acelerada adopción de tecnologías digitales en los puertos y el desarrollo de enfoques integrales de ciberseguridad que acompañen de manera efectiva dicho proceso. A pesar de la relevancia económica y estratégica de los puertos como infraestructuras críticas, en muchos contextos la seguridad digital se aborda de forma fragmentada, reactiva o limitada a aspectos técnicos, sin una adecuada articulación con la planificación estratégica, la gestión organizacional y las políticas de desarrollo sostenible (Banco Mundial, 2022; ENISA, 2022; IAPH, 2021). Esta situación incrementa la vulnerabilidad de los sistemas portuarios frente a incidentes cibernéticos que pueden afectar la continuidad operativa, la integridad de la información y la confianza de los actores involucrados.

La relevancia de este estudio se fundamenta en el impacto multidimensional que los incidentes de ciberseguridad pueden tener en el ámbito portuario. Un evento cibernético no solo compromete los sistemas tecnológicos, sino que puede generar interrupciones logísticas, pérdidas económicas, afectaciones a la seguridad física, daños reputacionales y consecuencias negativas para el desarrollo regional (Notteboom et al., 2021; Sullivan & Lee, 2021). En este sentido, la ciberseguridad se configura como un componente esencial de la sostenibilidad portuaria, en tanto contribuye a garantizar la estabilidad de los flujos comerciales, la protección de los recursos tecnológicos y la resiliencia de las instituciones frente a un entorno digital cada vez más complejo e incierto (Lam & Yap, 2019; World Economic Forum, 2021).

Desde una perspectiva teórica, la investigación se inscribe en los enfoques de la transformación digital concebida como un proceso sistémico e integral que articula tecnología, personas y procesos. Este enfoque sostiene que la digitalización trasciende la simple implementación de herramientas tecnológicas y requiere cambios estructurales en los modelos de gestión, la cultura organizacional y los mecanismos de toma de decisiones (Heilig et al., 2017; Smart ports in Industry 4.0, 2024). En el ámbito portuario, esta visión se vincula con el concepto de puertos inteligentes, los cuales integran tecnologías digitales para mejorar la eficiencia operativa, la sostenibilidad ambiental, la seguridad y la calidad de los servicios ofrecidos (Basulo-Ribeiro et al., 2024; Hawari et al., 2024).

Asimismo, el estudio se apoya en los fundamentos teóricos de la ciberseguridad y la seguridad de la información, particularmente en los principios de confidencialidad, integridad y disponibilidad, que constituyen la base para la protección de los activos digitales (ISO/IEC, 2022). Estos principios se complementan con los enfoques de gestión del riesgo promovidos por organismos internacionales, los cuales proponen identificar, evaluar y mitigar las amenazas y vulnerabilidades que afectan a los sistemas de información, especialmente en infraestructuras críticas como los puertos (NIST, 2020; OECD, 2020; IMO, 2017, 2021).

De manera complementaria, la teoría de la resiliencia organizacional aporta un marco conceptual relevante para analizar la capacidad de los puertos de anticipar, resistir, adaptarse y recuperarse frente a incidentes cibernéticos. La resiliencia no se limita a la respuesta ante eventos disruptivos, sino que implica la construcción de capacidades institucionales que permitan sostener las operaciones esenciales

en escenarios adversos (Lam & Yap, 2019; Sullivan & Lee, 2021). En el contexto portuario, esta noción adquiere especial relevancia, dado que la interrupción de los servicios puede afectar de forma directa a las cadenas de suministro regionales e internacionales (Notteboom et al., 2021).

Los antecedentes investigativos evidencian un creciente interés académico y técnico por el estudio de la digitalización portuaria, los puertos inteligentes y la incorporación de tecnologías emergentes en la gestión logística (UNCTAD, 2019; CEPAL, 2021; Schia, 2024). Paralelamente, existe una amplia producción científica y normativa sobre ciberseguridad en infraestructuras críticas y sistemas industriales (ENISA, 2022; Banco Mundial, 2022; Khan et al., 2023). No obstante, una revisión de la literatura revela que ambos campos suelen abordarse de manera separada, con escasa integración analítica entre transformación digital, ciberseguridad y desarrollo sostenible. En este sentido, el presente artículo aporta una visión holística que articula estos enfoques, destacando la ciberseguridad como un eje transversal de la transformación digital portuaria.

El contexto en el que se desarrolla esta investigación está marcado por la globalización del comercio marítimo, la intensificación de la competencia entre puertos y el aumento de la dependencia de sistemas digitales interconectados (UNCTAD, 2022). A ello se suma un entorno caracterizado por el crecimiento y sofisticación de las amenazas cibernéticas, que afectan de manera particular a las infraestructuras críticas (World Economic Forum, 2021; Grispos & Mahoney, 2022). Este escenario plantea desafíos significativos para los puertos, especialmente en regiones en proceso de modernización tecnológica, donde persisten brechas en capacidades técnicas, marcos normativos y formación especializada en ciberseguridad (CEPAL, 2021; Banco Mundial, 2020).

Finalmente, el objetivo general de este estudio es analizar el papel de la ciberseguridad en los procesos de transformación digital de los puertos, enfatizando su contribución a la construcción de puertos seguros, resilientes y orientados al desarrollo regional y tecnológico sostenible. Se parte de la premisa de que la integración estratégica de la ciberseguridad en la gestión portuaria no solo reduce los riesgos digitales, sino que fortalece la competitividad, la confianza institucional y la sostenibilidad de los sistemas portuarios en el largo plazo, tal como sugieren los marcos normativos y estudios recientes en el ámbito internacional (IMO, 2021; ENISA, 2022).

METODOLOGÍA

La investigación se desarrolla bajo un enfoque cualitativo, orientado a la comprensión integral de los procesos de transformación digital y ciberseguridad en el ámbito portuario, así como de sus implicaciones para el desarrollo regional y tecnológico sostenible. Este enfoque se selecciona debido a la naturaleza compleja, dinámica y contextual del fenómeno estudiado, el cual involucra dimensiones tecnológicas, organizacionales, normativas y estratégicas ampliamente reconocidas en la literatura sobre gestión portuaria y seguridad de infraestructuras críticas (UNCTAD, 2019; Banco Mundial, 2022; Khan et al., 2023).

En cuanto al tipo de investigación, el estudio se sitúa en un nivel descriptivo, analítico y exploratorio. Es descriptivo porque caracteriza las principales tendencias, enfoques y prácticas relacionadas con la digitalización portuaria y la ciberseguridad (Heilig et al., 2017; CEPAL, 2021); es analítico porque examina las relaciones conceptuales y funcionales entre ambos procesos, particularmente en términos de riesgo y resiliencia (Lam & Yap, 2019; Sullivan & Lee, 2021); y es exploratorio en tanto aborda un campo de estudio que, pese a su creciente relevancia, aún presenta vacíos teóricos y empíricos en la integración de la ciberseguridad como eje estratégico del desarrollo portuario sostenible (Smart ports in Industry 4.0, 2024).

El diseño metodológico es no experimental y de tipo observacional, dado que no se manipulan deliberadamente las variables de estudio, sino que se analizan fenómenos existentes a partir de fuentes documentales y marcos conceptuales consolidados (UNCTAD, 2022; ENISA, 2022). Desde una perspectiva temporal, la investigación adopta un diseño transversal, permitiendo ofrecer una visión actual del estado del conocimiento sobre transformación digital y ciberseguridad portuaria. Asimismo, el estudio se inscribe en un enfoque constructivista e interpretativo, considerando que el conocimiento se construye a partir del análisis crítico de discursos científicos, técnicos y normativos (OECD, 2020; NIST, 2020).

La población de estudio está constituida por documentos científicos, técnicos y normativos vinculados con la gestión portuaria, la transformación digital, la ciberseguridad y la protección de infraestructuras críticas. Esta población incluye artículos científicos indexados, informes de organismos internacionales, marcos regulatorios y documentos institucionales del sector marítimo-portuario y de la seguridad de la

información, tales como los emitidos por la IMO, la IAPH, ENISA, el Banco Mundial y la UNCTAD (IMO, 2017, 2021; IAPH, 2021; ENISA, 2022).

El proceso de selección de las fuentes se realiza mediante un muestreo intencional o teórico, basado en criterios de pertinencia temática, relevancia académica, actualidad y aporte al objeto de estudio. Se incluyen documentos que abordan explícitamente la digitalización portuaria, los puertos inteligentes, la ciberseguridad y la resiliencia en infraestructuras críticas, y se excluyen materiales sin respaldo científico o normativo suficiente (Banco Mundial, 2020; UNCTAD, 2019).

Las técnicas de recolección de datos se centran en la revisión documental sistemática y el análisis de contenido cualitativo. Este procedimiento permite identificar conceptos clave, enfoques teóricos, marcos normativos y tendencias emergentes, ampliamente recomendados para estudios de carácter conceptual y estratégico en el ámbito portuario y de la seguridad digital (ENISA, 2022; OECD, 2020). Para ello, se emplean matrices de análisis documental, fichas bibliográficas y registros analíticos que facilitan la organización, categorización e interpretación de la información.

Las categorías de análisis se construyen de forma inductiva y se articulan en torno a ejes como transformación digital portuaria, ciberseguridad, gestión del riesgo, infraestructuras críticas, resiliencia organizacional y desarrollo sostenible, en coherencia con los marcos conceptuales propuestos por la literatura especializada (ISO/IEC, 2022; NIST, 2020; Khan et al., 2023).

En cuanto a las consideraciones éticas, la investigación se rige por los principios de integridad científica y responsabilidad académica, garantizando la correcta citación de las fuentes conforme a las normas APA vigentes. Al basarse exclusivamente en fuentes secundarias de acceso público, no se involucran participantes humanos ni datos sensibles, lo que minimiza los riesgos éticos asociados al estudio.

Finalmente, se reconoce como limitación principal la ausencia de estudios empíricos de campo; sin embargo, esta limitación se compensa con la amplitud y diversidad de la literatura analizada, lo que permite construir una visión robusta e integradora del fenómeno estudiado. Asimismo, se reconoce el carácter dinámico del entorno tecnológico y normativo, lo que sugiere la necesidad de futuras investigaciones que actualicen y profundicen los hallazgos aquí presentados (World Economic Forum, 2021).

RESULTADOS Y DISCUSIÓN

El análisis cualitativo y descriptivo realizado a partir de la revisión sistemática de literatura permitió identificar patrones, categorías y hallazgos relevantes sobre la relación entre la transformación digital y la ciberseguridad en el contexto portuario. Los resultados se organizan de manera lógica y progresiva, atendiendo a los ejes conceptuales definidos en la metodología, y evidencian cómo la integración —o ausencia— de estrategias de ciberseguridad condiciona el éxito de los procesos de digitalización y su contribución al desarrollo regional y tecnológico sostenible.

En primer lugar, se identifican las principales dimensiones de la transformación digital portuaria abordadas en la literatura especializada. La tabla 1 presenta una síntesis de estas dimensiones y su impacto en la gestión portuaria, lo que permite comprender el alcance estructural del proceso de digitalización más allá de la mera adopción tecnológica.

Tabla 1. Dimensiones de la transformación digital en la gestión portuaria

Dimensión analizada	**Descripción cualitativa**	**Impacto identificado en la gestión portuaria**
Digitalización de procesos	Incorporación de sistemas digitales para la gestión administrativa, logística y operativa	Mejora de la eficiencia, reducción de tiempos y optimización de recursos
Interconectividad de sistemas	Integración de plataformas, redes y sistemas de información	Incremento de la trazabilidad y coordinación entre actores
Automatización y control	Uso de tecnologías automatizadas y sistemas de control industrial	Mayor productividad y dependencia tecnológica
Gestión basada en datos	Uso de datos en tiempo real para la toma de decisiones	Fortalecimiento de la planificación estratégica

Nota: Las dimensiones se derivan del análisis de literatura científica y técnica sobre puertos inteligentes y transformación digital. *Fuente:* Elaboración propia a partir de la revisión sistemática de la literatura.

Los resultados reflejados en esta tabla evidencian que la transformación digital portuaria es un proceso multidimensional que impacta de forma directa la eficiencia y competitividad de los puertos. Sin

embargo, también muestran un aumento progresivo de la dependencia de sistemas digitales, lo que incrementa la exposición a riesgos cibernéticos si no se integran mecanismos de protección adecuados.

En segundo lugar, el análisis permitió identificar las principales amenazas cibernéticas asociadas a los entornos portuarios digitalizados. La tabla 2 sintetiza las amenazas más recurrentes reportadas en la literatura y sus posibles consecuencias, destacando la vulnerabilidad de los puertos como infraestructuras críticas.

Tabla 2. Principales amenazas cibernéticas en entornos portuarios digitalizados

Tipo de amenaza	**Características principales**	**Consecuencias potenciales**
Ataques a sistemas de información	Acceso no autorizado, robo o alteración de datos	Pérdida de confidencialidad e integridad de la información
Ataques a sistemas operativos	Interrupción de sistemas de control y automatización	Paralización de operaciones portuarias
Vulnerabilidades humanas	Falta de formación y cultura de ciberseguridad	Incremento del riesgo de incidentes internos
Fallas en la gestión del riesgo	Ausencia de políticas y protocolos de seguridad	Exposición prolongada a amenazas digitales

Nota: Las amenazas se identifican a partir de estudios sobre ciberseguridad en infraestructuras críticas. *Fuente:* Elaboración propia con base en literatura científica y técnica especializada.

La información presentada en la tabla anterior pone de manifiesto que las amenazas cibernéticas no se limitan a aspectos tecnológicos, sino que incluyen factores organizacionales y humanos. Este hallazgo refuerza la necesidad de enfoques integrales de ciberseguridad que contemplen políticas, formación y gestión del riesgo como componentes esenciales de la transformación digital.

En tercer lugar, los resultados evidencian la relación entre las estrategias de ciberseguridad y la resiliencia de los sistemas portuarios. La tabla 3 muestra cómo la literatura vincula la implementación de medidas de ciberseguridad con la capacidad de los puertos para mantener la continuidad operativa y adaptarse a escenarios adversos.

Tabla 3. Relación entre ciberseguridad y resiliencia en puertos digitalizados

Estrategia de ciberseguridad	Enfoque descrito en la literatura	Aporte a la resiliencia portuaria
Gestión integral del riesgo	Identificación, evaluación y mitigación de amenazas	Reducción de impactos ante incidentes
Políticas y normativas	Marco regulatorio y protocolos de seguridad	Fortalecimiento de la gobernanza
Formación del personal	Capacitación en seguridad digital	Disminución de errores humanos
Monitoreo y respuesta	Sistemas de detección y respuesta a incidentes	Recuperación rápida de operaciones

Nota: La resiliencia se analiza desde una perspectiva organizacional y tecnológica. *Fuente:* Elaboración propia a partir del análisis de estudios sobre ciberseguridad y resiliencia.

Los resultados expuestos en esta tabla confirman que la ciberseguridad actúa como un habilitador de la resiliencia portuaria, permitiendo a los puertos anticipar, resistir y recuperarse frente a incidentes cibernéticos. Esta relación resulta clave para garantizar la sostenibilidad de los procesos de transformación digital en el largo plazo.

Finalmente, el análisis cualitativo permitió identificar el vínculo entre puertos seguros, ciberseguridad y desarrollo regional sostenible. La tabla 4 sintetiza los principales aportes que la literatura atribuye a la integración de la ciberseguridad en la transformación digital portuaria en términos de desarrollo regional y tecnológico.

Tabla 4. Aportes de la ciberseguridad portuaria al desarrollo regional sostenible

Eje de desarrollo	Aportes identificados	Implicaciones regionales
Competitividad económica	Continuidad y confiabilidad de las operaciones	Atracción de inversiones y comercio
Desarrollo tecnológico	Innovación segura y adopción de tecnologías	Fortalecimiento del ecosistema digital

Eje de desarrollo	Aportes identificados	Implicaciones regionales
Sostenibilidad institucional	Gobernanza y gestión responsable del riesgo	Confianza de actores públicos y privados
Impacto social y territorial	Estabilidad de cadenas logísticas	Beneficios para comunidades locales

Nota: El desarrollo regional se analiza desde una perspectiva económica, tecnológica e institucional. *Fuente:* Elaboración propia con base en la revisión sistemática de literatura.

Los resultados presentados en la tabla evidencian que la ciberseguridad no solo protege los sistemas portuarios, sino que también actúa como un factor clave para el desarrollo regional sostenible. La integración de estrategias de seguridad digital fortalece la competitividad, la innovación y la estabilidad institucional, justificando la necesidad de considerar la ciberseguridad como un pilar estratégico de la transformación digital portuaria.

En la discusión, los resultados obtenidos a partir de la revisión sistemática de la literatura y el análisis cualitativo permiten interpretar la transformación digital portuaria como un proceso estructural que redefine de manera integral la gestión de los puertos y su función en el desarrollo regional y tecnológico sostenible. Esta interpretación coincide con los enfoques que conciben la digitalización portuaria como una evolución sistémica que transforma procesos, estructuras organizacionales y modelos de gobernanza, más allá de la simple adopción de tecnologías aisladas (Heilig et al., 2017; UNCTAD, 2019; Schia, 2024). En este sentido, los puertos emergen como ecosistemas digitales complejos cuya eficiencia y competitividad dependen crecientemente de la confiabilidad, interoperabilidad y seguridad de sus sistemas tecnológicos (Lam & Yap, 2019; Basulo-Ribeiro et al., 2024).

El análisis de las dimensiones de la transformación digital identificadas evidencia una regularidad significativa en la literatura revisada: la mejora de la eficiencia operativa, la coordinación logística y la optimización de los flujos de información se encuentran estrechamente vinculadas con la interconectividad de los sistemas y el uso intensivo de datos (CEPAL, 2021; Hawari et al., 2024; Smart ports in Industry 4.0, 2024). No obstante, estos mismos factores incrementan la superficie de ataque y la exposición a riesgos cibernéticos, lo que confirma una relación de interdependencia entre digitalización y vulnerabilidad en los entornos portuarios altamente digitalizados (Grispos & Mahoney,

2022; Khan et al., 2023). Este hallazgo resulta relevante, ya que demuestra que los beneficios de la transformación digital no pueden analizarse de forma aislada de los riesgos asociados a la seguridad de la información.

En este contexto, la ciberseguridad se posiciona como un principio estructurante del proceso de transformación digital portuaria. Los resultados permiten interpretar que las amenazas cibernéticas que enfrentan los puertos no responden exclusivamente a factores tecnológicos, sino que se vinculan de manera directa con debilidades organizacionales, normativas y humanas. Esta visión coincide con los enfoques integrales de la seguridad de la información y la gestión del riesgo, que conciben la ciberseguridad como un sistema en el que interactúan personas, procesos y tecnología (ISO/IEC, 2022; NIST, 2020; OECD, 2020). Desde esta perspectiva, limitar la ciberseguridad a soluciones técnicas resulta insuficiente para la protección efectiva de infraestructuras críticas como los puertos (ENISA, 2022; IAPH, 2021).

La relación identificada entre ciberseguridad y resiliencia portuaria constituye uno de los aportes más relevantes del estudio. Los resultados muestran que la adopción de estrategias integrales de gestión del riesgo cibernético, políticas claras de seguridad de la información y mecanismos de monitoreo y respuesta fortalece la capacidad de los puertos para anticipar, resistir y recuperarse frente a incidentes cibernéticos (Banco Mundial, 2022; Sullivan & Lee, 2021). Esta regularidad valida los postulados de la teoría de la resiliencia organizacional aplicada a infraestructuras críticas y permite generalizar que la continuidad operativa portuaria depende, en gran medida, del nivel de madurez alcanzado en materia de ciberseguridad (Notteboom et al., 2021; World Economic Forum, 2021).

En comparación con investigaciones previas que abordan la digitalización portuaria y la ciberseguridad como campos analíticos separados, este trabajo aporta una visión integradora que constituye un elemento de novedad científica. La discusión evidencia que la ciberseguridad no debe concebirse como un componente accesorio ni reactivo, sino como un habilitador estratégico del desarrollo regional y tecnológico sostenible (Khan et al., 2023; Banco Mundial, 2020). Esta integración resulta especialmente pertinente en el contexto de las infraestructuras críticas, donde los impactos de los incidentes cibernéticos trascienden el ámbito organizacional y afectan a las cadenas logísticas, la economía regional y la confianza institucional (UNCTAD, 2022).

Desde una perspectiva prospectiva, los resultados sugieren la necesidad de avanzar hacia modelos de gobernanza portuaria que incorporen la ciberseguridad desde las fases iniciales de la planificación de la transformación digital. Esta proyección teórica abre nuevas líneas de investigación orientadas al análisis de la madurez en ciberseguridad portuaria, al diseño de marcos integrados de transformación digital segura y al estudio comparado de experiencias portuarias en distintos contextos regionales (IMO, 2017, 2021). Asimismo, se destaca la pertinencia de complementar futuros estudios con enfoques empíricos que incluyan estudios de caso y la participación de actores clave del sector.

En términos de aplicación práctica, la discusión resalta que la integración efectiva de la ciberseguridad en los procesos de transformación digital fortalece la competitividad, la sostenibilidad institucional y la confianza de los actores públicos y privados vinculados a la actividad portuaria (ENISA, 2022; IAPH, 2021). Este enfoque resulta particularmente relevante para regiones en proceso de modernización tecnológica, donde la adopción acelerada de soluciones digitales debe ser acompañada de estrategias sólidas de seguridad que garanticen un desarrollo portuario seguro y sostenible (CEPAL, 2021; Banco Mundial, 2020).

Finalmente, la discusión reafirma la pertinencia del estudio dentro de la línea de investigación sobre transformación digital, ciberseguridad e infraestructuras críticas, al consolidar un marco interpretativo que articula teoría, antecedentes y resultados. El trabajo contribuye a posicionar la ciberseguridad como un pilar estratégico para la construcción de puertos seguros, resilientes y alineados con los desafíos del desarrollo regional y tecnológico sostenible (Lam & Yap, 2019; Notteboom et al., 2021).

CONCLUSIONES

El análisis desarrollado permite concluir que la transformación digital de los puertos constituye un proceso estructural e irreversible, cuya efectividad y sostenibilidad dependen de la integración estratégica de la ciberseguridad en los modelos de gestión portuaria. La evidencia obtenida a partir de la revisión sistemática demuestra que, si bien la digitalización mejora la eficiencia operativa y la competitividad logística, incrementa de manera proporcional la exposición a riesgos cibernéticos, lo que exige enfoques de seguridad que trasciendan las soluciones técnicas aisladas y se integren de forma coherente a la planificación organizacional y estratégica (Heilig et al., 2017; Khan et al., 2023).

Los resultados sustentan la postura de que la ciberseguridad debe ser concebida como un habilitador del desarrollo regional y tecnológico sostenible, y no únicamente como un mecanismo de protección reactiva. La integración de políticas de gestión del riesgo, formación del capital humano y marcos normativos consistentes fortalece la resiliencia de los puertos y garantiza la continuidad de sus operaciones, con impactos positivos sobre las cadenas logísticas, la economía regional y la confianza institucional (Banco Mundial, 2022; Sullivan & Lee, 2021; World Economic Forum, 2021).

Asimismo, el estudio permite afirmar que la ausencia de una visión integrada entre transformación digital y ciberseguridad limita el impacto positivo de la innovación tecnológica en el ámbito portuario. Los enfoques fragmentados generan vulnerabilidades persistentes que pueden comprometer el funcionamiento de infraestructuras críticas, afectando no solo a las organizaciones portuarias, sino también a los sistemas productivos y territoriales que dependen de ellas (Grispos & Mahoney, 2022; UNCTAD, 2022). En este sentido, la ciberseguridad se consolida como un componente estratégico de la gobernanza portuaria contemporánea.

Desde una perspectiva teórica, las conclusiones refuerzan la pertinencia de articular los enfoques de transformación digital, gestión del riesgo y resiliencia organizacional para el análisis de los puertos en entornos altamente digitalizados. La coherencia entre estos marcos conceptuales permite comprender la seguridad digital como un proceso dinámico y sistémico, alineado con los objetivos de sostenibilidad y desarrollo regional, ampliando su aplicabilidad a otras infraestructuras críticas (ISO/IEC, 2022; NIST, 2020; OECD, 2020).

Finalmente, el estudio deja planteados interrogantes que abren oportunidades para futuras investigaciones, entre ellas la necesidad de desarrollar estudios empíricos que evalúen el nivel de madurez en ciberseguridad de puertos específicos, así como el análisis de modelos de gobernanza digital adaptados a distintos contextos regionales. Asimismo, resulta pertinente profundizar en el impacto de la cultura organizacional y la formación del personal en la reducción de riesgos cibernéticos, así como en el papel de las políticas públicas en la consolidación de puertos seguros y sostenibles (IMO, 2021; ENISA, 2022). Estas líneas pendientes invitan a otros investigadores a ampliar y complementar los resultados aquí presentados, fortaleciendo el conocimiento científico en torno a la transformación digital y la ciberseguridad portuaria.

REFERENCIAS BIBLIOGRÁFICAS

Banco Mundial. (2020). *Port reform toolkit* (3.ª ed.). World Bank. https://www.worldbank.org/en/topic/transport/publication/port-reform-toolkit-third-edition

Banco Mundial. (2022). *Cybersecurity and critical infrastructure protection*. World Bank Group. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099000004262214810

Basulo-Ribeiro, J., Pimentel, C., & Teixeira, L. (2024). Digital transformation in maritime ports: Defining smart gates through process improvement. *Future Internet, 16*(10), 350. https://doi.org/10.3390/fi16100350

Comisión Económica para América Latina y el Caribe (CEPAL). (2021). *Digitalización y logística portuaria en América Latina*. Naciones Unidas. https://www.cepal.org/es/publicaciones/47260

European Union Agency for Cybersecurity (ENISA). (2022). *Port cybersecurity: Good practices for cyber resilience*. https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices

Grispos, G., & Mahoney, W. R. (2022). Cybersecurity challenges in the shipping and port industry. *arXiv*. https://arxiv.org/abs/2208.03607

Heilig, L., Schwarze, S., & Voß, S. (2017). An analysis of digital transformation in ports. *Transportation Research Procedia, 20*, 377–384. https://doi.org/10.1016/j.trpro.2017.01.050

Hawari, S. M., Hadiprawoto, T. R., & Iriyanty, I. (2024). Smart port management in digital transformation. *International Journal of Marine Engineering Innovation and Research, 9*(3), 442–450. https://iptek.its.ac.id/index.php/ijmeir/article/view/21475

International Association of Ports and Harbors (IAPH). (2021). *Cybersecurity guidelines for ports*. https://sustainableworldports.org/cybersecurity/

International Maritime Organization (IMO). (2017). *Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3)*. https://www.imo.org/en/OurWork/Security/Pages/CyberSecurity.aspx

International Maritime Organization (IMO). (2021). *Revised guidelines on maritime cyber risk management*. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.1.pdf

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security management systems*. International Organization for Standardization. https://www.iso.org/standard/82875.html

Khan, M. A., Salah, K., & Jayaraman, R. (2023). Digital transformation and cybersecurity in smart ports. *IEEE Access, 11*, 11532–11547. https://doi.org/10.1109/ACCESS.2023.3241125

Lam, J. S. L., & Yap, W. Y. (2019). Digitalisation and resilience in ports. *Maritime Policy & Management, 46*(3), 327–347. https://doi.org/10.1080/03088839.2019.1571648

Notteboom, T., Pallis, A., & Rodrigue, J. P. (2021). Disruptions and resilience in global port systems. *Maritime Economics & Logistics, 23*, 179–210. https://doi.org/10.1057/s41278-020-00162-7

NIST. (2020). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). https://www.nist.gov/cyberframework

Organisation for Economic Co-operation and Development (OECD). (2020). *Cybersecurity risk management*. https://www.oecd.org/finance/cybersecurity-risk-management.htm

Schia, P. (2024). Smart ports and technological innovation. *International Journal of Digital Law, 4*(3), 131–150. https://doi.org/10.47975/digital.law.vol.4.n.3.schiavi

Smart ports in Industry 4.0: A systematic literature review. (2024). *Logistics, 8*(1), 28. https://doi.org/10.3390/logistics8010028

Sullivan, J., & Lee, J. (2021). Cyber resilience of critical infrastructures. *Journal of Critical Infrastructure Protection, 34*, 100454. https://doi.org/10.1016/j.ijcip.2021.100454

UNCTAD. (2019). *Port management series: The digitalization of ports*. United Nations. https://unctad.org/publication/digitalization-ports

UNCTAD. (2022). *Review of maritime transport*. United Nations. https://unctad.org/publication/review-maritime-transport-2022

World Economic Forum. (2021). *Global cybersecurity outlook*. https://www.weforum.org/reports/global-cybersecurity-outlook-2021