FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS
UNIVERSIDAD CENTRAL DEL ECUADOR

INGENIO
2026,Vol.9(2),JULIO-DICIEMBRE,PP 034-039

REVISTA INGENIO

# Análisis de la Madurez y Falencias de Ciberseguridad en el Sector Inmobiliario y de la Construcción ante la Transformación Digital

## Analysis of Cybersecurity Maturity and Deficiencies in the Real Estate and Construction Sector Facing Digital Transformation

Martin Sebastián Jacome Zabala | Universidad Tecnológica Israel
Tannia Cecilia Mayorga Jácome | Universidad Tecnológica Israel

Recibido: 29/11/2025
Recibido tras revisión: 29/04/2026
Aceptado: 15/07/2026
Publicado: 31/07/2026

**Palabras clave (UNESCO)**
Ciberseguridad, Industria de la construcción, Transformación digital, Gestión de riesgos, Protección de datos.

**KEY WORDS**
Cybersecurity, Construction industry, Digital transformation, Risk management, Data protection.

**RESUMEN**

Los sectores de la construcción y bienes raíces han estado en una fase importante de transformación tecnológica, donde han adoptado una variedad de herramientas modernas como el Modelado de Información de Construcción (BIM), Gemelos Digitales, Inteligencia Artificial, etc. Pero esta digitalización ha superado la capacidad del segmento para defender sus activos digitales. A diferencia de la manufactura o la banca, la construcción carece de marcos de ciberseguridad establecidos, dejando la información financiera, técnica y personal vulnerable a riesgos sistémicos de espionaje y sabotaje. 2) Objetivo: La intención de este estudio es diagnosticar esta brecha en ciberseguridad de la industria y descubrir algunas debilidades estructurales y culturales para prevenir una defensa efectiva. El programa busca comparar la madurez digital con diferentes industrias y proponer tecnologías de gestión de riesgos adaptadas al paisaje siempre cambiante de los proyectos de construcción. 3) Metodología: La recolección de datos fue cualitativa basada en una Revisión Sistemática de Literatura (SLR). De bases de datos clasificadas, se eligieron y revisaron en profundidad 20 artículos de impacto científico (2021-2025), revisando estudios de caso de diferentes países, incluidos, pero no limitados a, Australia, el Reino Unido, Asia y el mundo árabe. 4) Los principales hallazgos: Se encontró que la "seguridad de la información" tiene un papel en la configuración de los aspectos psicológicos y técnicos de la adopción de BIM y Contratos Inteligentes. Se observó que los riesgos eran tanto tecnológicos como humanos, debido a la baja percepción del riesgo y la baja disciplina organizacional. Además, el uso de IA generativa (ChatGPT) sin protocolos, abre nuevas amenazas a la privacidad. 5) Conclusiones clave: Se concluye que en lugar de adoptar herramientas genéricas de TI, se deben construir modelos específicos de construcción (por ejemplo, CISS para informes) y habilitar foros de intercambio de información para la defensa colectiva. La ciberseguridad es una disciplina de protección de activos estratégicos, no un costo operativo.

**ABSTRACT**

The construction and real estate industries are in a critical phase of technological transformation, adopting advanced tools such as Building Information Modeling (BIM), Digital Twins, and Artificial Intelligence. However, this digitalization has outpaced the sector's capacity to protect its digital assets. Unlike manufacturing or banking, construction lacks consolidated cybersecurity frameworks, exposing financial, technical, and personal information to systemic risks of espionage and sabotage. 2) Objectives: The main purpose of this researchre is to diagnose the current state of cybersecurity in the sector, identifying the structural and cultural gaps that hinder effective defense. It seeks to comparatively analyze digital maturity against other industries and propose risk management frameworks adapted to the dynamic nature of construction projects. 3) Methodology: A qualitative methodology based on a Systematic Literature Review (SLR) was employed. Twenty high-impact scientific articles (2021-2025) from indexed databases were selected and critically analyzed, evaluating case studies in diverse contexts such as Australia, the United Kingdom, Asia, and the Arab world. 4) Main results: The findings reveal that "information security" is a key psychological and technical barrier to the adoption of BIM and Smart Contracts. It was identified that the risks are not only technological but also human, stemming from a low perception of risk and a lack of organizational discipline. Furthermore, it is evident that the use of generative AI (ChatGPT) without protocols introduces unprecedented privacy vulnerabilities. 5) Main conclusions: It is concluded that the solution lies not in adopting generic IT tools, but in implementing specific models for construction (such as CISS for reporting) and fostering collective defense through information-sharing forums. Cybersecurity must be redefined as a strategic discipline for asset protection and not as an operational cost.

DOI: 10.29166/ingenio.v9i2.9324
pISSN 2588-0829
eISSN 2697-3243

fing.revista.ingenio@uce.edu.ec

## 1.Introducción

La economía global experimenta una transición acelerada hacia la Cuarta Revolución Industrial, caracterizada por la fusión de sistemas físicos y digitales. En este contexto, el sector de la construcción y el ámbito inmobiliario han iniciado una migración agresiva hacia la digitalización para mantener su competitividad. Este es un fenómeno mundial y medible; por ejemplo, la implementación de la estrategia nacional de transformación digital (2023-2029) en economías emergentes como Kazajistán ha posicionado exitosamente al país en el puesto 36 a nivel mundial en competitividad digital. Pero el progreso ha descubierto una fragilidad crítica: la infraestructura de seguridad de datos no se mantuvo al ritmo de la implementación tecnológica, estableciendo un contexto en el que la innovación superó a la protección. [1].

### 1.1 Contexto de la Problemática: La Asimetría Industrial

El problema no es tanto la digitalización en sí, sino la asimetría en su madurez de seguridad. La literatura científica destaca una brecha alarmante entre la construcción y otros sectores industriales, específicamente la manufactura. Un estudio comparativo exhaustivo demuestra que, aunque el sector manufacturero ha implementado normas de protección consistentes con los estándares de seguridad dentro de entornos controlados, la construcción se está quedando atrás.[2] .

Este estudio sugiere que, aunque el "Gemelo Digital" parece ser uno de los instrumentos habilitadores más significativos para la transformación económica —particularmente a raíz de la pandemia de COVID-19—, su implementación en la construcción enfrenta más desafíos que en la manufactura. Esta ausencia de unificación de estándares y serias deficiencias en la protección de datos a lo largo del ciclo de vida del proyecto llevan al sector a no alcanzar su máximo potencial, exponiéndolo a riesgos que ya han sido mitigados en otros sectores industriales[2].

Esta vulnerabilidad se agudiza debido a la naturaleza sistémica de las obras. A diferencia de una fábrica cerrada, un proyecto de construcción es un ecosistema de "límites superpuestos" (overlapping boundaries). Turk et al. (2022) argumentan que la industria es específica y no puede depender de soluciones genéricas prestadas de otros sectores . En una obra, la información fluye entre arquitectos, ingenieros y contratistas temporales a través de fronteras organizacionales difusas, lo que hace ineficaces los métodos tradicionales de defensa perimetral. Se ha propuesto un marco que identifica tres tipos de actividades ilícitas fundamentales a prevenir: robar, mentir y dañar, aplicables a cuatro elementos: activos de información, materiales, personas y sistemas[3] .

### 1.2 El Activo de la Información y el Factor Humano

En la economía moderna, la información —secretos comerciales, bases de datos de clientes, planos de infraestructura crítica— se ha convertido en el activo intelectual más valioso de las empresas constructoras. Se advierte que este capital es codiciado por competidores, estados rivales y grupos criminales, convirtiendo al espionaje industrial en una amenaza tangible. El estudio enfatiza que la seguridad no es solo tecnología, sino un enfoque basado en la "disciplina": reglas escritas y claras para superar la informalidad operativa del sector[4].

Sin embargo, la gestión de este activo enfrenta obstáculos internos. Al analizar la eficacia de la ciberseguridad en firmas del Reino Unido utilizando el modelo McKinsey 7S extendido, se descubrió estadísticamente que los elementos más críticos no son tecnológicos. Los hallazgos subrayan que las "relaciones con terceros" y el "cumplimiento normativo" son factores determinantes de la efectividad de la seguridad, superando a la infraestructura técnica. Esto confirma que la cadena de suministro fragmentada es el eslabón más débil del ecosistema[5].

### 1.3 Nuevas Tecnologías, Nuevos Vectores de Ataque

La incorporación de tecnologías disruptivas ha ampliado la superficie de ataque. La Inteligencia Artificial Generativa (como ChatGPT) se utiliza cada vez más para tareas administrativas, pero su adopción carece de controles de privacidad adecuados. Un análisis bibliométrico reciente identificó tres clústeres principales de riesgos asociados a estas herramientas: preocupaciones de privacidad y ética (Clúster Rojo), vulnerabilidades ante ciberataques y generación de malware (Clúster Verde), y problemas de sesgo y precisión (Clúster Azul)[6] .

De manera similar, la adopción de Contratos Inteligentes (Smart Contracts) enfrenta barreras significativas. Un estudio cuantitativo en el mercado de Arabia Saudita reveló que, aunque el 85.2% de los encuestados reconoce que el Internet de las Cosas (IoT) facilita estos contratos, existen 19 barreras críticas para su implementación. Entre ellas destacan las "preocupaciones por la ciberseguridad" y la falta de expertos capaces de auditar la seguridad de los códigos en Blockchain[7] .

### 1.4 Justificación y Necesidad de Estandarización

Pese al incremento de riesgos, el sector adolece de una opacidad crónica. Se señala que la ausencia de un marco estandarizado para la notificación de incidentes impide la creación de una base de datos centralizada, lo que bloquea el aprendizaje colectivo. La implementación de modelos cuantitativos como la Escala de Gravedad de Incidentes de Ciberseguridad (CISS) es imperativa para transformar incidentes cualitativos en métricas comparables que permitan priorizar recursos y evaluar dimensiones como la seguridad física y el impacto financiero [8].

### 1.5 Propósito del Estudio

El propósito de este trabajo es realizar un análisis exhaustivo y "humanizado" de las falencias de ciberseguridad en el sector, contrastando la realidad operativa con las exigencias digitales. Los objetivos específicos son:

1. Evaluar la brecha de madurez tecnológica entre la construcción y la manufactura.

2. Identificar los factores humanos y organizacionales que actúan como barreras de defensa.
3. Analizar las vulnerabilidades específicas de tecnologías emergentes (IA, BIM, Smart Contracts).
4. Sistematizar marcos de solución validados (CISS, Machine Learning) para ofrecer una guía práctica a los actores del sector.

## 2.Método

La presente investigación se desarrolló bajo un enfoque cualitativo de carácter descriptivo y analítico. Dado que la ciberseguridad en el sector de la construcción es un campo de estudio emergente y fragmentado, se determinó que el diseño metodológico más adecuado para abordar los objetivos planteados era la **Revisión Sistemática de Literatura (SLR).** Este método permite sintetizar la evidencia científica existente, identificar patrones comunes en diferentes contextos geográficos y evaluar la efectividad de los marcos teóricos propuestos por la academia en los últimos años[2].

El diseño de la investigación se alineó con enfoques metodológicos validados en estudios sectoriales previos. Por ejemplo, se tomó como referencia el rigor analítico empleado por Sonkor y García de Soto, quienes utilizaron un flujo de cinco pasos (definición del alcance, búsqueda, selección, análisis bibliométrico y discusión) para mapear los riesgos de la IA en la construcción[6]. De manera similar, se consideró el enfoque de triangulación metodológica propuesto por Siriwardhana et al., quienes validaron la importancia de recopilar perspectivas de expertos y utilizar la herramienta analítica SWOT (Fortalezas, Oportunidades, Debilidades y Amenazas) para examinar sistemáticamente los determinantes de la implementación tecnológica en la industria[9].

### 2.1 Material y Unidad de Análisis

Para la constitución del cuerpo teórico del estudio, se llevó a cabo una rigurosa selección de fuentes primarias. La unidad de análisis final consiste en 20 documentos científicos de alto impacto, incluyendo artículos de revistas, ponencias de conferencias internacionales y capítulos de libros especializados.

La base de datos bibliográfica se construyó priorizando la calidad y actualidad, asegurando que la información refleje el estado del arte post-pandemia y la reciente aparición de la Inteligencia Artificial. Los materiales provienen principalmente de editoriales prestigiosas como Elsevier, Springer e IEEE.

#### *2.1.1 Criterios de Inclusión y Exclusión*

Para garantizar la pertinencia de la muestra, se aplicaron los siguientes filtros:

- **Temporalidad (2021-2025):** Se seleccionaron exclusivamente investigaciones publicadas en los últimos cinco años. Este criterio fue fundamental para incluir estudios que abordaran tecnologías recientes como los Gemelos Digitales post-COVID y la IA generativa. Se excluyeron estudios anteriores que no contemplaran el panorama actual de amenazas cibernéticas (ej. ransomware moderno).
- **Temática Específica (Intersección Sectorial):** Se incluyeron únicamente aquellos estudios que abordaran la convergencia entre "Ciberseguridad/TI" y "Sector Construcción/Inmobiliario". Se descartaron artículos puramente técnicos de informática que carecieran de aplicación práctica en el entorno construido.
- **Diversidad Geográfica:** La muestra abarca estudios empíricos y teóricos de diversas regiones (Reino Unido, Australia, Noruega, Kazajistán, Malasia, Vietnam y Medio Oriente). Esto permite contrastar la madurez digital entre economías desarrolladas y emergentes.

### 2.2 Procedimiento de Análisis de Datos

El análisis de la información se estructuró siguiendo protocolos de categorización temática. Se extrajeron datos cuantitativos de los estudios empíricos (porcentajes de adopción, puntuaciones de riesgo) y se sintetizaron los marcos conceptuales cualitativos. Este proceso de síntesis se apoya en metodologías previas que han integrado revisiones literarias múltiples para construir marcos de evaluación de riesgos, como lo proponen Yao y García de Soto en el desarrollo de sus módulos de Machine Learning [10].

## 3. Resultados y Discusión

A partir de la revisión sistemática, se han identificado patrones críticos que explican el estado actual de vulnerabilidad en el sector. Los hallazgos se presentan categorizados por dimensiones estructurales, humanas y tecnológicas, contrastando la teoría académica con la evidencia empírica recolectada.

### 3.1 La Brecha de Madurez Digital: Comparativa Intersectorial

La literatura analizada coincide en un hallazgo estructural: la industria de la construcción sufre de un rezago tecnológico y de seguridad significativo en comparación con la industria manufacturera.

#### *3.1.1 Lecciones del "Gemelo Digital" (Manufactura vs. Construcción)*

El concepto de "Gemelo Digital" (Digital Twin) se ha convertido en el estándar para la Industria 4.0. Sin embargo, su implementación en la construcción enfrenta obstáculos que la manufactura ya ha superado. Según el estudio comparativo realizado por Abanda et al. (2025), mientras que la industria manufacturera aplica el gemelo digital a lo largo de **siete fases** del ciclo de vida del producto (desde la generación del concepto hasta el reciclaje), la construcción tiende a limitar su uso a fases aisladas, principalmente operación y mantenimiento [2]

El análisis revela que la construcción enfrenta "desafíos aún mayores" debido a la falta de unificación de estándares y, críticamente, a la debilidad en la protección de datos. A diferen cia de las fábricas que operan en redes cerradas, los proyectos de construcción requieren compartir datos sensibles en entornos abiertos. Abanda et al. concluyen con cinco lecciones clave que la construcción debe adoptar de la manufactura: (1) acelerar el despliegue de hardware (sensores),

(2) unificar estándares de definición, (3) aplicar la tecnología al ciclo de vida completo, (4) mejorar la protección de datos y propiedad intelectual, y (5) aumentar la apertura al cambio cultural [2]

#### *3.1.2 La Inercia Estructural (Caso Kazajistán)*

La vulnerabilidad no es solo técnica, sino sistémica. En el contexto de economías en desarrollo, Salykov et al. (2025) analizaron la transformación digital en Kazajistán. Aunque el país ha alcanzado el puesto **36 en el ranking mundial de competitividad digital** gracias a estrategias gubernamentales (2023-2029), el estudio encontró que la seguridad de los datos sigue siendo un "desafío persistente". La investigación concluye que la integración de tecnologías como IoT y BIM es crucial para el crecimiento, pero sin inversiones paralelas en ciberseguridad y adaptación regulatoria, la digitalización expone al sector a riesgos de soberanía de datos y espionaje [1]

### 3.2 El Factor Humano y la Cultura Organizacional

Contrario a la percepción tecnocéntrica del mercado, la revisión señala que el eslabón más débil es el ser humano y la falta de disciplina organizacional.

#### *3.2.1 Percepción de Riesgo y Enfoque Individual (Malasia)*

Un estudio cuantitativo realizado por Isa et al. (2024) en Malasia evaluó el impacto de las amenazas cibernéticas en las partes interesadas (stakeholders). Utilizando el **Índice de Importancia Relativa (RII)**, los encuestados clasificaron la "mejora de la seguridad del sitio de construcción" como el segundo beneficio más alto de la tecnología (RII Ranking 2). Sin embargo, paradójicamente, los hallazgos mostraron que los sistemas de ciberseguridad corporativos son "poco profundos". La industria no se percibe como un objetivo principal de ataques, lo que lleva a una estrategia de defensa basada en el "enfoque individual": la seguridad depende de que cada empleado actualice su antivirus personal, una medida insuficiente ante amenazas avanzadas [11]

#### *3.2.2 Privacidad y Resistencia al Monitoreo (Nueva Zelanda)*

La resistencia cultural también se manifiesta en el sitio de obra. Wu et al. (2022) realizaron una encuesta en Nueva Zelanda (N=236 participantes) sobre la adopción de Tecnologías de Monitoreo de Empleados en Tiempo Real (REMT). Los resultados mostraron una preparación moderada-alta: la afirmación "Creo que el monitoreo de empleados aumenta la eficiencia" obtuvo el puntaje medio más alto (**5.18 sobre 7**). No obstante, al aplicar la Teoría de Gestión de la Privacidad de la Comunicación (CPM), se detectó una barrera significativa: la falta de comprensión sobre cómo se protegen los datos recolectados genera desconfianza. Sin protocolos claros de anonimización, los trabajadores perciben el monitoreo como una herramienta de control punitivo más que de seguridad [12]

#### *3.2.3 La Amenaza de Terceros (Reino Unido)*

Profundizando en la dinámica interna, Badi y Nasaj (2024) aplicaron el modelo **McKinsey 7S** en firmas del Reino Unido. Su análisis estadístico jerarquizó los elementos que más influyen en la efectividad de la ciberseguridad. Los resultados destacaron que, más allá del "hardware" o "software", las "**Relaciones con Terceros**" y el "**Cumplimiento Normativo**" son los factores críticos de éxito. Esto valida que en la construcción, donde la subcontratación es la norma, la seguridad de una empresa principal es tan vulnerable como la de su subcontratista menos protegido [5]

### 3.3 Paradojas Tecnológicas: Vulnerabilidades en Herramientas Emergentes

La investigación revela una paradoja inquietante: las mismas tecnologías diseñadas para optimizar la eficiencia del sector están introduciendo vulnerabilidades críticas debido a una implementación que prioriza la funcionalidad operativa sobre la seguridad de la información.

#### *3.3.1 Inteligencia Artificial Generativa (ChatGPT)*

La irrupción de la Inteligencia Artificial Generativa ha marcado un nuevo hito de vulnerabilidad. Herramientas como ChatGPT se han integrado rápidamente en tareas administrativas y de gestión de proyectos. Sin embargo, según el análisis bibliométrico de Sonkor y García de Soto (2025), existen algunos riesgos especiales para la privacidad. Se identificaron tres grupos de riesgo principales al examinar la coocurrencia de términos:

1. Grupo Rojo (Privacidad y Ética): riesgos de acceso no autorizado y filtración de información cuando los modelos se entrenan con detalles confidenciales de proyectos[6].
2. Grupo Verde (Ciberataques y Vulnerabilidades): la IA puede crear código malicioso (malware) y ser utilizada para llevar a cabo tipos más avanzados de ataques de ingeniería social [6].
3. Grupo Azul (Sesgo y Precisión): Inevitablemente, problemas de "alucinaciones" (información falsa generada con confianza) que conducen a errores en la toma de decisiones técnicas [6].

Los autores concluyen que la falta de transparencia en cómo se procesan los datos de los usuarios convierte a estas herramientas en una "caja negra" de riesgo para la propiedad intelectual [6].

#### *3.3.2 Contratos Inteligentes: Potenciales vs. Barreras (Caso Arabia Saudita)*

Por otro lado, los contratos inteligentes (Smart Contracts) basados en Blockchain se presentan como la solución para automatizar pagos y reducir conflictos. Sin embargo, un estudio cuantitativo en el mercado de la construcción de Arabia Saudita muestra una realidad compleja. Alfalah et al. (2024) encuestaron a 50 profesionales y encontraron que, aunque el 85.2% está de acuerdo en que el IoT es una tecnología importante para facilitar estos contratos, persisten 19 barreras significativas [7].

Entre ellas, destacan las "preocupaciones por la ciberseguridad" y la fiabilidad de los datos en sistemas distribuidos. La inmutabilidad del Blockchain es una ventaja, pero si el código del contrato tiene vulnerabilidades, los fondos del proyecto pueden quedar comprometidos irreversiblemente, generando resistencia entre los actores del sector [7].

### 3.4 Marcos de Solución y Estrategias de Mitigación

Frente a este panorama de amenazas, la revisión de literatura arroja propuestas concretas que permiten transitar del diagnóstico a la acción, validadas mediante casos de estudio y modelos matemáticos.

#### *3.4.1 Estandarización de Reportes: Validación del Modelo CISS*

Uno de los hallazgos más pragmáticos es la validación del modelo de Escala de Gravedad de Incidentes de Ciberseguridad (CISS). Yao, Mantha y García de Soto (2025) aplicaron este modelo a un caso de estudio real: un incidente de phishing en una empresa de ingeniería y contratación en los Emiratos Árabes Unidos, durante un proyecto comercial de 5 millones de dólares [8].

El modelo permitió calcular un puntaje de severidad exacto de 1.95 (en una escala de 0 a 10), derivado de la siguiente ponderación:

$$CISS = 0.9 \times Severidad + 0.1 \times Criticalidad$$

El análisis desglosó el impacto en tres dimensiones: Individual (Puntaje 1.5), Financiero (Puntaje 0, debido a la contención rápida) y Operativo (Puntaje 5, por la interrupción de tareas) [8].

Esta cuantificación demuestra que el CISS es una herramienta viable para estandarizar reportes y comparar la gravedad de incidentes entre diferentes organizaciones.

#### *3.4.2 Automatización: Machine Learning y Explicabilidad (SHAP)*

Dada la escasez de expertos en ciberseguridad en las constructoras, la automatización es necesaria. Yao y García de Soto (2024) desarrollaron un marco de 6 módulos que integra técnicas de Aprendizaje Automático (Machine Learning) para identificar y estimar riesgos cibernéticos automáticamente [10].

El modelo utiliza Redes Neuronales Artificiales (ANN) como motor de predicción. Una innovación clave es la incorporación del análisis de valores SHAP (SHapley Additive exPlanations) para la priorización de factores de riesgo [10]. Esta técnica permite "abrir la caja negra" de la IA y cuantificar la contribución exacta de cada variable (ej. falta de capacitación, software obsoleto) a la predicción de riesgo, proporcionando a los gerentes una lista priorizada para la mitigación proactiva.

#### *3.4.3 Defensa Colectiva: El Modelo ISAC (Caso Noruega)*

Lo más importante es que se trata de trabajar juntos. Una investigación empírica en Noruega muestra que, aunque el sector puede carecer de fondos suficientes para un Equipo de Respuesta a Emergencias (CERT) especializado y dedicado exclusivamente a la construcción, existe una necesidad urgente de formar foros de intercambio de información. Skytterholm y Jaatun (2023) han demostrado que los actores de la industria buscan facilitar el intercambio de conocimientos sobre amenazas para mejorar su defensa colectiva, con énfasis en el establecimiento de un Centro de Intercambio y Análisis de Información (ISAC) [13].

## 4. Conclusiones

Este trabajo ha facilitado la identificación de la crisis de ciberseguridad en la industria inmobiliaria y de la construcción, mapeando un panorama de riesgo sistémico para el éxito de la transformación digital. Las siguientes conclusiones clave se derivan de la revisión del trabajo científico más reciente:

**Primera: La brecha de madurez es estructural.** También está claro que la construcción se está llevando a cabo con un agujero de seguridad mucho más denso que la manufactura. Esta falta de estándares uniformes en herramientas vitales como los Gemelos Digitales y los Pasaportes de Materiales significa que la propiedad intelectual se convierte en objeto de riesgo de espionaje industrial. El sector necesita acelerar la transición hacia hardware seguro y unificar los protocolos de datos para mitigar esta brecha.

**Segundo: este es un riesgo humano y organizacional.** La tecnología avanza más rápido que la cultura de seguridad. La percepción del riesgo es baja (como se ve en Malasia), y la seguridad se atribuye erróneamente a la responsabilidad individual. Pero la gestión de la cadena de suministro es su punto ciego: la seguridad de una empresa central es tan sensible como la de sus subcontratistas.

**Tercero: La gobernanza es crítica para la innovación.** Herramientas como ChatGPT y los Contratos Inteligentes aumentan la eficiencia, pero tienen vectores de ataque previamente no detectados: privacidad y vulnerabilidades de código. Toda su adopción debe ir de la mano con marcos de gobernanza de datos desde su fase de diseño (Privacidad desde el Diseño).

**Cuarta: La solución es la estandarización y la defensa colectiva.** Finalmente, se concluye que la importación de soluciones genéricas de TI es ineficaz. La industria requiere adoptar marcos específicos como el modelo CISS para métricas objetivas y algoritmos de Machine Learning para la predicción de riesgos. Además, es imperativo transitar hacia un modelo colaborativo (ISAC), entendiendo que la ciberseguridad no es una ventaja competitiva individual, sino un requisito sistémico para la sostenibilidad de la Construcción 4.0.

## 3.Referencias


[1] A. Salykov, U. Z. Shalbolova, y A. Junusova, «Transformation in Kazakhstan's construction industry amidst digitalisation of the economy», Infrastructure Asset Management. ICE Publishing, 2024. doi: 10.1680/jinam.24.00037.

[2] F. H. Abanda, N. Jian, S. E. Adukpo, V. V. Tuhaise, y M. Blanche Manjia, «Digital twin for product versus project lifecycles' development in manufacturing and construction industries», Journal of Intelligent Manufacturing, vol. 36, n.o 2. Springer, pp. 801-831, 2025. doi: 10.1007/s10845-023-02301-2.

[3] Ž. Turk, B. García de Soto, B. R. K. Mantha, A. MacIel, y A. Georgescu, «A systemic framework for addressing cybersecurity in construction», Automation in Construction, vol. 133. Elsevier B.V., 2022. doi: 10.1016/j.autcon.2021.103988.

[4] N. K. Bús y Z. Nyikes, «Cyber Security Challenges in Construction», Advanced Sciences and Technologies for Security Applications, vol. Part F2433. Springer, pp. 509-518, 2024. doi: 10.1007/978-3-031-47990-8_44.

[5] S. M. Badi y M. Nasaj, «Cybersecurity effectiveness in UK construction firms: an extended McKinsey 7S model approach», Engineering, Construction and Architectural Management, vol. 31, n.o 11. Emerald Publishing, pp. 4482-4515, 2024. doi: 10.1108/ECAM-12-2022-1131.

[6] M. S. Sonkor y B. García de Soto, «Using ChatGPT in construction projects: unveiling its cybersecurity risks through a bibliometric analysis», International Journal of Construction Management, vol. 25, n.o 7. Taylor and Francis Ltd., pp. 741-749, 2025. doi: 10.1080/15623599.2024.2355782.

[7] G. Alfalah, A. Al-Sakkaf, E. Mohammed Abdelkader, S. Rawdhan, M. E. Shaawat, y O. S. D. Alshamrani, «Studying Potentials and Barriers of Successful Implementation of Smart Contracts in Saudi Arabia's Construction Industry», Advances in Civil Engineering, vol. 2024, n.o 1. John Wiley and Sons Ltd, 2024. doi: 10.1155/adce/9646556.

[8] D. Yao, B. R. K. Mantha, y B. G. de Soto, «Implementation of the Cybersecurity Incident Severity Scale (CISS) to Assess Cyber Incidents in the Construction Sector», Proceedings of the International Symposium on Automation and Robotics in Construction. International Association for Automation and Robotics in Construction (IAARC), pp. 657-664, 2025. doi: 10.22260/ISARC2025/0086.

[9] S. D. Siriwardhana, R. C. Moehler, y. Fang, «Exploring the Determinants of Construction 4.0 Implementation in Australian Construction Industry: A SWOT Analysis», Lecture Notes in Civil Engineering, vol. 591 LNCE. Springer Science and Business Media Deutschland GmbH, pp. 830-841, 2025. doi: 10.1007/978-981-96-4051-5_80.

[10] D. Yao y B. García de Soto, «Integrating Machine Learning for Cyber Risk Analysis in Construction 4.0», Lecture Notes in Civil Engineering, vol. 629 LNCE. Springer Science and Business Media Deutschland GmbH, pp. 76-91, 2025. doi: 10.1007/978-3-031-87364-5_7.

[11] R. Isa, H. E. A. Baharuddin, y A. F. Othman, «Impacts of Cybersecurity Threats on Construction Stakeholders in Malaysia Amidst Industrial Revolution 4.0», Built Environment Journal, vol. 21, n.o S1. MARA University of Technology, pp. 49-58, 2024. doi: 10.24191/bej.v21iSI.2445.

[12] R. W. Wu, T. W. Yiu, y M. Babaeian Jelodar, «Real-time Employee Monitoring Technologies in the Construction Sector - Effect, Readiness and Theoretical Perspectives: The case of New Zealand», IOP Conference Series: Earth and Environmental Science, vol. 1101, n.o 8. Institute of Physics, 2022. doi: 10.1088/1755-1315/1101/8/082010.

[13] A. N. Skytterholm y M. G. Jaatun, «Exploring the Need for a CERT for the Norwegian Construction Sector», Springer Proceedings in Complexity. Springer Science and Business Media B.V., pp. 57-73, 2023. doi: 10.1007/978-981-19-6414-5_4.