La Ciberseguridad como Capacidad Estratégica: Relación con la Adopción Digital Gubernamental y la Efectividad Institucional

Amalia Hernandez Bonilla[1]
[1]Universidad Nacional Autónoma de Honduras, Honduras, *amalia.hernandez@unah.edu.hn*

Abstract: *The growing use of digital technologies, including artificial intelligence, increases the need to strengthen strategic cybersecurity capabilities to sustain digital transformation processes; while this expansion creates opportunities for institutions and organizations, it also heightens reliance on digital services and exposure to cyber risks. This study examines a time-ordered model in 150 countries, where the 2016 government digital adoption rate acts as an antecedent (X), Government Effectiveness in 2023 as a mediator (M), and the 2024 national cybersecurity capacity as an outcome (Y). Official public indicators, Pearson correlations, ordinary least squares regression with robust standard errors (HC3), and percentile bootstrap inference of the indirect effect with 5,000 resamples were used. All three bivariate associations were positive (DAI–GE: r = 0.564; DAI–GCI: r = 0.694; GE–GCI: r = 0.628; all with p < 0.001). The indirect effect was also positive (a×b = 30.995; 95% bootstrap CI [18.032, 45.680]). Positive associations were observed among the three indicators, along with a statistically significant positive indirect component in the DAI→GE→GCI specification. The reference years organize the measurements used but do not allow for observation of the evolution of each country or the identification of a causal mechanism. The results are interpreted as exploratory associations among national indicators.*

Keywords: *Dynamic capabilities, strategic cybersecurity, government digital adoption, institutional effectiveness, digital transformation.*

Resumen: *El creciente uso de tecnologías digitales incluida la inteligencia artificial incrementa la necesidad de fortalecer capacidades estratégicas de ciberseguridad que permitan sostener procesos de transformación digital pues por lo anterior se ha ampliado las oportunidades de las instituciones y organizaciones, pero también ha incrementado la dependencia de los servicios digitales y la exposición a riesgos cibernéticos. Este estudio examina un modelo temporalmente ordenado en 150 países, donde la adopción digital gubernamental de 2016 actúa como antecedente (X), Government Effectiveness de 2023 como mediador (M) y la capacidad nacional de ciberseguridad de 2024 como resultado (Y). Se utilizaron indicadores públicos oficiales, correlaciones de Pearson, regresión por mínimos cuadrados ordinarios con errores estándar robustos HC3 e inferencia bootstrap percentil del efecto indirecto con 5,000 remuestras. Las tres asociaciones bivariadas fueron positivas (DAI–GE: r = 0.564; DAI–GCI: r = 0.694; GE–GCI: r = 0.628; todas con p < 0.001). El efecto indirecto también fue positivo (a×b = 30.995; IC bootstrap del 95 % [18.032, 45.680]). Se observaron asociaciones positivas entre los tres indicadores y un componente indirecto estadístico positivo en la especificación DAI→GE→GCI. Los años de referencia ordenan las mediciones utilizadas, pero no permiten observar la evolución de cada país ni identificar un mecanismo causal. Los resultados se interpretan como asociaciones exploratorias entre indicadores nacionales.*

Palabras clave: *Capacidades dinámicas, ciberseguridad estratégica, adopción digital gubernamental, efectividad institucional, transformación digital.*

I. Introducción

Estamos en la era de la digitalización, la cual ha cambiado la manera en que las organizaciones crean valor, coordinando mejor los procesos y rediseñando los servicios que brindan. Este cambio no se limita a incorporar herramientas: transforma rutinas, capacidades y relaciones con los usuarios. Vial explica la transformación digital como un proceso de cambio organizacional provocado por combinaciones de tecnologías digitales, mientras Verhoef et al. distinguen etapas que van desde la digitalización de información hasta la reconfiguración integral de la organización. Estas perspectivas coinciden en que el resultado depende tanto de la tecnología como de las respuestas estratégicas y organizacionales que la acompañan [1], [2].

A medida que aumenta la dependencia de plataformas y datos, también crece la exposición a interrupciones de servicios, fraude, pérdida de información y deterioro de la confianza en las instituciones y organizaciones afectadas [3], [4].

Desde la teoría de capacidades dinámicas, las organizaciones responden a entornos cambiantes mediante la identificación de amenazas y oportunidades, la movilización de recursos y la reconfiguración de sus prácticas. Warner y Wäger sitúan la transformación digital como un proceso continuo de renovación estratégica, Yeow et al. muestran que la alineación digital requiere ajustes coordinados en estructuras y recursos, y Teece vincula estas capacidades con la adaptación de modelos de negocio y formas de creación de valor [5], [6], [7].

Lo anterior nos permite comprender la ciberseguridad de un modo diferente. En lugar de tratarla de manera aislada puede analizarse como una capacidad estratégica que articula normas, tecnología, conocimientos, cultura y aprendizaje para gestionar riesgos en entornos digitales.

Estudios recientes relacionan la gestión del riesgo cibernético con la resiliencia organizacional, especialmente cuando las organizaciones enfrentan grandes dificultades, presión regulatoria y dependencia de terceros [8], [9].

La literatura permite distinguir dos separaciones: entre los estudios técnicos de seguridad de la información y los trabajos de

estrategia y transformación digital, y entre la investigación organizacional y los análisis con indicadores nacionales. Este estudio aborda el segundo nivel mediante una comparación internacional [8], [10], [11].

Este estudio examina las relaciones entre adopción digital gubernamental, efectividad institucional y capacidad nacional de ciberseguridad en 150 países. La especificación se organiza según los años de referencia: DAI 2016→Government Effectiveness 2023→GCI 2024. Se plantean tres preguntas: ¿qué asociación existe entre DAI y efectividad institucional?, ¿cómo se relacionan ambos indicadores con la capacidad nacional de ciberseguridad?, y ¿qué componente indirecto estadístico se estima al incorporar la efectividad institucional como variable intermedia? Esta especificación es exploratoria y no identifica relaciones causales [1], [8], [12].

El estudio articula la discusión de ciberseguridad estratégica con la perspectiva de capacidades, sin medir directamente capacidades dinámicas organizacionales. Su aporte metodológico consiste en documentar la integración y depuración de indicadores públicos internacionales. Además, ofrece contexto para investigar posteriormente ciberseguridad, innovación digital y resiliencia en cooperativas [11], [13], [14], [15].

II. MARCO CONCEPTUAL Y ANTECEDENTES EMPÍRICOS

A. Capacidades Dinámicas y Transformación Digital

La teoría de capacidades dinámicas parte de una pregunta central: por qué algunas organizaciones pueden adaptarse, renovar sus recursos y sostener su desempeño cuando el entorno cambia. En contextos digitales, esa capacidad se expresa en la detección de oportunidades, la movilización de inversiones y la transformación de procesos y estructuras. Teece sitúa estas actividades en la base de la renovación estratégica, mientras Warner y Wäger describen microfundamentos específicos para la transformación digital [7], [5].

Yeow et al. muestran que la alineación con una nueva estrategia digital no ocurre de forma lineal. Requiere ajustes sucesivos entre la estrategia y las capacidades disponibles. Priyono y Hidayat complementan esta idea al identificar caminos alternativos para alinear recursos, estrategias y capacidades en procesos de innovación abierta. En conjunto, estos trabajos sugieren que la capacidad estratégica se construye mediante combinaciones de recursos y no mediante la adquisición aislada de tecnología [6], [13]. La evidencia del sector financiero palestino añade una perspectiva sobre la madurez digital: su desarrollo se ha estudiado en relación con las capacidades dinámicas y la planificación estratégica. Ese antecedente ayuda a explicar por qué adoptar tecnología exige decisiones coordinadas sobre recursos y dirección, sin suponer que la madurez de una organización pueda observarse directamente mediante los indicadores nacionales de este estudio [16].

La transformación digital tampoco equivale a automatización. Vial la caracteriza como un proceso que altera las rutas de creación de valor, mientras Verhoef et al. la vinculan con cambios en la experiencia del usuario, los modelos de negocio y las capacidades organizacionales. Por esta razón, la adopción de plataformas digitales puede considerarse un componente habilitador, pero no una medida suficiente de transformación o innovación [1], [2].

La innovación digital incorpora propiedades de recombinación, modularidad y generatividad. Nambisan et al. explican que estas propiedades modifican la manera de organizar la innovación, mientras Yoo et al. destacan que la convergencia entre componentes digitales crea nuevas posibilidades de diseño y coordinación. Esta literatura permite interpretar la adopción digital como una condición sobre la cual pueden desarrollarse procesos innovadores más amplios [17], [18].

En este artículo se utiliza el componente gubernamental del Digital Adoption Index. El indicador no mide innovación organizacional ni la calidad de un servicio específico. Su utilidad consiste en aproximar el grado en que el sector público ha incorporado tecnologías digitales en sus procesos. La distinción es necesaria para mantener coherencia entre el concepto analizado y el alcance real del indicador [1], [17], [19].

B. Ciberseguridad como Capacidad Estratégica

La seguridad de la información ha sido tratada durante décadas como un conjunto de controles destinados a preservar confidencialidad, integridad y disponibilidad. Aunque ese enfoque conserva relevancia, resulta limitado para explicar por qué organizaciones con tecnologías similares presentan resultados diferentes. Soomro et al. proponen una visión holística que combina personas, procesos, tecnología y gestión; Paananen et al. muestran que las políticas de seguridad son instrumentos de coordinación organizacional y no simples documentos de cumplimiento [3], [20].

La cultura y la conciencia de seguridad son parte de esa capacidad. Wiley et al. encuentran que las percepciones individuales se relacionan con el contexto cultural, mientras los modelos dirigidos a responsables de decisión integran factores humanos, técnicos y organizacionales. La capacidad cibernética surge así de rutinas y comportamientos que permiten prevenir, detectar, responder y aprender [4], [21].

Los estudios de ciberresiliencia amplían todavía más este planteamiento. Dupont describe tensiones entre control, flexibilidad y aprendizaje; Durst et al. relacionan la gestión del riesgo cibernético con la resiliencia en condiciones de turbulencia; y Gaudenzi y Baldi señalan que la distancia entre la percepción del riesgo y la acción efectiva puede limitar la respuesta organizacional [8], [9], [22].

Annarelli y Palombi sitúan las capacidades de digitalización en momentos distintos de la ciberresiliencia. El acceso y uso de información, el aprendizaje y la reconfiguración de recursos pueden contribuir a prepararse para una perturbación y a adaptar la organización después de ella. Este marco fortalece la interpretación estratégica de la ciberseguridad, aunque su alcance conceptual no permite atribuir esos procesos internos a la puntuación nacional del GCI [23]. Esta evidencia sugiere que la ciberseguridad puede funcionar como una capacidad estratégica cuando se integra en la dirección, la gestión de riesgos, el diseño de servicios y la continuidad. Su contribución no se reduce a evitar incidentes: también crea condiciones para que la organización adopte tecnología con mayor claridad sobre responsabilidades, riesgos y mecanismos de recuperación [10], [11].

A nivel país, el Global Cybersecurity Index reúne dimensiones legales, técnicas, organizacionales, de desarrollo de capacidades y cooperación. Por ello, su puntuación general aproxima un compromiso institucional amplio y no únicamente la disponibilidad de controles tecnológicos. Esta característica lo hace adecuado para explorar relaciones entre capacidad cibernética, adopción digital y efectividad institucional [24].

C. Resiliencia Organizacional y Efectividad Institucional

La resiliencia organizacional ha evolucionado desde una noción de recuperación posterior a la crisis hacia una perspectiva basada en capacidades. Duchek la organiza en anticipación, afrontamiento y adaptación, mientras Hillmann y Guenther advierten que el concepto debe utilizarse con precisión para evitar que se convierta en una etiqueta demasiado amplia. La resiliencia implica responder a la perturbación, pero también aprender y ajustar la organización [12], [25].

En empresas chinas, Zhang et al. encontraron que la innovación exploratoria y la de explotación intervenían en la relación estudiada entre transformación digital y resiliencia [26]. Los resultados de Putritamara et al. en MIPYMES apícolas muestran, a su vez, diferencias entre tipos de empresa [27]. Kwiotkowska identificó en plantas de cogeneración distintas combinaciones de madurez digital y capacidades dinámicas vinculadas con la resiliencia [28]. En conjunto, estos trabajos respaldan una interpretación sensible a los recursos y al contexto de cada organización; ninguno convierte el DAI gubernamental en una medida de innovación o resiliencia empresarial.

Los estudios sobre transformación digital muestran que las capacidades tecnológicas pueden fortalecer la resiliencia cuando se combinan con aprendizaje, innovación y respuesta ágil. Awad et al. identifican rutas mediadas por aprendizaje e innovación; Zhang et al. relacionan transformación digital con innovación ambidiestra; y otros trabajos señalan que las capacidades dinámicas facilitan la continuidad y adaptación frente a escenarios adversos [14], [29]**.** También existen aportes que conectan la capacidad digital con el contexto institucional. Dubey et al. incorporan la efectividad gubernamental al análisis de capacidades digitales y resiliencia de cadenas de suministro, mientras estudios sobre apoyo público muestran que las condiciones del entorno pueden fortalecer o limitar la respuesta organizacional. Estos resultados justifican examinar la efectividad institucional como una dimensión contextual, aunque no como una medición directa de resiliencia [15], [30]**.**

Government Effectiveness recoge percepciones sobre calidad de los servicios públicos, calidad de la administración, formulación de políticas y credibilidad institucional. El indicador no mide anticipación, recuperación o adaptación organizacional. En este trabajo se emplea como aproximación al desempeño institucional y se mantiene separada su interpretación de la resiliencia organizacional definida por la literatura [12], [24], [25]**.**

El argumento conceptual del estudio es, por tanto, prudente. Una mayor capacidad nacional de ciberseguridad puede acompañar niveles superiores de adopción digital, y ambas capacidades pueden relacionarse con instituciones más efectivas. Esta estructura es compatible con la teoría de capacidades dinámicas, pero requiere ser interpretada como asociación entre condiciones nacionales y no como secuencia causal comprobada [5], [8], [15]**.**

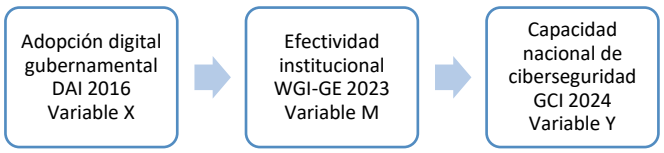


Fig. 1 Relación analítica entre las variables del estudio
No se les atribuye equivalencia con constructos organizacionales más amplios.

La Fig. 1 presenta la especificación del análisis indirecto exploratorio: DAI gubernamental 2016 como variable explicativa, Government Effectiveness 2023 como variable intermedia y GCI 2024 como variable de resultado. Las flechas representan las rutas estimadas mediante regresiones. El orden de los años de referencia no demuestra una secuencia causal ni permite observar cambios dentro de cada país. El DAI aproxima adopción digital gubernamental, Government Effectiveness aproxima efectividad institucional y el GCI aproxima compromiso nacional con la ciberseguridad [31], [32], [19], [24]**.**

III. METODOLOGÍA

A. Diseño y unidad de análisis

La investigación utiliza un diseño cuantitativo, no experimental, transversal y exploratorio. La unidad de análisis está constituida por países y no por organizaciones individuales. Esta decisión responde a la disponibilidad de indicadores internacionales comparables y al propósito de construir una lectura global que anteceda al análisis organizacional en cooperativas [24], [32].

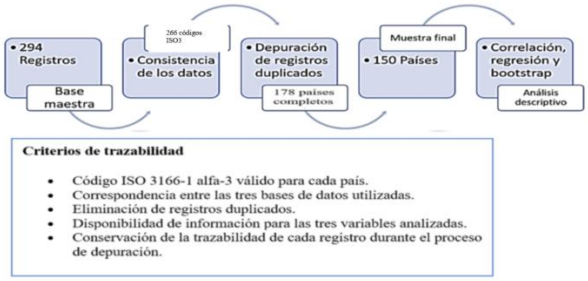


Fig. 2 Depuración de Registros
Del archivo inicial a la base completa y al subconjunto exploratorio.

El archivo inicial de integración contenía 294 filas, entre países, agregados regionales y observaciones duplicadas que no equivalen a 294 países. Al agruparlas por código ISO3 se identificaron 266 códigos únicos y 28 filas adicionales asociadas con códigos repetidos. En la revisión se detectó 27 asignaciones del puntaje GCI a un código de país incorrecto; los valores se cotejaron de nuevo con las fuentes DAI gubernamental 2016, Government Effectiveness 2023 y GCI 2024. Tras excluir agregados, resolver las correspondencias y exigir valores disponibles para las tres variables, se identificaron 178 países con información completa [19], [24], [32].

De los 178 países con datos completos se seleccionaron consecutivamente los primeros 150 registros del listado de trabajo facilitado por la autora, con el propósito de formar una muestra exploratoria. El orden y los códigos ISO3 de los 178 casos se conservan en la matriz de trazabilidad. Los otros 28 países también cuentan con los tres indicadores y quedaron fuera del subconjunto por su posición posterior al registro 150, no por datos faltantes. La selección no fue probabilística. Los resultados del subconjunto se contrastan con los obtenidos para los 178 países completos [19], [24], [32].

La diferencia entre los años de los indicadores constituye una condición relevante del diseño. El DAI corresponde a 2016, Government Effectiveness a 2023 y el GCI a 2024. La combinación se utiliza por cobertura y disponibilidad oficial, pero no representa una medición simultánea.[24], [32].

En figura 2 se distingue la depuración de registros de la selección exploratoria de 150 países. El proceso fue documentado en una matriz que conserva la fila de origen, la decisión de inclusión o exclusión y el motivo aplicado. Esta trazabilidad reduce el riesgo de incorporar agregados regionales o duplicados como si fueran países independientes [19], [24].

B. Variables y Operacionalización

TABLA I
OPERACIONALIZACIÓN DE VARIABLES

Variable	Indicador	Año	Escala	Fuente
Adopción digital Gubernamental Variable X	DAI – Government	2016	0–1	Banco Mundial [19]
Efectividad institucional Variable M	Government Effectiveness WGI-GE	2023	aprox. -2.5 a 2.5	WGI [24]
Capacidad nacional de Ciberseguridad Variable Y	Global Cybersecurity Index	2024	0–100	UIT [32]

Nota: El alcance conceptual se mantiene delimitado. Cálculos propios con la muestra depurada.

La selección de indicadores responde a tres criterios: reconocimiento internacional, cobertura amplia y disponibilidad pública. El DAI se interpreta como adopción digital gubernamental y Government Effectiveness como desempeño institucional, no como mediciones directas de innovación y resiliencia organizacional [1], [12], [19], [24].

C. Estrategia de Análisis

Se estimaron tres regresiones con constante: GE sobre DAI, GCI sobre DAI y GCI sobre DAI y GE conjuntamente. La ruta a corresponde a la asociación DAI–GE; la ruta b, a GE–GCI ajustada por DAI; la ruta c, a la asociación total DAI–GCI; y la ruta c′, a DAI–GCI ajustada por GE. El componente indirecto se calculó como a×b.

Las rutas describen asociaciones y no identifican efectos causales. La evaluación del componente indirecto se basó en el producto a×b y en un intervalo bootstrap percentil del 95 %, obtenido con 5,000 remuestras de países con reemplazo y semilla 2026092[31] [33], [34].

Las regresiones se estimaron mediante mínimos cuadrados ordinarios y su incertidumbre se evaluó con errores estándar robustos HC3. El bootstrap evita aproximar el intervalo del producto mediante una distribución normal, pero no corrige factores omitidos, selección no probabilística ni limitaciones de medición. El componente indirecto se interpreta como exploratorio [15], [19], [24], [32].

IV. RESULTADOS

A. Estadísticos Descriptivos

Dado que los indicadores tienen escalas y años de referencia distintos, sus magnitudes se interpretan por separado. Los resultados descriptivos corresponden a la muestra seleccionada y se contrastan posteriormente con los 178 países que disponen de información completa [19], [24], [32].

TABLA II
ESTADÍSTICOS DESCRIPTIVOS (N = 150)

Variable	Media	DE	Mín.	Mediana	Máx.
DAI Gov. 2016	0.5437	0.1777	0.1083	0.5519	0.9570
GE 2023	-0.0389	0.9938	-2.2754	-0.0927	2.3175
GCI 2024	69.5718	28.1747	0.0000	76.5000	100.0000

Nota: La Tabla II describe cada indicador por separado. Cálculos propios con la muestra depurada.

La Tabla II resume la distribución de los tres indicadores en los 150 países incluidos en el análisis principal. Se presentan la media, la desviación estándar, la mediana y los valores extremos para describir tanto el nivel central como la heterogeneidad de cada variable antes de examinar sus asociaciones [19], [24], [32].

Se muestra una dispersión amplia en las tres variables. La adopción digital gubernamental tiene una media de 0.5437 y valores entre 0.1083 y 0.9570. La mediana se encuentra próxima a la media, aunque la amplitud del rango muestra que la incorporación de tecnologías digitales en el sector público tampoco es homogénea. Esta variación es coherente con la diversidad de capacidades institucionales e infraestructura incluida en el índice (Tabla II) [19].

Government Effectiveness presenta una media de -0.0389 y una desviación estándar de 0.9938. Dado que el indicador se construye sobre una escala estandarizada, los valores positivos y negativos expresan posiciones relativas en la distribución internacional. La amplitud entre -2.28 y 2.32 permite analizar países con niveles institucionales contrastantes (Tabla II) [24]. El GCI registra una media de 69.57 puntos y una desviación estándar de 28.17, lo que refleja diferencias importantes en el compromiso nacional con la ciberseguridad. El rango completo, desde 0.00 hasta 100, confirma que los países incluidos se encuentran en etapas muy distintas de desarrollo cibernético (Tabla II) [32].

B. Correlaciones, *Regresiones y Componente Indirecto Exploratorio*

El patrón indica que los países con mayores puntuaciones de ciberseguridad tienden a presentar también un mayor nivel de adopción digital en el sector público. La magnitud es consistente con la idea de capacidades complementarias, aunque no establece cuál de ellas precede a la otra (Tabla III) [3], [8], [19], [24].

TABLA III
RUTA DE ANÁLISIS INDIRECTO EXPLORATORIO N=150

Ruta	B	EE HC3	β	R^2	p o IC 95 %
a: DAI → GE	3.153	0.372	0.564	0.318	<0.001
b: GE → GCI | DAI	9.830	1.866	0.347	0.564	<0.001
c: DAI → GCI total	110.046	8.159	0.694	0.482	<0.001
c′: DAI → GCI | GE	79.051	10.510	0.499	0.564	<0.001
Indirecto a×b	30.995	--	0.195	--	[18.032, 45.680]

Nota: B corresponde al coeficiente no estandarizado y β al coeficiente estandarizado.

La adopción digital gubernamental de 2016 se asoció positivamente con la efectividad institucional de 2023. Un incremento de una unidad en DAI se relacionó con un aumento promedio de 3.153 unidades en Government Effectiveness (a = 3.153; β = 0.564; p < 0.001). Dado que DAI se mide entre 0 y 1, una diferencia de 0.10 puntos en el índice equivale, en promedio, a 0.315 unidades de efectividad institucional.

A su vez, la efectividad institucional se relacionó positivamente con la capacidad nacional de ciberseguridad después de controlar la adopción digital (b = 9.830; β = 0.347; p < 0.001). La asociación total entre DAI y GCI fue c = 110.046 (β = 0.694; p < 0.001), mientras que la asociación directa se redujo a c′ = 79.051 (β = 0.499; p < 0.001) al incorporar Government Effectiveness. La identidad c = c′ + a×b se cumplió dentro del redondeo.

El efecto indirecto fue a×b = 30.995, con un intervalo bootstrap percentil del 95 % de [18.032, 45.680].

El intervalo no incluye cero. Una diferencia de 0.10 puntos en DAI corresponde, en la parametrización del modelo, a un componente indirecto estimado de aproximadamente 3.10 puntos de GCI. Esta equivalencia describe una asociación estadística entre países; no representa una mejora observada ni demuestra un mecanismo causal. El intervalo del efecto indirecto es percentil al 95 %, obtenido con 5,000 remuestras y semilla 2026092. Los resultados evidencian una relación positiva y estadísticamente significativa entre DAI y GE (β = 0.564, p < 0.001), así como entre GE y GCI, controlando DAI (β = 0.347, p < 0.001).

El efecto total de DAI sobre GCI también fue significativo (β = 0.694, p < 0.001). Al incorporar GE como variable mediadora, el efecto directo de DAI sobre GCI disminuyó a β = 0.499 (p < 0.001), mientras que el efecto indirecto fue significativo, con un intervalo de confianza del 95 % que no incluye el cero. Las asociaciones total y ajustada entre DAI y GCI permanecieron positivas, mientras el componente indirecto estimado fue distinto de cero según el intervalo bootstrap. Estos resultados describen una descomposición estadística de la asociación en la especificación propuesta, sin demostrar mediación causal. [32], [19], [24]. La Fig. 3 complementa el análisis al mostrar la dispersión de los países y los ajustes lineales descriptivos.

Las tres dispersiones muestran patrones positivos, coherentes con las correlaciones reportadas. Representan asociaciones entre indicadores nacionales medidos en distintos años y no permiten inferir causalidad ni realizar predicciones temporales. [32], [19], [24].

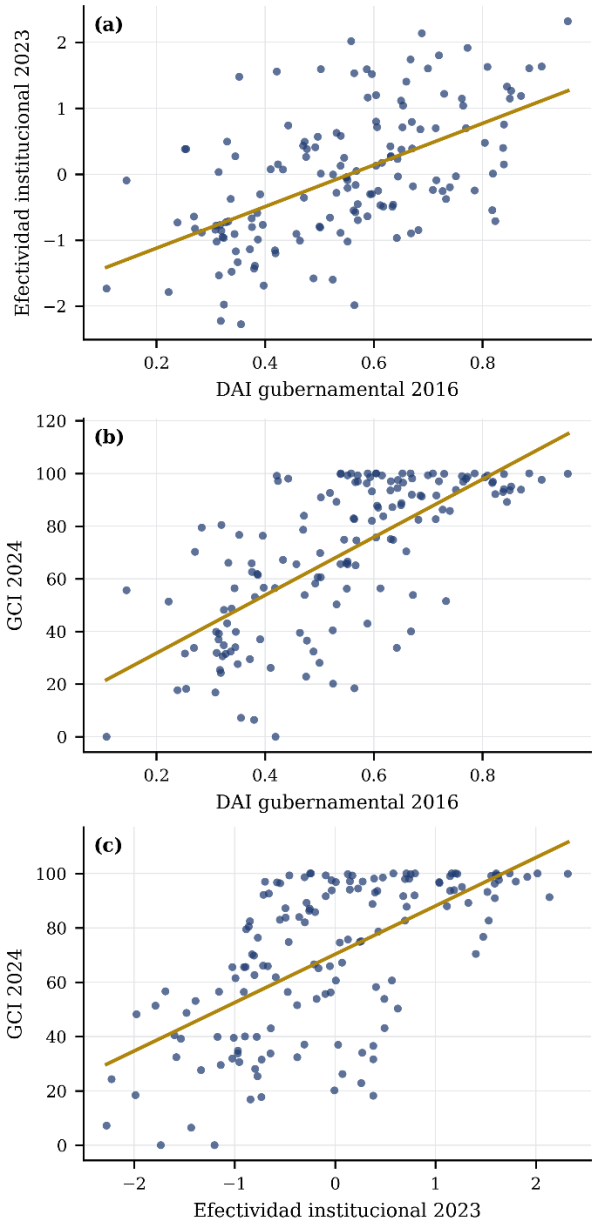


Fig. 3 Asociaciones observadas en 150 países
Cada punto es un pais. Las rectas son ajustes lineales descriptivos; sin implicación causal ni predicción temporal. Fuente: Cálculos propios.

V. DISCUSIÓN

La adopción digital gubernamental registrada en 2016 presenta una asociación positiva con la efectividad institucional de 2023 y con la puntuación de ciberseguridad de 2024. En la especificación propuesta, GE ocupa una posición intermedia. El estudio no observa cómo los Estados desarrollaron, coordinaron o reconfiguraron esas capacidades[3], [8], [10], [32].

La teoría de capacidades dinámicas orienta la discusión sobre la relación entre recursos digitales y capacidades institucionales. En esta especificación, Government Effectiveness ocupa una posición intermedia y presenta una asociación positiva con GCI después de ajustar por DAI. Sin embargo, el estudio no mide procesos de absorción, coordinación, financiación o reconfiguración. Estos procesos constituyen interpretaciones teóricas que deberán examinarse mediante diseños y mediciones específicos [5], [13]**.** [15], [32], [24].

El componente indirecto positivo es compatible con la especificación propuesta. No demuestra un proceso de maduración ni que una variación en DAI produzca mejoras institucionales o de ciberseguridad. Ingreso, capital humano, infraestructura, región y estabilidad política podrían contribuir a las asociaciones observadas [8], [35], [36], [11]. Esta interpretación también es coherente con la ciberresiliencia. Las organizaciones y sistemas resilientes no buscan eliminar toda perturbación; desarrollan capacidades para anticipar, responder, recuperar y adaptar prácticas. La ciberseguridad contribuye a ese proceso cuando se conecta con aprendizaje, continuidad, cultura y toma de decisiones [22], [9], [37], [12]**.**

Los resultados no permiten sustituir resiliencia organizacional por efectividad institucional. Government Effectiveness refleja una dimensión del contexto nacional y no las capacidades internas de una cooperativa, empresa o institución específica. La distinción protege la coherencia conceptual y señala la necesidad de continuar la investigación con instrumentos organizacionales directos [12], [24], [25]**.**

Para el sector cooperativo, el análisis funciona como antecedente internacional. Las cooperativas operan dentro de marcos nacionales que influyen en regulación, conectividad, proveedores y confianza digital. Sin embargo, un entorno favorable no reemplaza la necesidad de capacidades internas de gobernanza, gestión de riesgos, cultura y continuidad [8], [35], [11]**.**

La lectura directiva es especialmente relevante para organizaciones con recursos limitados. La ciberseguridad estratégica no implica comenzar por soluciones complejas; requiere priorizar activos, responsabilidades, proveedores, respaldos y respuesta. Cuando estas prácticas se integran con la adopción digital, pueden reducir la fragilidad que surge al digitalizar procesos sin fortalecer simultáneamente la capacidad de protección y recuperación [4], [10], [35], [38]**.** El estudio también contribuye al debate sobre medición. Los indicadores públicos permiten comparar países y observar patrones de alcance global, pero simplifican fenómenos organizacionales complejos. La claridad sobre lo que mide cada variable es tan importante como el resultado estadístico, especialmente cuando el objetivo es conectar evidencia macrocontextual con futuras investigaciones en cooperativas [1], [12], [24], [25].

VI. PRUEBAS DE CONSISTENCIA

A. Asociaciones no paramétricas

Las correlaciones de Pearson describen relaciones lineales y pueden ser sensibles a observaciones extremas. Para examinar si el patrón general dependía de esa condición, se calcularon correlaciones de Spearman sobre la misma muestra de 150 países. Los coeficientes fueron 0.695 para GCI–DAI, 0.645 para GCI–Government Effectiveness y 0.564 para DAI–Government Effectiveness, con $p < 0.001$ en los tres casos. La cercanía con los coeficientes de Pearson indica que el orden relativo de los países conserva la misma estructura de asociación (Tabla IV) [15], [24], [32]**.**

La coincidencia entre ambos métodos es relevante porque los indicadores internacionales suelen presentar asimetrías y diferencias amplias entre países. En este caso, el patrón se mantiene al analizar rangos y al limitar moderadamente los valores extremos. Los países mejor posicionados en capacidad cibernética tienden también a ocupar posiciones superiores en adopción digital y efectividad institucional, aun cuando el análisis se basa en rangos y no en distancias absolutas [2], [8], [15]**.**

TABLA IV
PRUEBAS DE CONSISTENCIA DE LAS ASOCIACIONES

Prueba	DAI–GE	GCI–GE	GCI–DAI
Pearson	0.564	0.628	0.694
Spearman	0.564	0.645	0.695
Winsorización 2.5%	0.559	0.627	0.696

Nota: La winsorización de 2.5 % se aplicó por variable, limitando tres valores en cada extremo de la muestra de 150 países; los países permanecieron en el análisis. Todos los coeficientes presentan $p < 0.001$. Cálculos propios con la muestra depurada.

B. Estimación robusta y valores extremos

El modelo conjunto de GCI 2024, con DAI gubernamental 2016 y Government Effectiveness 2023 como indicadores explicativos, se estimó mediante mínimos cuadrados ordinarios y errores estándar robustos HC3. La asociación ajustada de GE con GCI fue positiva ($B = 9.830$; EE HC3 = 1.866; $p < 0.001$), al igual que la de DAI con GCI ($B = 79.051$; EE HC3 = 10.510; $p < 0.001$). El modelo describió aproximadamente el 56.4 % de la variación observada en GCI en los 150 países (Tabla III). HC3 modifica la incertidumbre estimada, no los coeficientes de mínimos cuadrados [15], [24], [32].

También se aplicó una winsorización de 2.5% en ambos extremos de cada variable. Las correlaciones resultantes fueron prácticamente iguales a las originales: 0.696 para GCI–DAI, 0.627 para GCI–Government Effectiveness y 0.559 para DAI–Government Effectiveness. La estabilidad sugiere que el resultado principal no depende de las observaciones ubicadas en los extremos de la distribución (Tabla IV) [8], [15]**.**

En el modelo conjunto, los indicadores explicativos son DAI y Government Effectiveness. Con su correlación de 0.563703, el factor de inflación de la varianza es aproximadamente 1.47 para ambos, bajo una regresión con constante y esos dos indicadores

como únicos predictores. Este resultado no señala una inflación elevada de la varianza por colinealidad, aunque no demuestra independencia conceptual entre los indicadores.[5], [15].

Las pruebas de consistencia no corrigen las limitaciones temporales ni convierten el diseño en causal. Su función está acotada a verificar que las asociaciones se mantengan cuando se utilizan rangos, errores robustos y tratamiento moderado de valores extremos. El resultado fortalece la confianza en la estabilidad estadística del patrón, no en una dirección causal entre las variables [12], [25].

C. Sensibilidad frente a la base completa de 178 países

El análisis con los 178 países completos permite valorar cuánto cambian las estimaciones cuando se incorpora a los 28 países omitidos del subconjunto reconstruido. Se mantuvieron las mismas variables y especificaciones estadísticas para que la comparación refleje únicamente la composición de la muestra (Tabla V) [15], [24], [32].

TABLA V
CONTRASTE DE OCHO ESTIMACIONES CON N = 150 Y N = 178

Medida	N = 150	N = 178
r DAI–GE	0.563703	0.580450
r DAI–GCI	0.693955	0.693727
r GE–GCI	0.627739	0.624021
a: DAI→GE	3.153065	2.752097
b: GE→GCI | DAI	9.830024	9.990941
c: DAI→GCI	110.045605	98.442694
c′: DAI→GCI | GE	79.050901	70.946650
a×b	30.994704	27.496044

En los 178 países, el intervalo bootstrap percentil del 95 % para a×b fue [16.760, 39.676], frente a [18.032, 45.680] en los 150. Ambos intervalos se calcularon con 5,000 remuestras y semilla 2026092. La comparación evalúa sensibilidad a la composición de la muestra; no justifica por sí sola el recorte a 150 países [19], [24], [32].

VII. CONTRIBUCIONES DEL ESTUDIO

A. Contribución Conceptual

La primera contribución consiste en situar la ciberseguridad dentro de una conversación de dirección estratégica. La literatura técnica ha avanzado en controles, amenazas y cumplimiento, pero el análisis organizacional requiere comprender cómo esas prácticas se integran con decisiones, rutinas y capacidades. Al vincular el GCI con adopción digital y efectividad institucional, el estudio muestra que la ciberseguridad puede analizarse como parte de un sistema de capacidades complementarias [3], [22].

Esta lectura no pretende convertir todo control de seguridad en capacidad estratégica. La diferencia depende de la integración. Un recurso técnico se vuelve estratégicamente relevante cuando se conecta con gobernanza, aprendizaje, continuidad y objetivos de transformación. Ese argumento coincide con la teoría de capacidades dinámicas y con trabajos recientes que vinculan gestión del riesgo cibernético, innovación y resiliencia [5], [13], [8], [11].

La segunda contribución conceptual es la separación entre adopción e innovación digital. El DAI registra una forma de utilización tecnológica en el sector público, pero no permite observar la creación de nuevos servicios, modelos o procesos. El artículo utiliza esa información como condición habilitadora y reserva la innovación digital para la discusión teórica y para futuras mediciones organizacionales [1], [17], [18], [19].

B. Contribución metodológica

El estudio documenta la integración de indicadores internacionales mediante códigos ISO3 y registra las decisiones de depuración necesarias para obtener unidades comparables. El proceso permitió pasar de los registros iniciales a países identificados de forma única y con información disponible para las tres variables. Su aporte metodológico reside en hacer trazable la construcción de la base analítica, con el detalle de exclusiones y correspondencias consignado en la matriz de datos. Las fuentes de GCI y efectividad gubernamental documentan sus respectivos indicadores, mientras que las decisiones de integración corresponden a este estudio [24], [32].

La muestra de 150 países permite superar el alcance de análisis regionales preliminares y observar una diversidad mayor de configuraciones institucionales. Aun así, el tamaño de la muestra no elimina los problemas de medición. La contribución metodológica reside en combinar cobertura con transparencia sobre los años, las escalas y el significado de cada indicador [15], [24], [32].

La incorporación de correlaciones paramétricas y no paramétricas, errores robustos, winsorización y bootstrap ofrece una lectura más completa que una única correlación. Las distintas estimaciones convergen en relaciones positivas, lo que fortalece la consistencia interna del análisis. La conclusión se mantiene deliberadamente limitada a asociaciones observadas. Esta estabilidad se refiere a las comprobaciones especificadas y a las bases examinadas**;** no establece causalidad ni subsana el desfase temporal entre indicadores [8], [12], [15].

C. Contribución para la Investigación en Cooperativas

El artículo aporta el nivel macrocontextual del compendio doctoral. El primer estudio del compendio examinó bibliométricamente la producción sobre innovación y ciberseguridad en empresas digitalizadas de América Latina e identificó tendencias y vacíos de investigación [39]. El presente trabajo analiza relaciones mediante indicadores globales; y la siguiente fase trasladará los constructos al nivel organizacional. Esta secuencia permite evitar que el estudio en cooperativas se desarrolle sin una base teórica e internacional previa [11], [12], [14]. En la fase organizacional será necesario definir y medir, mediante instrumentos adecuados para cooperativas, la gobernanza cibernética, la cultura de seguridad, la gestión de riesgos, la innovación digital y la resiliencia. El resultado nacional no podrá utilizarse como sustituto de esas mediciones,

pero sí ayudará a interpretar las condiciones del entorno donde las organizaciones operan [8], [35], [14].

La futura comparación entre países y cooperativas también puede revelar diferencias entre capacidad nacional y capacidad organizacional. Una cooperativa puede construir prácticas maduras en un entorno nacional con brechas, mientras otra puede permanecer vulnerable aun cuando opere en un país mejor posicionado. Esa tensión constituye una línea de investigación relevante para dirección empresarial [9], [11], [38].

VIII. IMPLICACIONES PARA LA DIRECCIÓN EMPRESARIAL

La primera implicación es incorporar la ciberseguridad a la planificación de la transformación digital. Las decisiones sobre plataformas, canales, datos y proveedores deben incluir criterios de protección y continuidad desde el diseño. Esta integración evita que la seguridad sea tratada como una corrección posterior y la convierte en parte de la arquitectura del servicio [15], [4], [10]. La segunda es gestionar capacidades complementarias. Invertir en herramientas sin fortalecer políticas, responsabilidades, cultura y aprendizaje puede producir una seguridad aparente. Del mismo modo, digitalizar procesos sin preparar respuesta y recuperación puede trasladar riesgos operativos hacia plataformas críticas [21], [9].

La tercera es desarrollar indicadores comprensibles para la alta dirección. Además de incidentes, conviene observar disponibilidad, tiempos de recuperación, cumplimiento de proveedores, resultados de capacitación, pruebas de respaldo y riesgos asociados con nuevos servicios. Este enfoque facilita decisiones basadas en exposición y continuidad, no únicamente en adquisición tecnológica [4], [35], [11].

En cooperativas, la confianza de los socios es un activo central. La protección de datos y la continuidad de servicios inciden en la percepción de legitimidad y seguridad. Por ello, la ciberseguridad debe vincularse con la estrategia, el control interno y la innovación de servicios, manteniendo una implementación gradual acorde con tamaño, recursos y nivel de digitalización [35], [11], [38]. Estas orientaciones proceden del marco conceptual y no constituyen intervenciones evaluadas por el análisis nacional. Su pertinencia y sus resultados deberán examinarse directamente en cooperativas.

IX. LIMITACIONES Y LÍNEAS FUTURAS

La especificación DAI 2016→Government Effectiveness 2023→GCI 2024 ordena los indicadores según sus años de referencia. Sin embargo, una medición de cada indicador no permite observar trayectorias dentro de los países, comprobar la estabilidad del DAI ni establecer cuándo se desarrollaron las capacidades institucionales y de ciberseguridad. El orden de las fechas no identifica un mecanismo causal ni descarta explicaciones alternativas [19], [24], [32].

Una segunda limitación es conceptual. El GCI aproxima el compromiso nacional con la ciberseguridad; el DAI gubernamental mide adopción digital, no innovación; y Government Effectiveness mide efectividad institucional, no resiliencia organizacional. Estudios futuros deberán usar indicadores recientes y medidas directas de innovación, adaptación y continuidad [1], [12], [25].

Una tercera limitación es la heterogeneidad entre países. Las asociaciones podrían reflejar diferencias compartidas de ingreso, capital humano, infraestructura digital, calidad regulatoria o región que no se controlaron en estos modelos. Tampoco pueden trasladarse automáticamente los resultados nacionales a las cooperativas [2], [15], [30].

La siguiente fase deberá recolectar datos primarios en estas organizaciones y medir su gobernanza cibernética, innovación digital y resiliencia, con participación de directivos y responsables de gestión [8], [35], [14].

Podrá examinar, por separado, recursos, colaboración externa y adaptabilidad: Mu et al. estudiaron dimensiones de resiliencia de nicho en empresas manufactureras [40] mientras Saemaldaher y Emeagwali analizaron vínculos entre innovación abierta, adaptabilidad y resiliencia [41]. Estos trabajos orientan preguntas para cooperativas; no son resultados de la comparación nacional. Una extensión posterior podría emplear indicadores comparables medidos en varios años e incorporar controles por ingreso, capital humano, infraestructura digital y región para examinar la estabilidad de estas asociaciones.

El subconjunto exploratorio se formó por selección consecutiva no probabilística de los primeros 150 registros del listado documentado de 178 países completos. Los 28 restantes tenían datos en los tres indicadores; quedaron fuera por su posición en ese listado. Por ello, los valores p e intervalos de la muestra de 150 deben interpretarse dentro de ese criterio de selección, sin atribuirle representatividad probabilística. La comparación con los 178 países muestra la sensibilidad de los resultados a la composición de la muestra, pero no resuelve el desfase temporal, los posibles factores compartidos ni la falta de identificación causal [19], [24], [32].

X. CONCLUSIONES

En los 150 países seleccionados, DAI gubernamental 2016, Government Effectiveness 2023 y GCI 2024 presentaron asociaciones positivas. La especificación DAI→GE→GCI produjo un componente indirecto positivo y estadísticamente distinguible de cero mediante el intervalo bootstrap. El resultado describe una asociación entre indicadores nacionales; no demuestra que la adopción digital haya generado maduración institucional ni que esta haya producido mayor capacidad de ciberseguridad [19], [24], [32] [33].

La aportación consiste en estimar asociaciones entre indicadores nacionales y evaluar su sensibilidad mediante las comprobaciones especificadas y la comparación con los 178 países completos. El marco de capacidades orienta la interpretación conceptual, pero no se valida directamente con estas mediciones. Estudios posteriores deberán utilizar datos

temporalmente comparables, controles justificados y diseños que permitan examinar cambios dentro de los países [3], [8], [11].

Las asociaciones observadas son compatibles con esa discusión, pero no demuestran que una capacidad organizacional produzca adopción digital o mejor desempeño institucional [19], [24], [32].

La contribución del artículo consiste en integrar indicadores internacionales manteniendo sus límites conceptuales: adopción digital no equivale a innovación, y efectividad institucional no equivale a resiliencia organizacional [1], [12], [25]. Los resultados ofrecen contexto para el estudio posterior de cooperativas, donde será necesario medir directamente sus decisiones, prácticas y capacidades [35], [11], [14]. En el compendio doctoral, este análisis se sitúa entre el estudio bibliométrico previo sobre innovación y ciberseguridad en empresas digitalizadas latinoamericanas y una futura investigación organizacional en cooperativas [39]. Esta última permitirá examinar cómo se relacionan la gobernanza cibernética, la innovación digital y la resiliencia en organizaciones concretas.

REFERENCES

[1] G. Vial, «Understanding digital transformation: A review and a research agenda», *J. Strateg. Inf. Syst.*, vol. 28, n.º 2, pp. 118-144, jun. 2019, doi: 10.1016/j.jsis.2019.01.003.

[2] P. C. Verhoef *et al.*, «Digital transformation: A multidisciplinary reflection and research agenda», *J. Bus. Res.*, vol. 122, pp. 889-901, ene. 2021, doi: 10.1016/j.jbusres.2019.09.022.

[3] Z. A. Soomro, M. H. Shah, y J. Ahmed, «Information security management needs more holistic approach: A literature review», *Int. J. Inf. Manag.*, vol. 36, n.º 2, pp. 215-225, abr. 2016, doi: 10.1016/j.ijinfomgt.2015.11.009.

[4] R. Diesch, M. Pfaff, y H. Krcmar, «A comprehensive model of information security factors for decision-makers», *Comput. Secur.*, vol. 92, p. 101747, may 2020, doi: 10.1016/j.cose.2020.101747.

[5] K. S. R. Warner y M. Wäger, «Building dynamic capabilities for digital transformation: An ongoing process of strategic renewal», *Long Range Plann.*, vol. 52, n.º 3, pp. 326-349, jun. 2019, doi: 10.1016/j.lrp.2018.12.001.

[6] A. Yeow, C. Soh, y R. Hansen, «Aligning with new digital strategy: A dynamic capabilities approach», *J. Strateg. Inf. Syst.*, vol. 27, n.º 1, pp. 43-58, mar. 2018, doi: 10.1016/j.jsis.2017.09.001.

[7] D. J. Teece, «Business models and dynamic capabilities», *Long Range Plann.*, vol. 51, n.º 1, pp. 40-49, feb. 2018, doi: 10.1016/j.lrp.2017.06.007.

[8] S. Durst, C. Hinteregger, y M. Zieba, «The effect of environmental turbulence on cyber security risk management and organizational resilience», *Comput. Secur.*, vol. 137, p. 103591, feb. 2024, doi: 10.1016/j.cose.2023.103591.

[9] B. Gaudenzi y B. Baldi, «Cyber resilience in organisations and supply chains: from perceptions to actions», *Int. J. Logist. Manag.*, vol. 35, n.º 7, pp. 99-122, dic. 2024, doi: 10.1108/IJLM-09-2023-0372.

[10] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, y D. A. Alabbad, «Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations», *Sensors*, vol. 23, n.º 15, p. 6666, jul. 2023, doi: 10.3390/s23156666.

[11] K. Singh, S. Chatterjee, M. Mariani, y S. F. Wamba, «Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment», *Technovation*, vol. 143, p. 103219, may 2025, doi: 10.1016/j.technovation.2025.103219.

[12] Stephanie Duchek, «Organizational resilience: a capability-based conceptualization», *Bus. Res.*, vol. 13, n.º 1, pp. 215-246, abr. 2020, doi: 10.1007/s40685-019-0085-7.

[13] A. Priyono y A. Hidayat, «Dynamic Capabilities for Open Innovation: A Typology of Pathways toward Aligning Resources, Strategies and Capabilities», *J. Open Innov. Technol. Mark. Complex.*, vol. 8, n.º 4, p. 206, dic. 2022, doi: 10.3390/joitmc8040206.

[14] J. A. R. Awad y Rodrigo Martín-Rojas, «Digital transformation influence on organisational resilience through organisational learning and innovation», *J. Innov. Entrep.*, vol. 13, n.º 1, p. 69, oct. 2024, doi: 10.1186/s13731-024-00405-4.

[15] R. Dubey, D. J. Bryde, Y. K. Dwivedi, G. Graham, C. Foropon, y T. Papadopoulos, «Dynamic digital capabilities and supply chain resilience: The role of government effectiveness», *Int. J. Prod. Econ.*, vol. 258, p. 108790, abr. 2023, doi: 10.1016/j.ijpe.2023.108790.

[16] Y. A. Alrub y S. M. Sánchez-Cañizares, «Dynamic Capabilities and Digital Transformation: Toward Strategic Planning in the Digital Age—Evidence from Palestine», *Adm. Sci.*, vol. 15, n.º 1, p. 21, ene. 2025, doi: 10.3390/admsci15010021.

[17] S. Nambisan, K. Lyytinen, A. Majchrzak, y M. Song, «Digital Innovation Management: Reinventing Innovation Management Research in a Digital World», *MIS Q.*, vol. 41, n.º 1, pp. 223-238, mar. 2017, doi: 10.25300/MISQ/2017/41:1.03.

[18] Y. Yoo, O. Henfridsson, y K. Lyytinen, «The New Organizing Logic of Digital Innovation: An Agenda for Information Systems Research», *Inf. Syst. Res.*, vol. 21, n.º 4, pp. 724-735, 2010, doi: 10.1287/isre.1100.0322.

[19] Banco Mundial, «World Development Report 2016: Digital Dividends», *Inf. Sobre El Desarro. Mund. 2016 Divid. Digit. Cuad. "Panorama Gen.*, 2016, doi: , 10.1596/978-1-4648-0671-1.

[20] H. Paananen, M. Lapke, y M. Siponen, «State of the art in information security policy development», *Comput. Secur.*, vol. 88, p. 101608, ene. 2020, doi: 10.1016/j.cose.2019.101608.

[21] A. Wiley, A. McCormac, y D. Calic, «More than the individual: Examining the relationship between culture and Information Security Awareness», *Comput Secur*, vol. 88, n.º C, ene. 2020, doi: 10.1016/j.cose.2019.101640.

[22] B. Dupont, «The cyber-resilience of financial institutions: significance and applicability», *J. Cybersecurity*, vol. 5, n.º 1, p. tyz013, ene. 2019, doi: 10.1093/cybsec/tyz013.
[23] A. Annarelli y Giulia Palombi, «Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework», *Sustainability*, vol. 13, n.º 23, p. 13065, nov. 2021, doi: 10.3390/su132313065.
[24] Kaufmann, Daniel y A. Kraay, «Indicadores Mundiales de Gobernanza: Metodología y Actualización de 2024», nov. 2024. doi: dx.doi.org/10.2139/ssrn.5154675.
[25] Julia Hillmann y Edeltraud Guenther, «Organizational Resilience: A Valuable Construct for Management Research?», *Int. J. Manag. Rev.*, vol. 23, n.º 1, pp. 7-44, ene. 2021, doi: 10.1111/ijmr.12239.
[26] J. Zhang, H. Li, y H. Zhao, «The Impact of Digital Transformation on Organizational Resilience: The Role of Innovation Capability and Agile Response», *Systems*, vol. 13, n.º 2, p. 75, ene. 2025, doi: 10.3390/systems13020075.
[27] J. A. Putritamara, B. Hartono, H. Toiba, H. N. Utami, M. S. Rahman, y D. Masyithoh, «Do Dynamic Capabilities and Digital Transformation Improve Business Resilience during the COVID-19 Pandemic? Insights from Beekeeping MSMEs in Indonesia», *Sustainability*, vol. 15, n.º 3, p. 1760, ene. 2023, doi: 10.3390/su15031760.
[28] A. Kwiotkowska, «Creating Organizational Resilience through Digital Transformation and Dynamic Capabilities: Findings from fs/QCA Analysis on the Example of Polish CHP Plants», *Sustainability*, vol. 16, n.º 14, p. 6266, jul. 2024, doi: 10.3390/su16146266.
[29] J. Zhang, J. Long, y A. M. E. Von Schaewen, «How Does Digital Transformation Improve Organizational Resilience?—Findings from PLS-SEM and fsQCA», *Sustainability*, vol. 13, n.º 20, p. 11487, oct. 2021, doi: 10.3390/su132011487.
[30] Y. Gao, X. Yang, y S. Li, «Government Supports, Digital Capability, and Organizational Resilience Capacity during COVID-19: The Moderation Role of Organizational Unlearning», *Sustainability*, vol. 14, n.º 15, p. 9520, ago. 2022, doi: 10.3390/su14159520.
[31] J.-J. Igartua y A. F. Hayes, «Mediation, Moderation, and Conditional Process Analysis: Concepts, Computations, and Some Common Confusions», *Span. J. Psychol.*, vol. 24, p. e49, 2021, doi: 10.1017/SJP.2021.46.
[32] U. I. de T. ITU, «Global Cybersecurity Index 2024», *5th*, 2024, [En línea]. Disponible en: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024
[33] A. F. Hayes, *Introduction to mediation, moderation, and conditional process analysis: a regression-based approach*. en Methodology in the social sciences. New York: The Guilford Press, 2022.
[34] R. M. Barón y David A Kenny, «The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations», vol. 51, n.º 6, pp. 1173-1182, 1986, doi: 10.1037/0022-3514.51.6.1173.
[35] S. A. Al-Somali, R. R. Saqr, A. M. Asiri, y N. A. Al-Somali, «Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture», *Sustainability*, vol. 16, n.º 5, p. 1880, feb. 2024, doi: 10.3390/su16051880.
[36] A. Garcia-Perez, J. G. Cegarra-Navarro, M. P. Sallos, E. Martinez-Caro, y A. Chinnaswamy, «Resilience in healthcare systems: Cyber security and digital transformation», *Technovation*, vol. 121, p. 102583, mar. 2023, doi: 10.1016/j.technovation.2022.102583.
[37] M. S. D. Araujo, B. A. S. Machado, y F. U. Passos, «Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance», *Appl. Sci.*, vol. 14, n.º 5, p. 2116, mar. 2024, doi: 10.3390/app14052116.
[38] H. Hokmabadi, S. M. H. S. Rezvani, y C. A. De Matos, «Business Resilience for Small and Medium Enterprises and Startups by Digital Transformation and the Role of Marketing Capabilities—A Systematic Review», *Systems*, vol. 12, n.º 6, p. 220, jun. 2024, doi: 10.3390/systems12060220.
[39] A. P. Hernandez Bonilla y Á. E. Acevedo Duque, «Análisis bibliométrico sobre innovación y ciberseguridad: un enfoque estratégico para empresas digitalizadas en Latinoamérica», *Innovare Rev. Cienc. Tecnol.*, pp. 1-9, dic. 2025, doi: 10.69845/innovare.v14i2.563.
[40] R. Mu, Y. Xu, y J. Zhang, «Digital Transformation, Enterprise Niche Resilience, and Substantive Innovation in Manufacturing Single Champion Enterprises», *Systems*, vol. 13, n.º 4, p. 235, mar. 2025, doi: 10.3390/systems13040235.
[41] K. Saemaldaher y O. L. Emeagwali, «The Role of Open Innovation in Enhancing Organizational Resilience and Sustainability Performance Through Organizational Adaptability», *Sustainability*, vol. 17, n.º 13, p. 5846, jun. 2025, doi: 10.3390/su17135846.