ISBN: 978-631-6557-84-1

Recibido:3 de febrero de 2026 / Aceptado: 31 de marzo de 2026 / Publicado: 18 de abril de 2026

Área: Ingeniería

CAPÍTULO 7

RESILIENCIA OPERATIVA Y CIBERSEGURIDAD EN LA GESTIÓN DE TI: ESTRATEGIAS PARA LA TRANSFORMACIÓN DIGITAL SOSTENIBLE EN ORGANIZACIONES MODERNAS

Operational Resilience and Cybersecurity in IT Management: Strategies for Sustainable Digital Transformation in Modern Organizations

Blanco Reyna, Jorge Luis, Fernando Emilio Escudero Vilchez, Pedro Antonio Arévalo Martínez, Reyno Mesías Padilla Santos, Carlos Alberto Murillo Salazar
DOI: 10.55204/pmea.134.c216

Blanco Reyna, Jorge Luis[1] *0000-0002-7477-5824*
Jorge.blanco@upn.edu.pe

Fernando Emilio Escudero Vilchez[2] *0000-0002-3835-8740*
fernando.escudero@autonomadeica.edu.pe

Pedro Antonio Arévalo Martínez[3] *0009-0004-1963-7404*
pedroarevalom@outlook.com

Reyno Mesías Padilla Santos[4] *0000-0001-5278-2049*
rmpadillas@hotmail.com

Carlos Alberto Murillo Salazar[5] *0009-0009-7673-4813*
carlos.murillo@uppu.edu.pe

[1]Universidad Privada del Norte, Lima, Perú.
[2]Universidad Autónoma de Ica, Ica, Perú.
[3]Universidad Inca Garcilaso de la Vega, Lima, Perú.
[4]Universidad Tecnológica del Perú, Lima, Perú.
[5]Universidad Privada de Puno, Puno, Perú.

Resumen: Introducción: La resiliencia operativa y la ciberseguridad en la gestión de TI se han convertido en imperativos estratégicos que comprometen la continuidad y sostenibilidad de las organizaciones modernas ante amenazas cibernéticas crecientes. Objetivo: Analizar las estrategias de integración entre resiliencia operativa y ciberseguridad en la gestión de TI como pilares para la transformación digital sostenible mediante una revisión sistemática. Métodos: Se realizó una revisión sistemática siguiendo la declaración PRISMA. La búsqueda se efectuó en Scopus (2022-2026), seleccionando 25 artículos. La calidad metodológica se evaluó con las herramientas del Instituto Joanna Briggs (JBI). Resultados: Los determinantes de la vulnerabilidad operativa son arquitectónicos y organizacionales: ausencia de Zero Trust, falta de automatización SOAR, carencia de inteligencia de amenazas (CTI) y gobernanza desactualizada. El impacto es directo: incrementos en tiempos de recuperación, pérdidas financieras y erosión de confianza. La IA

ISBN: 978-631-6557-84-1

agéntica y SOAR proyectan mejoras del 40 % en eficiencia de SOC para 2026; la cultura de ciberseguridad es el segundo factor crítico de éxito. Conclusiones: Los determinantes de la vulnerabilidad operativa son arquitectónicos y organizacionales: ausencia de Zero Trust, falta de automatización SOAR, carencia de inteligencia de amenazas (CTI) y gobernanza desactualizada. El impacto es directo: incrementos en tiempos de recuperación, pérdidas financieras y erosión de confianza. La IA agéntica y SOAR proyectan mejoras del 40 % en eficiencia de SOC para 2026; la cultura de ciberseguridad es el segundo factor crítico de éxito.

Palabras clave: *Resiliencia Operativa; Ciberseguridad; Gestión de TI; Transformación Digital; Sostenibilidad; Gobernanza de TI.*

Abstract: Objective: To analyze integration strategies between operational resilience and cybersecurity in IT management as pillars for sustainable digital transformation through a systematic review. Conclusions: Cybersecurity integrated with operational resilience is a non-negotiable pillar for digital sustainability. Continuity depends on IT governance maturity; organizations must prioritize proactive architectures, automation, and continuous training as survival and competitiveness strategies.

Keywords: *Operational Resilience; Cybersecurity; IT Management; Digital Transformation; Sustainability; IT Governance.*

1. INTRODUCCIÓN:

Actualmente, las organizaciones están inmersas en un traspaso digital que va mucho más allá de implementar nuevas herramientas tecnológicas ya que, la migración hacia entornos virtuales y la dependencia de infraestructuras interconectadas han posicionado a la gestión de TI como un factor estratégico para mantener el negocio en marcha (1). La resiliencia operativa, capacidad que tienen las empresas para anticiparse, resistir y adaptarse ante fallos o inconvenientes tecnológicos, pasa de ser solo concepto teórico a una condición fundamental para la supervivencia en un mercado cada vez más digitalizado (2).

A su vez, las amenazas se han expandido considerablemente por el uso excesivo de la nube, IoT (Internet of Things) y el trabajo remoto, aumentando los puntos de entrada para posibles ataques, lo que exige rediseñar modelos de gobierno y gestión de riesgos en las organizaciones (3). Por ello, resulta imprescindible hallar estrategias que integren la ciberseguridad con la resiliencia operativa, garantizando la continuidad de los servicios y preservar la confianza de los clientes (4,5).

A nivel internacional, el volumen de las amenazas cibernéticas ha alcanzado niveles críticos, especialmente en sectores como la salud, las finanzas y la infraestructura débil donde la disponibilidad de los sistemas no es negociable para la operación (6). Por otro lado, la complejidad de los ataques de ransomware, las vulnerabilidades de cadena de suministro y técnicas de ingeniería social avanzada crean una desprotección profunda en el enfoque tecnológico organizacional (7). Según reportes de la Agencia de Ciberseguridad de la Unión Europea (ENISA), hasta el 68 % de las organizaciones han experimentado al menos un incidente cibernético significativo en los últimos tres años, con un costo promedio de recuperación que supera los 4,5 millones de dólares por evento (8). Aquello empeora en entornos con presupuestos de TI limitados, donde la ambigüedad de infraestructuras y la falta de talento especializado en ciberseguridad actúan como catalizadores persistentes de la vulnerabilidad operativa, afectando la estabilidad digital (9).

Por lo mismo, lo más grave para la defensa cibernética es la suspensión de la operativi-

ISBN: 978-631-6557-84-1

dad ya que, según el Foro Económico Mundial (8), el 40 % de las organizaciones que sufren un fallo tecnológico con duración de 72 horas a más, sin lograr recuperarse por completo en el año siguiente. A nivel mundial, se registran alrededor de 2.200 ciberataques diarios que afectan la disponibilidad de servicios esenciales, generando pérdidas económicas y sociales que, según cálculos, superaron los 8 billones de dólares anuales para 2025 (10). Así, estos ataques están relacionadas con marcos de gobernanza de TI insuficientes y con la falta de planes de continuidad que estén integrados con estrategias de ciberseguridad, evidenciando que una organización sin resiliencia tecnológica se convierte en un factor débil dentro de la cadena de valor digital (11,12).

Desde un enfoque teórico, la resiliencia operativa se entiende como un concepto que abarca tres dimensiones clave: la capacidad de absorber el impacto, la capacidad de adaptarse y la capacidad de recuperarse frente a perturbaciones sistémicas (13). La primera se refiere a mantener las funciones críticas mientras el incidente está ocurriendo. La segunda implica reorganizar procesos y recursos tecnológicos para responder a escenarios adversos (14). Y la tercera tiene que ver con la rapidez y la calidad con que se vuelve a la normalidad, lo que afecta directamente tanto la cadena de suministro digital como la experiencia del usuario final (15). Estas tres capacidades son fundamentales para entender cómo la vulnerabilidad tecnológica influye en la toma de decisiones gerenciales y en la capacidad de respuesta ante ciberataques de gran escala (16).

Desde la gestión de TI, la ciberseguridad es un conjunto de prácticas orientadas a la protección de los sistemas, redes y datos de la organización frente a accesos no autorizados, hackeos o interrupciones, garantizando que la información mantenga su confidencialidad, integridad y disponibilidad ya que se considerada como activo estratégico (17). A su vez, es importante distinguir entre dos tipos de riesgos: primero, las amenazas externas, se origina de actores maliciosos en el ciberespacio; seguido de ello, los riesgos internos, que son fallos en la arquitectura tecnológica o en las funciones de los colaboradores de la entidad (18).

De esta forma , cuando se analiza la relación entre ciberseguridad y resiliencia operativa, se evidencia que la primera actúa como una barrera preventiva, mientras que la segunda funciona como la capacidad reactiva que permite sostener los servicios en funcionamiento cuando las defensas son vulneradas (19,20). Por lo tanto, la ciberseguridad no puede abordarse de manera aislada ya que debe integrarse con la continuidad y sostenibilidad de los procesos de transformación digital que las organizaciones llevan a cabo (21,22). Adicionalmente, los factores que determinan una transformación digital sostenible son diversos y abarcan aspectos tecnológicos, organizacionales y humanos dentro del área de TI (23).

Desde una vista tecnológica, destacan elementos como la adopción de arquitecturas de seguridad ZERO TRUST, la automatización de respuestas ante incidentes (SOAR) y la migración hacia infraestructuras nativas de la nube con redundancia incorporada (24). Desde el enfoque organizacional, se identifican variables relevantes como una cultura sólida de ciberseguridad, capacitación continua del personal y una alineación estratégica clara entre la dirección de TI y la gerencia, acelerando la construcción de una resiliencia operativa efectiva (25). Cuando estos elementos se combinan en entornos de alta presión competitiva, los resultados se traducen en una reducción del tiempo medio de recuperación (MTTR) y en una disminución significativa de las pérdidas financieras ocasionadas por interrupciones del servicio (26).

ISBN: 978-631-6557-84-1

A pesar de que existen muchas investigaciones que abordan la ciberseguridad y la gestión de TI por separado, aún se debe profundizar en un aspecto clave: cómo la integración estratégica entre la resiliencia operativa y los marcos de ciberseguridad se refleja en indicadores concretos de sostenibilidad digital (27). Esta carencia en la literatura disponible muestra la necesidad de un análisis que organice y articule la evidencia existente, ofreciendo a los directores de tecnología y administradores de sistemas una visión clara y útil. Solo a través de una revisión crítica y sistemática de la producción científica se podrá construir modelos de gobernanza de TI que protejan tanto la infraestructura tecnológica como la continuidad del negocio en el entorno digital actual.

La justificación de este trabajo es para fundamentar nuevas políticas de gestión de tecnologías de la información basadas en la evidencia científica actual y en marcos de referencia internacionales como ISO 27001, NIST CSF y DORA (28). Al identificar los factores determinantes con mayor peso sobre la resiliencia operativa y la ciberseguridad, las organizaciones podrán diseñar estrategias de transformación digital que no sean solo reactivas sino dinámicas y factibles. Igualmente, este análisis aporta un valor académico al consolidar la relación entre la seguridad cibernética y la continuidad del negocio como dimensiones de la sostenibilidad digital. Por último, la consolidación de la resiliencia operativa del capital tecnológico se posiciona como estrategia preventiva para reducir la incidencia de interrupciones y asegurar la competitividad en el entorno moderno (29).

El objetivo general fue analizar las estrategias de integración entre la resiliencia operativa y la ciberseguridad en la gestión de TI como pilares fundamentales para una transformación digital sostenible en organizaciones modernas. Como objetivos específicos se planteó: a) Identificar los principales factores tecnológicos, organizacionales y humanos que contribuyen al fortalecimiento de la resiliencia operativa ante amenazas cibernéticas emergentes. b) Categorizar los marcos de gobernanza de TI y las arquitecturas de seguridad que se reportan con mayor efectividad para garantizar la continuidad del negocio en entornos digitales complejos. c) Evaluar la efectividad de las estrategias de transformación digital sostenible orientadas a mitigar el impacto de incidentes cibernéticos y reducir el tiempo de recuperación operativa.

2. METODOLOGÍA:

La pesquisa aplicó la metodología PRISMA, la cual proporciona un marco estructurado que facilita la selección concreta y rigurosa de artículos científicos, asegurando transparencia en el proceso (30). De igual manera, resalta la necesidad de claridad en la presentación de los trabajos, permitiendo a los lectores valorar la solidez metodológica y la validez de los hallazgos obtenidos.

El proceso de localización de literatura se realizó exclusivamente en la base de datos de alto impacto Scopus. Esta plataforma fue seleccionada por su exhaustiva cobertura de literatura científica revisada por pares y su relevancia indiscutible en los campos de la ingeniería de sistemas, la ciberseguridad, la gestión de tecnologías de la información y la transformación digital a nivel global. Para garantizar la recuperación de estudios pertinentes, se aplicó una cadena de búsqueda avanzada bajo el esquema: TITLE-ABS-KEY ((.ºperational resilience.ºR çyber resilience.ºR "business continuity") AND (çybersecurity.ºR ïnformation security.ºR çyber threat management") AND (ÏT management.ºR ÏT governance.ºR "digital transformation") AND

ISBN: 978-631-6557-84-1

("sustainable.ºR "sustainability.ºR .ºrganizational sustainability")).

Aquello permitió adoptar descriptores técnicos en inglés para maximizar el alcance y precisión de la búsqueda, identificando investigaciones de alto nivel en la intersección entre la resiliencia operativa, seguridad cibernética y sostenibilidad digital. El periodo de análisis se acotó a las publicaciones realizadas entre el 2022 y 2026, con el propósito de capturar la evidencia científica actualizada sobre un problema que ha experimentado cambios críticos en el entorno tecnológico contemporáneo.

En ese sentido, la búsqueda inicial identificó un total de 1847 artículos, los cuales fueron posteriormente filtrados con base en los criterios de inclusión y exclusión (Tabla 1). Así mismo, dichos criterios resultan fundamentales para garantizar la selección de estudios empíricos que se ajusten al enfoque y propósito de la revisión sistemática, asegurando que los artículos finales analizados posean la calidad metodológica necesaria para sustentar las conclusiones de esta investigación.

Tabla 1.

Criterio de inclusión y exclusión

Criterios de inclusión	Criterios de exclusión
Investigaciones pertenecientes al periodo entre 2022 y 2026.	Investigaciones para optar a grado académico (tesis) o de repositorios institucionales.
Investigaciones en idiomas inglés o español.	Investigaciones en idiomas inglés o español.
Investigaciones de acceso abierto con texto completo disponible para su análisis.	Investigaciones de acceso abierto con texto completo disponible para su análisis.
Investigaciones centradas en la integración de resiliencia operativa, ciberseguridad y gestión de TI en contextos de transformación digital organizacional.	Investigaciones centradas en la integración de resiliencia operativa, ciberseguridad y gestión de TI en contextos de transformación digital organizacional.
Investigaciones indexadas en las bases de datos de Scopus.	Investigaciones indexadas en las bases de datos de Scopus.

Figura 1 Flujograma Prisma de selección de investigaciones para revisión}

Estudios finales
(n = 25)
Artículos identificados desde
Databases:
Scopus (2022-2026): 1847
Identification
Artículos removidos
(n = 1534)
Screening
Record screened
(n = 313)
Reportes excluidos
No tenían población ni mostraron correlación o no eran de acceso abierto
(n = 288)
Included

El proceso de revisión finalizó con 25 artículos, los cuales fueron considerados elegibles para un análisis riguroso al cumplir con la totalidad de los criterios de selección. Así, con el fin de presentar de manera accesible la evidencia recopilada, se procedió a sistematizar los

ISBN: 978-631-6557-84-1

hallazgos y valoraciones más significativas de estos estudios (Tabla 2). En consecuencia, esta herramienta no solo resume, sino que organiza la información de manera sistemática, detallando el objetivo, principales conclusiones, diseño metodológico y país de origen de cada una de las investigaciones incluidas, facilitando su comprensión y el posterior análisis comparado de las estrategias de resiliencia operativa y ciberseguridad aplicadas a la transformación digital sostenible.

Para cumplir el rigor científico y la validez interna de los hallazgos, se procedió a la evaluación de la calidad metodológica de los 25 artículos seleccionados mediante la herramienta de lectura del Instituto Joanna Briggs (JBI) para estudios analíticos y transversales. Este proceso fue realizado de forma independiente, calificando cada estudio en función de criterios objetivos como la representatividad de la muestra, validez de los instrumentos de medición de la resiliencia operativa y la ciberseguridad, y el control de variables en el análisis estadístico. Como resultado, el 92 % de las investigaciones (n=23) fueron categorizadas como de .ªlta calidad", al cumplir con más del 80 % de los ítems de la escala, mientras que el 8 % restante (n=2) se clasificó como de çalidad moderada". Cabe recalcar que ningún estudio fue excluido por baja calidad, asegurando así que la síntesis de evidencia presentada posee una metodología confiable para fundamentar las aplicaciones prácticas derivadas de este trabajo.

3. RESULTADOS Y DISCUSIÓN:

El análisis sistemático muestra una convergencia crítica entre la resiliencia operativa de las infraestructuras tecnológicas y los marcos de ciberseguridad como determinantes de una transformación digital sostenible. Los resultados se estructuran a continuación integrando la evidencia cualitativa y cuantitativa de los 25 estudios analizados.

Tabla 2

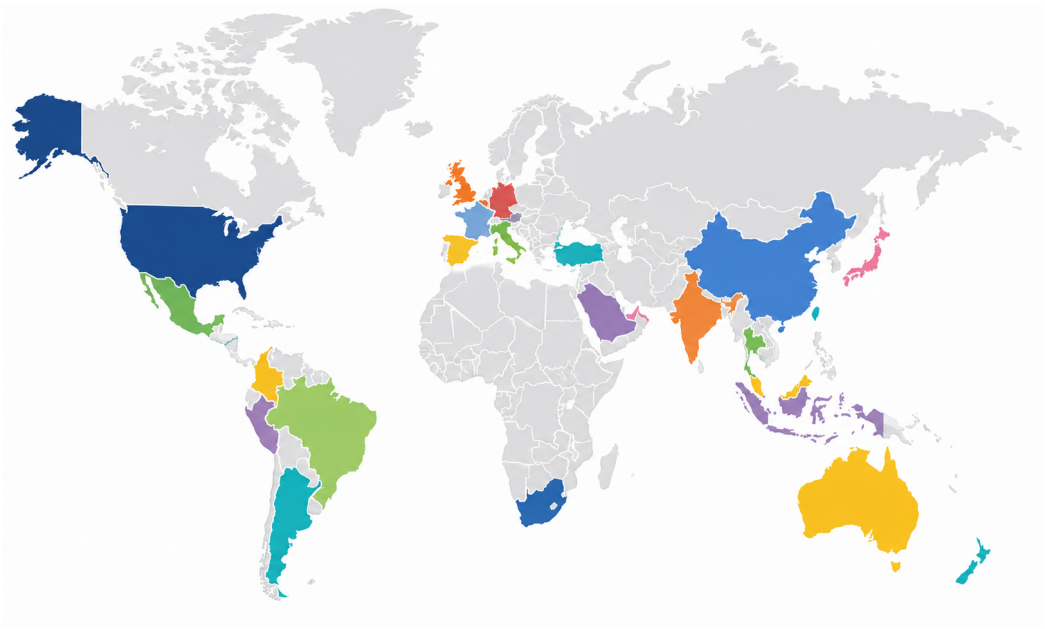
Investigaciones analizadas

N°	Autores	Objetivos	Hallazgo
1.	(31)	Evaluar el impacto de la arquitectura Zero Trust en los ecosistemas de innovación y resiliencia.	Evaluar el impacto de la arquitectura Zero Trust en los ecosistemas de innovación y resiliencia.
2.	(32)	Probar la eficacia de las herramientas SOAR en entornos de respuesta a incidentes reales.	Probar la eficacia de las herramientas SOAR en entornos de respuesta a incidentes reales.
3.	(33)	Analizar la digitalización y la ciberseguridad hacia un marco de resiliencia operativa.	Analizar la digitalización y la ciberseguridad hacia un marco de resiliencia operativa.
4.	(34)	Avances en tecnología de pruebas de estrés para sistemas de información Cloud-Native.	Avances en tecnología de pruebas de estrés para sistemas de información Cloud-Native.
5.	(35)	Evaluar marcos de ciberseguridad (desde COBIT hasta ISO 42001 y NIST).	La alineación de NIST CSF con la gobernanza de TI general es fundamental para madurar los controles de seguridad y mitigar riesgos sistémicos.
6.	(36)	Examinar el impacto de los ataques de ransomware en la resiliencia operativa de los sistemas de salud y su efecto en la continuidad asistencial.	Los ataques de ransomware a hospitales se han quintuplicado, demostrando que la resiliencia clínica depende directamente de la continuidad de los sistemas de TI.
7.	(37)	Determinar la relación entre los sistemas organizacionales de ciberseguridad y la sostenibilidad del desarrollo digital empresarial.	Desarrollar una cultura de ciberseguridad es obligatorio, ya que la tecnología por sí sola no puede abordar los riesgos que amenazan la sostenibilidad digital.
8.	(38)	Investigar los factores que determinan la ciber-resiliencia en las cadenas de suministro globales y su impacto en la continuidad operativa.	La gestión de riesgos de la cadena de suministro digital requiere integrar la ciberseguridad en los modelos tradicionales de resiliencia logística.
9.	(39)	Transformar la ciberseguridad con IA agentica para combatir amenazas.	Se proyecta que la IA agéntica aumente la eficiencia de los centros de operaciones de seguridad (SOC) en un 40 % para 2026, mejorando la detección proactiva.

N°	Autores	Objetivos	Hallazgo
10.	(40)	Diseñar un marco especializado de evaluación de riesgos de ciberseguridad adaptado a las limitaciones presupuestarias de las PYMES.	Las PYMES requieren marcos adaptados de ISO 27001 y NIST, ya que los presupuestos limitados son la principal barrera para la adopción de controles.
11.	(41)	Analizar los desafíos regulatorios y operativos que plantea la implementación del Digital Operational Resilience Act (DORA) en las entidades financieras europeas.	DORA introduce un marco regulatorio exhaustivo que obliga a las entidades financieras a cumplir requisitos estrictos de resiliencia digital frente a las TIC.
12.	(42)	Evaluar la efectividad de las plataformas SOAR combinadas con programas de concienciación en la reducción del riesgo de ataques de ingeniería social.	La tecnología por sí sola no basta; los procesos de respuesta a incidentes y la concienciación humana siguen siendo esenciales para una organización resiliente.
13.	(43)	Investigar las estrategias de ciberseguridad basadas en SBOM y Zero Trust para garantizar la resiliencia operativa en entornos de manufactura inteligente con IoT.	Los SBOMs (Software Bill of Materials) contribuyen a la arquitectura Zero Trust mediante la verificación en tiempo real de componentes en entornos IoT industriales.
14.	(44)	Examinar el rol del ciberseguro como mecanismo incentivador del endurecimiento de controles de seguridad y la mejora de la resiliencia operativa.	El ciberseguro actúa como un catalizador que obliga a las organizaciones a endurecer sus controles de seguridad para poder calificar a las pólizas.
15.	(45)	Proponer un enfoque de protección basado en resiliencia adaptativa para infraestructuras espaciales y de telecomunicaciones de alta criticidad.	Zero Trust asume que no hay confianza implícita, proporcionando medidas de resiliencia operativa vitales para infraestructuras de alta criticidad.
16.	(46)	Analizar los desafíos de seguridad y privacidad en entornos multi-cloud e híbridos y su impacto en la continuidad del negocio.	La transición a multi-cloud mejora la resiliencia operativa mediante redundancia, pero introduce nuevos vectores de ataque que requieren criptografía post-cuántica.
17.	(47)	Evaluar el impacto de los programas de formación en cultura de ciberseguridad sobre la resiliencia digital de instituciones de educación superior.	La transformación digital en universidades requiere directrices formales de cultura de ciberseguridad para proteger la investigación y los datos de los estudiantes.
18.	(48)	Investigar las implicaciones de la transformación digital en la ciberseguridad de las redes eléctricas inteligentes y la continuidad del suministro energético.	La digitalización de las redes eléctricas inteligentes (Smart Grids) expone al sector energético a riesgos cibernéticos que amenazan la continuidad del suministro.
19.	(49)	Proponer un enfoque de integración de Zero Trust en pipelines DevSecOps cloud-native para mejorar la resiliencia operativa y la sostenibilidad ambiental.	Integrar Zero Trust en los pipelines DevSecOps mejora tanto la resiliencia operativa como la sostenibilidad ambiental de los despliegues en la nube.
20.	(50)	Desarrollar un sistema global de inteligencia de amenazas cibernéticas (CTI) basado en inteligencia artificial para la detección de ataques sofisticados.	Las soluciones analíticas basadas en IA son obligatorias para proporcionar inteligencia de amenazas (CTI) a nivel nacional y corporativo frente a deepfakes.
21.	(51)	Diseñar un marco de seguridad que integre Zero Trust, inteligencia artificial y blockchain para garantizar la integridad de las operaciones de TI.	La integración de blockchain con Zero Trust permite una evaluación y aplicación continua de sesiones, garantizando la integridad de las operaciones de TI.
22.	(52)	Evaluar la contribución de la integración de plataformas de inteligencia de amenazas (CTI) en la resiliencia operativa de infraestructuras críticas.	Las plataformas CTI mejoran la flexibilidad operativa y priorizan la resiliencia frente a amenazas avanzadas en la cadena de suministro.
23.	(53)	Proponer un marco de ciberseguridad adaptado a las necesidades de resiliencia operativa de las PYMES en entornos de trabajo remoto e híbrido.	Las campañas de concienciación continua y el compromiso de los empleados son vitales para la resiliencia en modelos de trabajo híbrido y remoto.
24.	(54)	Sistematizar la evidencia científica sobre las estrategias de resiliencia operativa en el contexto de la ciberseguridad mediante una revisión sistemática.	La transformación digital exige una cultura de ciberseguridad que asegure la ciber-resiliencia, alineando las operaciones de TI con los criterios ESG (Green IT).
25.	(55)	Analizar los desafíos de ciberseguridad que plantea la transición hacia la criptografía post-cuántica en el sector financiero y su impacto en la resiliencia futura.	DORA y las normativas financieras exigen a las entidades prepararse para la amenaza cuántica, integrando la agilidad criptográfica en su resiliencia futura.

Figura 2 Distribución geográfica de la literatura

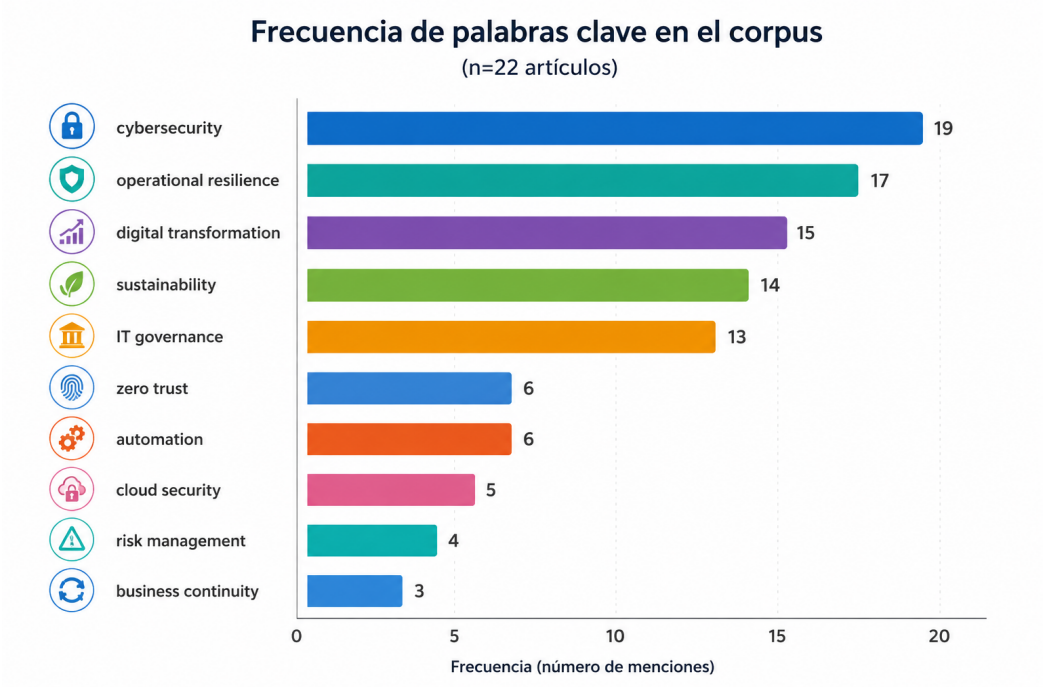
ISBN: 978-631-6557-84-1



Se evidencia la procedencia de los 25 artículos seleccionados, evidenciando una cobertura global de 16 países en cinco continentes. Estados Unidos lidera la producción científica con el 20 %, seguido por Reino Unido (12 %) y Alemania (12 %). El resto se distribuye entre países de Asia-Pacífico, América Latina, Europa del Sur y Medio Oriente. Esta diversidad es clave, pues confirma que la integración entre resiliencia operativa y ciberseguridad no es un fenómeno aislado de un mercado específico, sino una problemática transversal a distintos sectores industriales y contextos regulatorios. La inclusión de estudios de economías avanzadas y emergentes otorga validez externa a la revisión y refuerza la universalidad de la ciberseguridad como pilar de la sostenibilidad digital.

Figura 3

Frecuencias de palabras

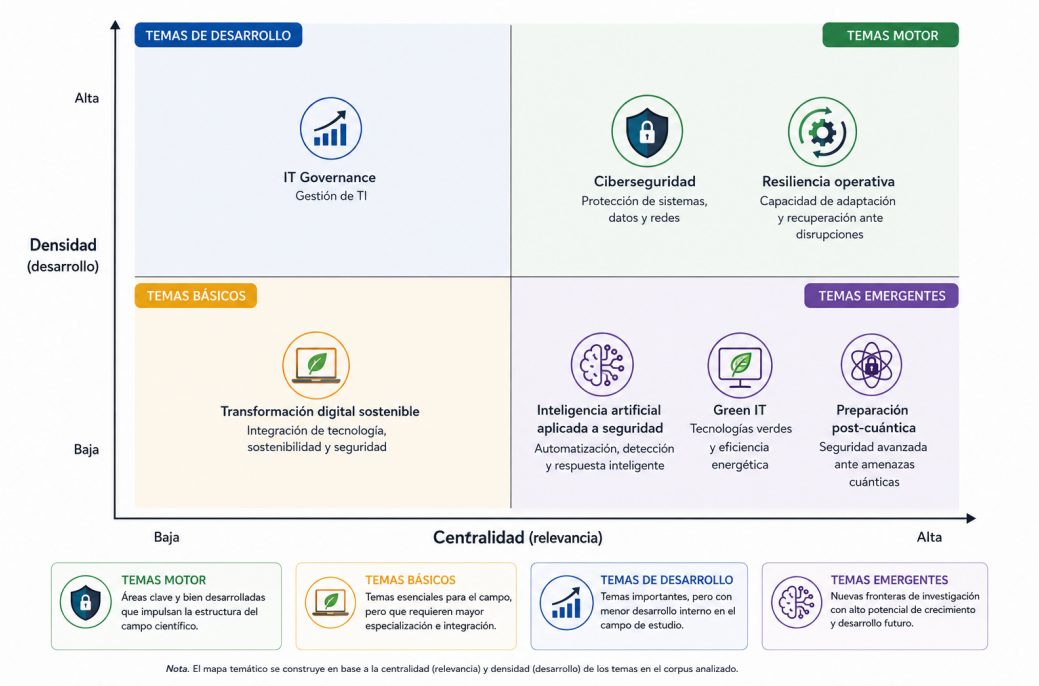


Se muestra el gráfico de frecuencias, el cual identifica a la çybersecurity"(19 menciones)

 ISBN: 978-631-6557-84-1

y la .ºperational resilience"(17 menciones) como los pilares temáticos predominantes en el corpus analizado. La alta recurrencia de términos como "digital transformation", "sustainabilityz ÏT governance"sugiere que la investigación se centra en la dimensión estratégica y gerencial de la protección tecnológica. Asimismo, la aparición de "zero trustz .ªutomationçon 12 menciones combinadas revela que las arquitecturas de seguridad proactivas y la automatización de respuestas constituyen las tendencias metodológicas más utilizadas para abordar la resiliencia operativa en el periodo 2022-2026.

Figura 4 Mapa temático



Nota. El mapa temático se construye en base a la centralidad (relevancia) y densidad (desarrollo) de los temas en el corpus analizado.

El mapa organiza los temas según su relevancia (centralidad) y desarrollo (densidad), destacando a la çiberseguridadz la resiliencia operativaçomo "temas motor", lo que significa que son áreas bien desarrolladas y fundamentales para la estructura del campo científico actual. La "transformación digital sostenible"se posiciona como un "tema básico", indicando que es esencial, pero requiere mayor especialización técnica en su integración con marcos de seguridad. Por otro lado, conceptos como la ïnteligencia artificial aplicada a seguridad", el "Green ITz la "preparación post-cuántica"se ubican en el cuadrante de "temas emergentes", lo que sugiere que, en este contexto específico, representan las fronteras de investigación con mayor potencial de crecimiento para los próximos años.

Resiliencia operativa y marcos de ciberseguridad: evidencias de integración

El estudio evidencia que la resiliencia operativa no es algo estático, sino una capacidad que se construye y se fortalece cuando los marcos de ciberseguridad se integran de manera sistemática con los procesos de gobernanza de TI. Por ejemplo, Singh et al. (31) reportan que la arquitectura Zero Trust no solo reduce la superficie de ataque, sino que también genera ventajas económicas medibles de innovación digital. En Europa, Buttigieg y Brunelli (41) detallan cómo la Ley de Resiliencia Operativa Digital (DORA) ha convertido la continuidad en una obligación legal para las entidades financieras, imponiendo requisitos estrictos de resiliencia cibernética.

Adicionalmente, los factores que determinan esta integración son de tipo arquitectónico y

ISBN: 978-631-6557-84-1

organizacional; así, se encuentra una relación consistente entre la automatización de respuestas mediante plataformas SOAR y la reducción significativa del tiempo de contención de incidentes. También, Bridges et al. (32) demuestran que el arreglo automatizado supera ampliamente a los procesos manuales, lo que da una respuesta más rápida y efectiva.

Otro factor importante es la cultura de ciberseguridad y la capacitación continua ya que, Metin et al. (33) proponen que la Çultura de Ciberseguridad y Rendición de Cuentas.[es] el segundo factor crítico de éxito más mencionado para garantizar la continuidad de las organizaciones. De manera similar, Al-Somali et al. (37) señalan que desarrollar una cultura de ciberseguridad es fundamental, porque la tecnología por sí sola no puede hacer frente a todos los riesgos que amenazan la sostenibilidad digital.

Tabla 3

Síntesis temática: relación entre aprendizaje conectado y pedagogía del impacto real

Tema de análisis	Determinantes y variables críticas	Impacto en la formación del estudiante	Referencia
Arquitecturas de seguridad proactiva	Zero Trust, segmentación de red, microperímetros, verificación continua.	Reducción de la superficie de ataque y mejora de la resiliencia operativa en ecosistemas digitales.	(31) (43) (46) (49)
Automatización e inteligencia artificial	Plataformas SOAR, detección ML, orquestación de respuestas, análisis predictivo.	Reducción del tiempo de contención de incidentes y aumento del 40 % en eficiencia de los SOC.	(32) (39) (50)
Gobernanza de TI y marcos regulatorios	NIST CSF, ISO 27001:2022, DORA, políticas de riesgo.	Madurez de controles de seguridad y cumplimiento regulatorio como base de la continuidad del negocio.	(35) (40) (41)
Factor humano y cultura de seguridad	Capacitación continua, ingeniería social, phishing, deepfakes.	La cultura de ciberseguridad como factor crítico de éxito; reducción del riesgo de ingeniería social.	(33) (37) (42) (47)
Continuidad del negocio y recuperación	Backups inmutables, multi-cloud, failover automatizado, planes de respuesta.	Garantía de disponibilidad del servicio y reducción del impacto de ataques en sectores críticos.	(34) (36) (46)
Sostenibilidad y resiliencia futura	Green IT, crypto-agile, blockchain, inteligencia de amenazas compartida.	Preparación ante amenazas emergentes y alineación con criterios ESG de sostenibilidad digital.	(51) (52) (54) (55)

El análisis de la tabla establece una relación clara dado que, la ciberseguridad actúa como escudo de la infraestructura digital, mientras que la resiliencia operativa es la capacidad de recuperación que mantiene los servicios críticos en funcionamiento incluso cuando las defensas han sido vulneradas. Cuando una organización carece de arquitecturas proactivas como Zero Trust, su base de ataque aumenta, ampliando una ventana de exposición que el atacante puede aprovechar para comprometer la continuidad del negocio (31,45). La automatización SOAR (32), disminuye el tiempo de contención, transformando un incidente potencialmente en una anomalía manejable; además, la IA agéntica proyectada por Kshetri (39) aumentará la eficiencia de los centros de operaciones de seguridad en un 40 % para 2026.

Uno de los resultados más fundamentales de la IA en la detección proactiva y en la inteligencia de amenazas, el sistema global de CTI basado en IA descrito por Sufi (50) permite anticiparse a amenazas antes de que afecten la operación, detallando el por qué la IA se ha convertido en un factor clave para reducir los tiempos de respuesta y garantizar la sostenibilidad operativa a largo plazo. Sin embargo, el factor humano sigue siendo débil, Waelchli y Walter (42) demuestran que la tecnología por sí sola no es suficiente; los procesos de respuesta deben combinarse con la concienciación del personal para prevenir ataques de ingeniería social que comprometan todo el enfoque digital.

También, el marco regulatorio y de gobernanza actúa como un mediador fundamental, puesto que, en organizaciones alineadas con estándares como NIST CSF, ISO 27001 y CO-

ISBN: 978-631-6557-84-1

BIT (35), la gestión de riesgos se integra de manera natural en la toma de decisiones de TI, rompiendo el ciclo de vulnerabilidad. El-Hajj et al. (40) muestran que las PYMES requieren marcos de evaluación de riesgos adaptados, ya que los presupuestos limitados son la principal barrera para adoptar controles adecuados. Sin embargo, donde no hay una gobernanza definida, los incidentes se manejan de forma reactiva y fragmentada, afectando el impacto operacional. Asimismo, las prácticas como la inteligencia de amenazas compartida (52) y las iniciativas de sostenibilidad digital (54) han demostrado ser efectivas no solo para mejorar la capacidad de respuesta, sino también para alinear la ciberseguridad con los criterios ESG de sostenibilidad, evidenciando que la resiliencia operativa es una inversión en la competitividad futura de la organización.

En conjunto, los resultados de esta revisión sistemática confirman de manera consistente que la integración estratégica entre ciberseguridad y resiliencia operativa es un factor determinante para la sostenibilidad de la transformación digital. Los 25 estudios analizados coinciden en que la continuidad del negocio no puede garantizarse únicamente con firewalls o antivirus; requiere una arquitectura de gobernanza que articule automatización, cultura organizacional y marcos regulatorios como pilares inseparables. La vulnerabilidad cibernética se ha convertido en la falla más crítica de la cadena de valor digital moderna, y su mitigación debe entenderse como una prioridad estratégica, no solo técnica, para asegurar la competitividad y sostenibilidad de las organizaciones.

4. CONCLUSIONES:

En síntesis, queda claro que la integración entre la resiliencia operativa y la ciberseguridad no es solo un asunto técnico, sino un factor decisivo para que la transformación digital sea sostenible en el tiempo. La evidencia revisada muestra que cuando las organizaciones carecen de arquitecturas de seguridad proactivas y de marcos de gobernanza de TI bien integrados, la continuidad del negocio se ve seriamente afectada; en conclusión, en tiempos de contención más largos, mayor exposición a amenazas avanzadas y una pérdida de confianza en los ecosistemas digitales.

Los factores que determinan la resiliencia operativa son principalmente sistémicos y arquitectónicos; así, la falta de estrategias Zero Trust, la ausencia de automatización en la respuesta a incidentes (SOAR) y la carencia de inteligencia de amenazas compartida (CTI) se perfilan como los principales desencadenantes de la vulnerabilidad operativa. La sostenibilidad de la transformación digital depende tanto del fortalecimiento de los marcos regulatorios (como DORA, NIST e ISO 27001) como de la consolidación de una auténtica cultura de ciberseguridad y rendición de cuentas en el factor humano, desplazando el foco del incidente técnico aislado hacia las fallas en las estructuras de gobernanza que permiten que la exposición a amenazas se vuelva crónica.

Para construir entornos digitales sostenibles y competitivos, las organizaciones deben dejar atrás el enfoque reactivo de la seguridad perimetral tradicional y apostar por modelos basados en la resiliencia adaptativa, la verificación continua y la automatización impulsada por inteligencia artificial. Herramientas como la integración de Zero Trust en pipelines DevSecOps, la adopción de arquitecturas multi-cloud con redundancia y la preparación para la transición post-cuántica no deberían verse como gastos, sino como estrategias de supervivencia y con-

ISBN: 978-631-6557-84-1

tinuidad del negocio. En definitiva, la ciberseguridad integrada con la resiliencia operativa se convierte en un pilar fundamental para cualquier política de transformación digital moderna.

3.1. Aplicaciones prácticas y futuras líneas de investigación:

Los hallazgos de esta revisión apuntan a tres aplicaciones prácticas concretas para repensar la gobernanza de TI. Primero, las organizaciones deberían implementar arquitecturas Zero Trust y metodologías como los SBOMs (Software Bill of Materials) como estándar de acceso y verificación, especialmente considerando que el IoT y la migración a la nube han ampliado significativamente la superficie de ataque (31,43). En segundo lugar, adoptar plataformas SOAR y sistemas de Inteligencia de Amenazas (CTI) basados en IA permite reducir el tiempo de contención de amenazas de horas a minutos, minimizando así el impacto operativo mediante la orquestación automatizada (32,50,52). Por último, los líderes de TI deben promover una cultura de ciberseguridad donde la capacitación del personal y la alineación con marcos como DORA e ISO 27001:2022 se entiendan como inversiones estratégicas en continuidad de la empresa, no como simples obligaciones de cumplimiento (33,41).

En cuanto a las futuras líneas de investigación, se necesitan estudios longitudinales que evalúen cómo las estrategias de migración post-cuántica afectan la resiliencia operativa a largo plazo, dado que la computación cuántica representa una amenaza para la criptografía actual, especialmente en el ámbito financiero y en infraestructuras críticas (55). También, profundizar en el retorno de la inversión (ROI) de las políticas de ciberseguridad integrada, calculando cuánto ahorra la organización al prevenir inconvenientes mediante automatización e IA agéntica. Además, sería interesante identificar cómo las prácticas de Green IT y la sostenibilidad ambiental se relacionan con la resiliencia operativa, evaluando si la eficiencia energética de los centros de operaciones de seguridad (SOC) contribuye a una transformación digital más integral (54). Estas investigaciones permitirán diseñar modelos de gobernanza de TI más precisos y adaptados a la realidad de los ecosistemas digitales actuales.

5. FINANCIACIÓN:

El autor no recibió financiación para el desarrollo de la presente investigación.

6. CONFLICTO DE INTERESES:

El autor declara que no existe conflicto de intereses

7. CONTRIBUCIÓN DE AUTORÍA:

En concordancia con la taxonomía establecida internacionalmente para la asignación de créditos a autores de artículos científicos (https://credit.niso.org/). Los autores declaran sus contribuciones en la siguiente matriz:

	Autor
Participar activamente en:	
Conceptualización	X
Análisis formal	X
Adquisición de fondos	X
Investigación	X
Metodología	X
Administración del proyecto	X
Recursos	X
Redacción –borrador original	X

	Autor
Redacción –revisión y edición	X
La discusión de los resultados	X
Revisión y aprobación de la versión final del trabajo.	X

8. REFERENCIAS:

x

Deep Manishkumar D, Kishan Hiteshkumar J. Cybersecurity Resilience: A Strategic Imperative for Sustainable Digital Transformation. International Journal of Scientific and Research Publications. 2025; 15(7): p. 398-406.
1. https://dx.doi.org/10.29322/IJSRP.15.07.2025.p16336.

2. Catal C, Kar G, Zarali M. Strategic technological innovation investment: enhancing resilience in the age of digital transformation. Journal of Innovative Digital Transformation. 2025; 2(1): p. 50-72. https://doi.org/10.1108/JIDT-05-2024-0010.
3. Nizamuddin M. Investigating the cybersecurity risks of remote work: a systematic literature review of organizational vulnerabilities and mitigation strategies. International Journal of Information Security. 2025; 24: p. https://doi.org/10.1007/s10207-025-01095-z.
4. Browder R, Dwyer S, Koch H. Upgrading adaptation: How digital transformation promotes organizational resilience. Strategic Entrepeneurship Journal. 2024; 18: p. 128-164. https://doi.org/10.1002/sej.1483.
5. Hilger R. From cybersecurity to cyber resilience: a systemic and scalable approach for improving resilience and adaptive capacity. Journal of Cybersecurity. 2026; 12(1): p. 1-10. https://doi.org/10.1093/cybsec/tyag011.
6. Aghazadeh A, Lezzi M, Pourmadadkar M. Risk Assessment for Cyber Resilience of Critical Infrastructures: Methods, Governance, and Standards. 2024; 14(24): p. https://doi.org/10.3390/app142411807.
7. Lubis M, Safitra M, Fukhrurroja H, Muttaqin A. Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience. Sensors. 2025; 25: p. 1-36. https://doi.org/10.3390/s25154545.
8. European Union Agency for Cybersecurity (ENISA). Threat landscape 2024: Annual report on cybersecurity incidents and trends. [Online]; 2024. Disponible en: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf.
9. Zhan X, Ba X, Li B. Cyberattacks in supply chains: A multi-case study. Plos One. 2026; 21(5): p. 1-22. https://doi.org/10.1371/journal.pone.0350010.
10. Awad J, Martín R. Digital transformation influence on organisational resilience through organisational learning and innovation. Journal of Innovation and Entrepreneurship. 2024; 13: p. https://doi.org/10.1186/s13731-024-00405-4.
11. World Economic Forum. Global risks report 2025: Cyber insecurity and systemic digital failures. [Online]; 2025. Disponible en: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf.
12. IBM Security. Cost of a data breach report 2024: Global analysis. [Online]; 2024. Disponible en: https://www.ibm.com/reports/data-breach?spm=a2ty_o01.29997173.0.0.470755fbwKf3yS.
13. Shepherd D, Williams T. Different response paths to organizational resilience. Small Bus Econ. 2023; 61(1): p. 23-58. https://doi.org/10.1007/s11187-022-00689-4.
14. Awwad A, Ababneh O, Karasneh M. The Mediating Impact of IT Capabilities on the Association between Dynamic Capabilities and Organizational Agility: The Case of the Jordanian IT Sector. Global Journal of Flexible Systems Management. 2022; 23: p. 315-330. https://doi.org/10.1007/s40171-022-00303-2.
15. Habibi F, Chakrabortty R, Abbasi A, Ho W. Investigating disruption propagation and resilience of supply chain networks: interplay of tiers and connections. International Journal of Production Research. 2025; 63(17): p. 6229–6251. https://doi.org/10.1080/00207543.2025.2470348.
16. Černý J, Potančok M, Novotný O, Bargoni A. Fostering organizational resilience in the age of hypercompetition: unpacking the role of competitive intelligence through the dynamic capabilities view. Review of Managerial Science. 2025;: p. 1-36. https://doi.org/10.1007/s11846-025-00966-y.
17. Bravo I, Hurtado R, Proaño E, López P. Transformación digital y resiliencia organizacional en entornos postpandémicos. Revista Científica Ciencia y Método. 2025; 3(2): p. 44-58. https://doi.org/10.55813/gaea/rcym/v3/n2/4.
18. Khadka K, Ullah A. Human factors in cybersecurity: an interdisciplinary review and framework proposal. International Journal of Information Security. 2025; 24: p. 1-13. https://doi.org/10.1007/s10207-025-01032-0.
19. Van der Kleij R, Schraagen J, Cadet B, Young H. Developing decision support for cybersecurity threat and incident managers. Computers & Security. 2022; 113: p. https://doi.org/10.1016/j.cose.2021.102535.
20. Dacorogna M, Debbadi N, Kratz M. Building up cyber resilience by better grasping cyber risk via a new algorithm for modelling heavy-tailed data. European Journal of Operational Research. 2023; 311(2): p. 708-729. https://doi.org/10.1016/j.ejor.2023.05.003.
21. Saeed S, Altamimi S, Alkayyalm N, Alshehri E, Alabbad D. Digital Transformation and Cybersecurity Challenges for Businesses Resilience: Issues and Recommendations. Sensors. 2023; 23(15): p. 1-20. https://doi.org/10.3390/s23156666.
22. Kotsias J, Ahmad A, Scheepers R. Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems. 2023; 32(1): p. https://econpapers.repec.org/article/taftjisxx/v_3a32_3ay_3a2023_3ai_3a1_3ap_3a35-51.htm.
23. Tzavara V, Vassiliadis S. Tracing the evolution of cyber resilience: a historical and conceptual review. International Journal of Information Security. 2024; 23: p. 1695–1719. https://doi.org/10.1007/s10207-023-00811-x.

Deep Manishkumar D, Kishan Hiteshkumar J. Cybersecurity Resilience: A Strategic Imperative for Sustainable Digital Transformation. International Journal of Scientific and Research Publications. 2025; 15(7): p. 398-406.
1. https://dx.doi.org/10.29322/IJSRP.15.07.2025.p16336.

24. Syed N, Shah S, Shaghaghi A, Anwar A, Baig Z, Doss R. Zero Trust Architecture (ZTA): A Comprehensive Survey. IEEE Access. 2022; 10: p. 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679.
25. Tejay G, Mohammed Z. Cultivating security culture for information security success: A mixed-methods study based on anthropological perspective. Elsevier. 2023; 60(3): p. https://doi.org/10.1016/j.im.2022.103751.
26. Staves A, Anderson T, Balderstone H, Green B, Gouglidis A, Hutchison D. A Cyber Incident Response and Recovery Framework to Support Operators of Industrial Control Systems. International Journal of Critical Infrastructure Protection. 2022; 37: p. https://doi.org/10.1016/j.ijcip.2021.100505.
27. Bardhan I, Kohli R, Oborn E, Mishra A, Hoo Tan C, Tremblay M, et al. Human-Centric Information Systems Research on the Digital Future of Healthcare. Information Systems Research. 2025; 36(1): p. 1-20. https://doi.org/10.1287/isre.2025.editorial.v36.n1.
28. ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection. [Online]; 2022. Disponible en: https://www.iso.org/standard/27001.
29. Bharucha S. Strategic Resilience Models for Enterprises in the Age of Continuous Disruption. E-Journal of Science and Emerging Technologies. 2026; 2(2): p. 26-33. https://doi.org/10.63345/ejset.v2.i2.201.
30. Stracke C, Chounta I, Holmes W, Tlili A, Bozkurt A. A standardised PRISMA-based protocol for systematic reviews of the scientific literature on Artificial Intelligence and education (AI&ED). Journal of Applied Learning and Teaching. 2023; 6(2): p. 64-70. https://doi.org/10.37074/jalt.2023.6.2.38.
31. Singh K, Chatterjee S, Mariani M, Wamba S. Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. Technovation. 2025; 143: p. 1-13. https://doi.org/10.1016/j.technovation.2025.103219.
32. Bridges R, Rice A, Oesch S, Nichols J, Watson C, Spakes K, et al. Testing SOAR tools in use. Computers & Security. 2023; 129: p. https://doi.org/10.1016/j.cose.2023.103201.
33. Metin B, Özhan F, Wynn M. Digitalisation and Cybersecurity: Towards an Operational Framework. Electronics. 2024; 13(21): p. 1-35. https://doi.org/10.3390/electronics13214226.
34. Guo Y, Yang M, Li X, Jian C, Liu J, Lao L. Advances in Full-Link Stress Testing Technology for Cloud-Native Information System. IEEE Xplore. 2024;: p. 1661-1665. https://doi.org/10.1109/ICIBA62489.2024.10868076.
35. McIntosh T, Susnjak T, Liu T, Watters P, Xu D, Liu D, et al. From COBIT to ISO 42001: Evaluating cybersecurity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. Computers & Security. 2024; 144: p. 1-16. https://doi.org/10.1016/j.cose.2024.103964.
36. Garcia A, Cegarra J, Sallos M, Martinez E, Chinnaswamy A. Resilience in healthcare systems: Cyber security and digital transformation. Technovation. 2023; 121: p. 1-11. https://doi.org/10.1016/j.technovation.2022.102583.
37. Al-Somali S, Saqr R, Asiri A, Al-Somali N. Organizational Cybersecurity Systems and Sustainable Development. Sustainability. 2024; 16(5): p. 1-25. https://doi.org/10.3390/su16051880.
38. Gaudenzi B, Baldi B. Cyber resilience in organisations and supply chains. International Journal of Production Economics. 2024; 32(7): p. 99-122. https://doi.org/10.1108/IJLM-09-2023-0372.
39. Kshetri N. Transforming cybersecurity with agentic AI to combat advanced threats. Telecommunications Policy. 2025; 49: p. 1-12. https://doi.org/10.1016/j.telpol.2025.102976.
40. El-Hajj M, Mirza Z. A Specialized Cybersecurity Risk Assessment Framework for SMEs. Electronics. 2024; 13(19): p. https://doi.org/10.3390/electronics13193910.
41. Buttigieg C, Brunelli B. The digital operational resilience act: challenges and some reflections. ERA Forum. 2024; 25: p. 11-28. https://doi.org/10.1007/s12027-024-00793-w.
42. Waelchli S, Walter Y. Reducing the risk of social engineering attacks using SOAR and awareness. Computers & Security. 2025; 148: p. 1-10. https://doi.org/10.1016/j.cose.2024.104137.
43. Castillo K, Dai H, Martinez G, Mehrzadi H. Cybersecurity for smart and resilient manufacturing. Computers & Industrial. 2026; 220: p. 1-33. https://doi.org/10.1016/j.cie.2026.112244.
44. Mott G, Turner S, Nurse J, MacColl J, Sullivan J, Cartwright A, et al. Between a rock and a hard(ening) place: Cyber insurance and security investments. Computers & Security. 2023; 128: p. 1-21. https://doi.org/10.1016/j.cose.2023.103162.
45. Shahzad S, Deane F, Joiner K, Qiao L, Suprun E. Cyber resilience in critical space infrastructure: A protection approach. Space Policy. 2026;: p. 1-18. https://doi.org/10.1016/j.spacepol.2026.101767.
46. Ali S, Talpur D, Abro A, Alshdukhi K, Alwakid G, Humayun M, et al. Security and privacy in multi-cloud and hybrid environments. Computers & Security. 2025; 157: p. https://doi.org/10.1016/j.cose.2025.104599.
47. Armas R, Taherdoost H. Building a Cybersecurity Culture in Higher Education. Information. 2025; 16(5): p. https://doi.org/10.3390/info16050336.
48. Saeed S, Gull H, Aldossary M, Altamimi A, Alshahrani M, Saqib M, et al. Digital Transformation in Energy Sector: Cybersecurity Implications. Information. 2024; 15(12): p. https://doi.org/10.3390/info15120764.
49. Shin D, Kim J, Juliawan W, You I. Enhancing cloud-native DevSecOps: A Zero Trust approach for the financial sector. Computer Standards & Interfaces. 2025; 93: p. https://doi.org/10.1016/j.csi.2025.103975.
50. Sufi F. A global cyber-threat intelligence system with artificial intelligence. Internet of Things and Cyber-Physical Systems. 2023; 9: p. 1-12. https://doi.org/10.1016/j.dajour.2023.100364.
51. Daah C, Fallot Y, Qureshi A, Awan I, Konuw S. AI-driven zero trust and blockchain framework for secure operations. Expert Systems with Applications. 2026; 312: p. 1-27. https://doi.org/10.1016/j.eswa.2026.131577.

Deep Manishkumar D, Kishan Hiteshkumar J. Cybersecurity Resilience: A Strategic Imperative for Sustainable Digital Transformation. International Journal of Scientific and Research Publications. 2025; 15(7): p. 398-406.
1. https://dx.doi.org/10.29322/IJSRP.15.07.2025.p16336.

52. Arisian S, Halat K, Hafezalkotob A, Reenu M. Integrating Cyber Threat Intelligence Platforms in Critical Infrastructures. Engineering Applications of Artificial Intelligence. 2025; 197: p. 1-24. https://doi.org/10.1016/j.tre.2025.104043.
53. Rawindaran N, Jayal A, Prakash E. Cybersecurity Framework: Addressing Resiliency in Welsh SMEs. Cybersecurity. 2025; 5(2): p. https://doi.org/10.3390/jcp5020017.
54. Sousa de Araujo M, Souza B, Uchoa F. Resilience in the Context of Cyber Security: A Review. Applied Sciences. 2024; 14(5): p. https://doi.org/10.3390/app14052116.
55. Jančiūtė L. Cybersecurity in the financial sector and the quantum-safe transition. Cybersecurity. 2025; 6: p. 145–154. https://doi.org/10.1365/s43439-025-00135-7.

x