ISBN: 978-628-96613-3-0. ISSN: 2414-6390. Digital Object Identifier: https://dx.doi.org/10.18687/LACCEI2026.1.1.1896

Toward a Resilient Digital Ecosystem: A Strategic Analysis of Cybersecurity in Costa Rica

Tania Torres-Guillen [1]; Javier Rojas-Segura[2]; José Martinez-Villavicencio[3]
[1, 2, 3] Tecnológico de Costa Rica, Costa Rica, *ttorres@estudiantec.cr, jarojas@tec.ac.cr, jomartinez@tec.ac.cr*

Abstract– ***Cybersecurity is a strategic challenge that shapes the stability, trust, and digital future of nations. Following the high-impact cyberattacks experienced in recent years, Costa Rica faces the need to rethink its level of preparedness in an increasingly sophisticated digital environment. Using a qualitative approach, this study analyzes the state of cybersecurity in Costa Rica through the application of the SWOT–TOWS model, integrating indicators from the National Cyber Security Index and a case study analysis of local governments. The findings reveal that, although Costa Rica has made significant progress, its level of cyber maturity remains insufficient in light of the scale and complexity of current threats. The TOWS analysis enables the transformation of diagnosis into action by proposing strategies aimed at strengthening digital governance, fostering local technological innovation, and consolidating a preventive culture within public institutions. Overall, this study not only provides a snapshot of the current state of cybersecurity in Costa Rica but also offers a roadmap toward a more resilient, autonomous, and trustworthy digital ecosystem.***

Keywords—cybersecurity, comparative analysis, SWOT-TOWS, National Cyber Security Index, NCSI.

Hacia un Ecosistema Digital Resiliente: Un análisis Estratégico de la Ciberseguridad en Costa Rica

Tania Torres-Guillen [1]; Javier Rojas-Segura[2]; José Martinez-Villavicencio[3]
[1, 2, 3] Tecnológico de Costa Rica, Costa Rica, *ttorres@estudiantec.cr, jarojas@tec.ac.cr, jomartinez@tec.ac.cr*

Resumen– ***La ciberseguridad es un desafío estratégico que define la estabilidad, la confianza y el futuro digital de las naciones. Costa Rica, tras enfrentar ataques cibernéticos de alto impacto en los últimos años, se encuentra ante la necesidad de repensar su preparación frente a un entorno digital cada vez más sofisticado. Mediante un enfoque cualitativo este trabajo propone un análisis del estado de la ciberseguridad en Costa Rica, mediante la aplicación del modelo FODA–CAME, integrando los indicadores del National Cyber Security Index y un estudio de casos sobre gobiernos municipales. Los resultados evidencian que, aunque Costa Rica ha dado pasos importantes, la madurez cibernética sigue siendo insuficiente frente a la magnitud de las amenazas actuales. El análisis CAME permite transformar el diagnóstico en acción dado que propone estrategias para fortalecer la gobernanza digital, fomentar la innovación tecnológica local y consolidar una cultura preventiva desde las instituciones. En conjunto, este estudio no solo revela la radiografía actual de la ciberseguridad en Costa Rica, sino que también ofrece una hoja de ruta hacia un ecosistema digital más resiliente, autónomo y confiable.***

Palabras clave-- ciberseguridad, análisis comparativo, FODA–CAME, National Cyber Security Index, NCSI.

I. Introducción

La digitalización global ha impulsado una transformación profunda en los sistemas productivos, gubernamentales y sociales, generando múltiples beneficios, pero también una creciente exposición al riesgo cibernético. En este entorno, la ciberseguridad se ha consolidado como una estrategia para la sostenibilidad y competitividad nacional, al ser esencial para la protección de los activos tecnológicos, la privacidad de los datos y la confianza pública en los servicios digitales [1].

Costa Rica busca fortalecer la gobernanza, el marco legal y las capacidades técnicas, pero persisten brechas en inversión, formación y coordinación institucional [2]. El país enfrenta un panorama de amenazas en aumento: las denuncias por delitos informáticos crecieron de 1.662 en 2018 a 6.634 en 2024, un incremento del 300%, lo que evidencia la fragilidad del ecosistema digital costarricense [1].

Acorde al National Cyber Security Index (NCSI) [3], Costa Rica ocupa el puesto 70 de más de 160 países a nivel mundial con un puntaje de 48,33 sobre 100, lo que refleja un nivel medio-bajo de madurez cibernética. De acuerdo con los porcentajes otorgados a cada indicador, si bien existen avances en materia legal, como la protección de datos personales (100%) y la lucha contra el cibercrimen (81%), aún se evidencian debilidades críticas en investigación, innovación y defensa digital. Mientras que las municipalidades o gobiernos locales presentan un promedio de madurez cibernética de 1,2 sobre 4, lo que revela limitaciones estructurales y escasa capacidad para gestionar incidentes de seguridad [4].

Ref. [5] indica que la ciberseguridad debe abordarse desde un enfoque interdisciplinario, cooperativo y multilateral, articulando esfuerzos entre los gobiernos y la academia, propone que los Estados asuman un rol activo en la promoción de capacidades y la generación de ecosistemas de ayuda mutua entre industria, academia y gobiernos, con el fin de crear una cultura de seguridad digital sostenible. La realidad costarricense comparte características similares a la observada en otros países, una de las principales vulnerabilidades radica en la falta de conciencia y formación en seguridad cibernética entre los colaboradores, lo que puede llevarlos a que caigan en engaños como ataques de *phishing* [6].

Por ello, el objetivo de este estudio es analizar el estado de la ciberseguridad en Costa Rica, a nivel del gobierno nacional y de los gobiernos municipales, mediante la integración del análisis FODA–CAME, basado en los resultados del NCSI [3] y el estudio de casos de los gobiernos municipales [4], para identificar las brechas en la madurez cibernética y proponer estrategias concretas. Para orientar dicho objetivo, se la plantea la siguiente pregunta: ¿Qué estrategias pueden implementarse para mejorar la madurez cibernética de Costa Rica? Esta pregunta guía a la comprensión del impacto de las brechas existentes en la infraestructura de ciberseguridad, así como sus fortalezas.

II. Revisión de Literatura

En la actualidad, el avance acelerado de la digitalización impulsa la innovación y la transparencia en las instituciones, pero también expone a la sociedad a un nuevo tipo de vulnerabilidad: el riesgo cibernético. Por tanto, la ciberseguridad se consolida no solo como una necesidad técnica, sino como un componente esencial del desarrollo sostenible y la gobernanza moderna, capaz de equilibrar los beneficios de la conectividad con la protección de los derechos digitales y la confianza social [7].

A. Conceptualización de la Ciberseguridad

Ref. [8] describe a la ciberseguridad como una disciplina dentro de las ciencias de la computación, enfocada en el diseño e implementación de mecanismos para proteger la información y la infraestructura tecnológica. En términos generales, la ciberseguridad abarca la comprensión de diversos ataques cibernéticos y el diseño de estrategias de defensa que ayuden a preservar propiedades fundamentales, tales como la confidencialidad, la integridad y la disponibilidad de la información [9]. Sin embargo, los ataques actuales se han

vuelto más sofisticados y están dirigidos a víctimas específicas en función de las motivaciones del atacante, tales como obtener ganancias financieras, espionaje, coerción o venganza, aunque los ataques oportunistas, que no tienen un objetivo claro, también son muy comunes [10]. Por estas razones, la seguridad cibernética se mantiene como una preocupación prioritaria, dado que piratas informáticos y *crackers* continúan representando una amenaza constante. Con el desarrollo de las Tecnologías de la Información y la Comunicación (TIC), el uso generalizado de sistemas de software ha transformado la sociedad moderna de muchas maneras, pero también ha creado nuevos problemas en la protección de la información confidencial y sensible [11]. Las acciones más frecuentes son la detección de fraudes, la identificación de *malware*, la clasificación de *spam*, el *phishing*, la desactivación de *firewalls* y antivirus, el registro de pulsaciones de teclas, las URLs maliciosas y los ataques de sondeo, entre otras [12].

El entorno anónimo del ciberespacio permite innovadoras formas de actividad delictiva, al ampliar las modalidades de criminalidad y el rango de víctimas, que abarca desde individuos hasta gobiernos [7].

B. Los Gobiernos y su Vulnerabilidad Cibernética

La transformación digital de los gobiernos constituye una de las manifestaciones más visibles de la sociedad digital contemporánea. La digitalización, entendida como un proceso global que redefine la estructura y funcionamiento de los estados, las sociedades y los individuos, se ha convertido en una tendencia ineludible que configura la identidad de los gobiernos modernos. No obstante, su incorporación a la sociedad digital se produce en condiciones de desigualdad tecnológica y vulnerabilidad cibernética, derivadas de factores estructurales, económicos y organizativos, determinados por las condiciones tecnológicas, socioeconómicas, políticas y culturales de cada territorio [13]. En el caso costarricense, las municipalidades enfrentan desafíos similares a los observados en otros países en desarrollo como limitaciones financieras, escasez de personal especializado en TIC y deficiencias en la infraestructura digital de las zonas rurales. Estas carencias, sumadas a la creciente dependencia de plataformas extranjeras y servicios en la nube, exponen a los gobiernos municipales a riesgos en materia de ciberseguridad, que van desde la pérdida de datos hasta la interrupción de servicios esenciales [4].

La teoría y la práctica de la sociedad digital destacan que las tecnologías digitales, en rápida evolución, generan transformaciones profundas que exigen la adaptación de individuos, organizaciones y gobiernos [13], [14]. Esto demuestra que, más allá de disponer de recursos o herramientas, es esencial contar con un compromiso genuino desde los niveles más altos de la organización para incentivar al personal técnico y consolidar una cultura de ciberseguridad dentro de las municipalidades [4].

La brecha digital se impone como una dimensión crítica de la vulnerabilidad cibernética, mientras que algunos gobiernos avanzan hacia la integración plena de las tecnologías en su gestión, otros permanecen rezagados, lo que amplía las diferencias en capacidad de respuesta ante amenazas y ataques informáticos [7], [13]. Esta situación no solo afecta la eficiencia institucional, sino también la equidad social, dado que el acceso a servicios digitales seguros constituye hoy un nuevo derecho civil y humano [7]. Comprender el nivel de madurez digital y de ciberseguridad de los gobiernos municipales resulta esencial para evitar el rezago tecnológico, reducir la exposición a amenazas y consolidar una infraestructura digital resiliente [13].

La coordinación institucional y el liderazgo son pilares fundamentales para garantizar una gestión integral de la seguridad digital. Ref. [2] busca precisamente consolidar una estructura de gobernanza que articule los esfuerzos de los distintos actores públicos y privados. La existencia de marcos normativos robustos, así como de mecanismos de cooperación nacional e internacional, permite que las organizaciones actúen bajo lineamientos unificados frente a los riesgos digitales. Sin embargo, la ausencia de una autoridad central o la débil coordinación entre instituciones puede generar vacíos en la implementación efectiva de políticas de ciberseguridad.

C. Recursos Humanos y Capacidades Técnicas Especializadas

Uno de los desafíos más persistentes en materia de ciberseguridad es la escasez de talento especializado y la limitada formación técnica del personal encargado de la protección digital [3], [15]. Aunque se ha avanzado en la educación y el desarrollo profesional, todavía existe un déficit de capacidades que restringe la madurez de los sistemas de seguridad. Ref. [16] revela que el 86% de las empresas encuestadas a nivel global reportaron dificultades para cubrir vacantes en puestos de ciberseguridad. Esto demuestra que la inversión en capacitación, certificaciones y programas de desarrollo profesional constituye un requisito indispensable para fortalecer la resiliencia organizacional. Además, como se ha señalado, la escasez de profesionales en ciberseguridad genera una evidente deficiencia en la estructura necesaria para establecer un entorno de seguridad adecuado en el país, lo cual refleja una carencia significativa en la preparación de talento especializado [17]. Siendo que la creciente complejidad de los ciberataques representa una de las principales amenazas para las organizaciones contemporáneas, los ataques actuales son más específicos, persistentes y tecnológicamente avanzados [10].

D. Madurez Cibernética en Gobiernos Municipales

El estudio de [4], denominado Riesgo y Vulnerabilidad Cibernética en los gobiernos municipales de Costa Rica, constituye un aporte académico orientado a evaluar la madurez cibernética en el nivel municipal. Dicha investigación, desarrollada bajo un diseño de estudios de casos múltiples, analizó cinco municipalidades en 14 dimensiones organizacionales. Aplicó el Modelo de Madurez en Ciberseguridad (ECM^2), al igual que [18]. Ref. [4] seleccionó cinco municipalidades en distintas zonas de Costa Rica, En la Tabla I se presenta una breve caracterización de cada una, que

incluye información relevante sobre la población, presupuesto, índice de desarrollo humano cantonal (IDH-C) e índice de competitividad cantonal (ICC). Estos datos proporcionan una visión de la realidad específica de cada municipalidad, lo cual es crucial para contextualizar los resultados obtenidos en el análisis.

TABLA I
DATOS CONTEXTUALES DE LAS MUNICIPALIDADES ESTUDIADOS

Municipalidad	Población	Presupuesto Millones US$	IDH-C[1]	Categoría según IDH-C	ICC[2]
Atenas	30.407	5,83	0,831	Muy alto	0,470
Tilarán	21.232	10,07	0,772	Alto	0,443
Acosta	22.542	8,65	0,722	Alto	0,402
Dota	9.364	4,59	0,691	Medio	0,400
San Mateo	6.952	4,76	0,678	Medio	0,455

[1]Índice de Desarrollo Humano Cantonal 2022 [2]Índice de Competitividad Cantonal 2022-2023. Tomado de [4]

Una vez analizado el perfil de cada una de las cinco municipalidades, los resultados revelaron un nivel de riesgo alto, tal como se observa en la Tabla II, lo que refleja la limitada capacidad de los gobiernos municipales para prevenir, gestionar y responder ante amenazas digitales. Las áreas más críticas fueron Políticas de Ciberseguridad, Seguridad en las Comunicaciones y Gestión de Incidentes de Ciberseguridad, mientras que las dimensiones con mejor desempeño fueron Ciberseguridad en las Operaciones y Recurso Humano, destacando las campañas de concientización interna.

TABLA II
PRINCIPALES RESULTADOS CUANTITATIVOS DEL ESTUDIO DE CASOS

Dimensión Evaluada	Promedio (0–4)	Nivel de Riesgo	Observaciones Principales
Políticas de ciberseguridad	1,0	Alto	Escasa actualización y difusión limitada.
Organización interna	1,0	Alto	Falta de roles definidos y políticas de teletrabajo.
Ciberseguridad y recurso humano	1,6	Medio	Existencia parcial de campañas de concientización.
Manejo de activos	1,2	Alto	Almacenamiento seguro insuficiente.
Ciberseguridad en las operaciones	1,6	Medio	Mejores resultados en respaldo e integridad de la información.
Seguridad en las comunicaciones	0,9	Alto	Políticas débiles de confidencialidad y correo electrónico.
Gestión de incidentes de ciberseguridad	1,0	Alto	Sin protocolos ni análisis de causas.
Sistemas de información	1,2	Alto	Bajo nivel de mantenimiento de los sistemas de TI
Requerimientos legales (protección de datos)	1,0	Alto	Ausencia de políticas formales de protección de datos.
Promedio general	1,2 / 4	Alto	Bajo nivel de madurez cibernética.

Tomado de [4]

Ref. [4] indica que, los resultados reflejaron un contexto de riesgo cibernético elevado y una madurez institucional municipal deficiente, donde prevalecieron limitaciones financieras, brechas en infraestructura y escasa formación del personal técnico. La vulnerabilidad cibernética de los gobiernos municipales respondió no solo a la falta de recursos tecnológicos, sino también a la ausencia de cultura organizacional en ciberseguridad y a la discontinuidad de las políticas públicas municipales. Los hallazgos sugieren que el nivel de digitalización de los gobiernos municipales es diverso, con avances y rezagos significativos entre las diferentes municipalidades. Además, las municipalidades carecen de una infraestructura tecnológica adecuada, lo que dificulta la implementación de políticas de ciberseguridad robustas. La capacidad administrativa y presupuestaria también varía ampliamente entre los gobiernos municipales, ya que algunos tienen recursos suficientes para avanzar en la digitalización y ciberseguridad, mientras que otros enfrentan restricciones financieras y de personal.

E. National Cyber Security Index (NCSI)

El NCSI es un instrumento internacional creado en 2018 por la e-Governance Academy de Estonia, con el propósito de medir la preparación y el compromiso de los países en materia de ciberseguridad. Su objetivo es evaluar en qué medida los Estados cuentan con las capacidades necesarias para prevenir, gestionar y responder a amenazas digitales, así como para garantizar la protección de sus infraestructuras críticas y servicios esenciales. Se estructura a partir de 49 indicadores, organizados en 12 áreas de capacidad, las cuales se agrupan en tres grandes bloques: estratégico, preventivo y responsivo. Entre estas áreas se incluyen componentes como el desarrollo de políticas nacionales de ciberseguridad, la cooperación internacional, la educación y desarrollo del talento, la protección de datos personales, la defensa cibernética, la gestión de incidentes y la lucha contra el cibercrimen. Cada indicador es medido a partir de evidencias verificables (leyes, instituciones, programas, protocolos, mecanismos de cooperación, entre otros), lo cual aporta transparencia y comparabilidad al modelo [3].

A diferencia de otros índices que presentan resultados de carácter general, el NCSI ofrece un ranking dinámico y accesible en línea, que permite comparar el desempeño de más de 160 países en tiempo real. Además de su función comparativa, este índice se ha consolidado como una herramienta de fortalecimiento de capacidades, ya que no solo posiciona a los países en relación con sus pares, sino que también identifica brechas y áreas de mejora en la gestión de la ciberseguridad nacional. El NCSI posicionó a Costa Rica en el puesto 70 de más de 160 países a nivel mundial, con un puntaje global de 48,33 sobre 100, lo que refleja un nivel medio-bajo de preparación cibernética nacional. De acuerdo con el informe de 2025, Costa Rica presenta fortalezas en el ámbito legal y de respuesta ante el cibercrimen, pero mantiene brechas importantes en investigación, desarrollo y defensa cibernética militar, tal como se presenta en la Tabla III.

TABLA III
PRINCIPALES RESULTADOS OBTENIDOS EN EL NCSI

Dimensión / Indicador	Puntaje	Observaciones principales
1. Política Nacional de Ciber.	40%	Existen políticas y liderazgo, pero sin plan de acción actualizado.
2. Contribución Global en Ciber.	50%	Participación parcial en iniciativas internacionales.
3. Educación y Desarrollo Profesional	60%	Inclusión de competencias en primaria y secundaria; baja oferta universitaria.
4. Investigación y Desarrollo (I+D)	0%	Ausencia de programas y estudios doctorales en ciber.
5. Infraestructura Crítica de Información (CII)	25%	Identificación limitada de infraestructuras críticas y requisitos dispersos.
6. Ciber. Habilitadores Digitales	50%	Avances en firmas electrónicas e identificación digital.
7. Análisis y Concientización de Amenazas	50%	Publicación parcial de informes de amenazas y campañas públicas.
8. Protección de Datos Personales	100%	Legislación y autoridad nacional consolidadas.
9. Respuesta a Incidentes (CIRC)	64%	Capacidad operativa nacional y cooperación internacional establecidas.
10. Gestión de Crisis Cibernéticas	22%	Poca evidencia de ejercicios nacionales o reservas operativas.
11. Lucha contra el Cibercrimen	81%	Legislación completa y capacidad de investigación consolidada.
12. Defensa Cibernética Militar	0%	Inexistencia de doctrina o capacidades militares ciber.
Promedio General Nacional	48.33 / 100	Avances legales y operativos, pero con grandes brechas en innovación y defensa.

El desempeño de Costa Rica en 2025 evidencia un sistema de ciberseguridad en desarrollo, con avances normativos y operativos, pero con atrasos estructurales en innovación tecnológica, coordinación interinstitucional y capacidades militares. Destaca el 100% en protección de datos personales y el 81% en cibercrimen, mientras que la investigación y defensa militar presentan los niveles más bajos del índice con un 0% [3].

F. Análisis FODA

El FODA (Fortalezas, Oportunidades, Debilidades y Amenazas) es una herramienta estratégica ampliamente utilizada para evaluar tanto los factores internos como externos de una organización o sistema. Esta herramienta permite identificar los aspectos más importantes que afectan el desempeño y la capacidad de adaptación ante las amenazas y oportunidades. Ref. [11] indica que el análisis FODA proporciona un marco estructurado que facilita la toma de decisiones más informadas y efectivas, lo que a su vez contribuye a mitigar los riesgos potenciales asociados con las amenazas cibernéticas. En el caso específico de las TIC, que han transformado profundamente la sociedad moderna, el FODA puede identificar fortalezas como la capacidad de monitoreo continuo, la escalabilidad y la seguridad de los datos, de manera similar debilidades como la dependencia de la conectividad a internet y las potenciales inexactitudes en los sensores utilizados para la recolección de datos [19]. En este sentido, el FODA ofrece una visión completa de los modelos de seguridad, permitiendo construir estrategias alineadas con los requisitos prácticos y priorizando medidas de protección basadas en evidencia cuantificada [11]. Este enfoque también ha sido aplicado en diversos sectores industriales para gestionar riesgos y adaptar las tecnologías a nuevas realidades, como en la industria de la construcción 4.0 en Australia, donde el FODA ayudó a identificar amenazas de ciberseguridad y a desarrollar un ecosistema industrial más resiliente [20]. En el ámbito gubernamental, puede revelar tanto fortalezas institucionales como la existencia de marcos normativos y estructuras organizativas en ciberseguridad, pero también puede destacar las debilidades sistémicas, como la falta de políticas de respuesta ante incidentes o la dependencia tecnológica del exterior.

G. Análisis CAME

El análisis CAME (Corregir, Afrontar, Mantener y Explotar) es una metodología complementaria que amplía el análisis FODA, permitiendo transformar los diagnósticos identificados en acciones estratégicas concretas. Este análisis permite un enfoque dinámico y adaptable a las circunstancias cambiantes del entorno, facilitando la implementación de acciones correctivas y la gestión de riesgos [21]. Este marco se basa en la interacción de los factores estratégicos identificados en el FODA, donde se busca corregir las debilidades internas de una organización, como la falta de personal especializado o deficiencias en la infraestructura de ciberseguridad. A su vez, afrontar las amenazas, como los riesgos de ciberseguridad derivados de la creciente dependencia digital y la exposición a ciberataques, es una prioridad esencial para mantener la resiliencia operativa del gobierno. Además, el análisis CAME destaca la importancia de mantener las fortalezas existentes, tales como políticas de protección efectivas o una estructura organizativa robusta, mientras se explotan las oportunidades que ofrece la digitalización para mejorar la eficiencia y la accesibilidad de los servicios gubernamentales [21]. Al aplicar el CAME al contexto de la ciberseguridad, los gobiernos pueden desarrollar estrategias más sostenibles y orientadas al largo plazo. La interacción entre las fortalezas, debilidades, oportunidades y amenazas identificadas, se derivan cuatro tipos de estrategias que orientan la toma de decisiones [22], tal como se muestra en la Tabla IV.

TABLA IV
PRINCIPALES RESULTADOS OBTENIDOS EN EL NCSI

Tipo de Estrategia	Descripción
Reorientación	Buscan transformar las debilidades internas en oportunidades de mejora, aprovechando los factores externos favorables.
Supervivencia	Se orientan a reducir las debilidades existentes y a proteger a la organización frente a posibles amenazas del entorno.
Defensivas	Pretenden aprovechar las fortalezas disponibles para mitigar o contrarrestar el impacto de las amenazas externas.
Ofensivas	Comprenden acciones que potencian fortalezas internas para aprovechar al máximo las oportunidades del entorno.

III. Metodología

El presente estudio adopta un enfoque cualitativo, basado en la revisión y el análisis estratégico de información secundaria. Su propósito es integrar los hallazgos del estudio de casos sobre riesgo y vulnerabilidad cibernética en los gobiernos municipales de Costa Rica [4] y los resultados del Índice Nacional de Ciberseguridad (NCSI) [3], con el fin de elaborar un análisis FODA–CAME que permita identificar las condiciones actuales de madurez cibernética del país. Este se complementa con un análisis documental específicamente de la Estrategia Nacional de Ciberseguridad 2023-2027 [2]. De acuerdo con [23], el enfoque cualitativo busca comprender los fenómenos sociales y tecnológicos desde su contexto natural, priorizando la interpretación de los hechos por encima de la medición cuantitativa. Por tanto, el estudio no pretende generar nuevos datos empíricos, sino interpretar de manera integral los resultados de investigaciones previas y fuentes oficiales, a fin de identificar fortalezas, debilidades, oportunidades y amenazas en la gestión cibernética del Estado costarricense. Los hallazgos se transforman en estrategias mediante la aplicación del modelo CAME, el cual permite orientar las políticas de fortalecimiento institucional y la formulación de acciones sostenibles en materia de ciberseguridad.

Esta metodología busca caracterizar los factores internos y externos que inciden en la gestión de la ciberseguridad a nivel nacional y local, sin manipular variables, sino observando los fenómenos tal como se presentan en su contexto real [23]. A su vez, el enfoque cualitativo posibilita la interpretación de los hallazgos desde una perspectiva analítica y contextual, integrando información documental, institucional y comparativa.

Para efectos de la interpretación y clasificación de los resultados obtenidos, de acuerdo con la literatura metodológica sobre análisis estratégico y evaluación comparativa, la clasificación de los resultados en fortalezas y debilidades puede sustentarse en criterios relativos al desempeño promedio del conjunto analizado. En este sentido, diversos autores señalan que los valores que se sitúan por encima del promedio general reflejan un desempeño superior relativo y, por tanto, pueden interpretarse como fortalezas, mientras que aquellos ubicados por debajo del promedio evidencian brechas de desempeño y se clasifican como debilidades [22], [23]. Este enfoque es coherente con la aplicación del análisis FODA basado en indicadores cuantitativos, ya que permite identificar ventajas y limitaciones internas no de forma absoluta, sino en relación con el comportamiento general del sistema evaluado. En consecuencia, en este estudio se consideran fortalezas los factores que obtuvieron valores superiores al promedio general, y debilidades aquellos que se situaron por debajo de dicho promedio.

IV. Resultados

Este estudio evaluó el estado de la ciberseguridad en el Gobierno de Costa Rica, tanto a nivel nacional como local, mediante un análisis FODA y la aplicación de estrategias CAME. Los resultados muestran avances en áreas como la legislación y cooperación internacional, pero también destacan desafíos importantes, como la falta de coordinación institucional y la escasez de personal especializado, que limitan la eficacia de las políticas de ciberseguridad.

A. Análisis FODA según National Cybersecurity Index

El análisis del NCSI para Costa Rica 2025 permite evaluar el grado de madurez cibernética del país, considerando sus capacidades institucionales, regulatorias y técnicas. Los resultados, con una puntuación total de 48,33 puntos y una posición 70 de 160 países a nivel mundial (Tabla III), reflejan un estado intermedio de desarrollo, ya que existen bases legales y estratégicas relevantes, pero aún persisten brechas significativas en la ejecución práctica, la coordinación interinstitucional y la inversión en investigación aplicada. En la Tabla V se presenta el análisis FODA.

TABLA V
ANÁLISIS FODA DEL NCSI PARA COSTA RICA EN EL 2025

FORTALEZAS	**OPORTUNIDADES**
F1: Marco legal e institucional consolidado en protección de datos personales (100%). F2: Alta conciencia sobre ciberseguridad en Costa Rica, impulsada por la disponibilidad de recursos educativos y análisis de amenazas (50%) F3: Compromiso internacional en cibercrimen (81%) y cooperación global (50%), incluyendo la adhesión al Convenio de Budapest. F4: Existencia de unidades especializadas en investigación y persecución de ciberdelitos (100%) F5: Alta capacidad nacional de respuesta ante incidentes (64%) gracias al CSIRT-CR y la cooperación regional.	O1: Fortalecimiento de alianzas público-privadas y académicas en materia de ciberseguridad. O2: Creación de un entorno digital confiable que impulse la economía digital nacional (público y privado) O3: Fortalecimiento de la implementación de tecnologías de firma electrónica e identificación digital a través de iniciativas del sector privado.
DEBILIDADES	**AMENAZAS**
D1: Falta de coordinación estratégica y liderazgo institucional (40%). D2: Ausencia de una autoridad central de gobernanza en ciberseguridad (0%) D3: Escasa inversión en investigación, desarrollo e innovación (I+D) (0%.) D4: Débil defensa digital y baja protección de infraestructuras críticas (25%). D5: Dependencia de lineamientos administrativos sin obligatoriedad integral (0%)	A1: Incremento en la frecuencia y sofisticación de los ciberataques a instituciones públicas y privadas. A2: Escasez de profesionales especializados en ciberseguridad y falta de educación digital temprana. A3: Dependencia tecnológica del exterior (servicios en la nube, software, infraestructura crítica). A4: Riesgos crecientes para la seguridad nacional y la estabilidad económica derivados de ataques de alto impacto.

B. Análisis FODA de los Gobiernos Municipales

Los resultados del estudio de Ref. [4], sobre el riesgo y vulnerabilidad cibernética en los gobiernos municipales, mostraron un promedio de madurez de 1,2 sobre 4 (Tabla II). Lo que corresponde a un nivel de riesgo alto, evidenciando que estos gobiernos poseen escasa capacidad para prevenir, gestionar y responder ante amenazas cibernéticas. En la Tabla VI se detalla el análisis FODA de los gobiernos municipales.

TABLA VI
ANÁLISIS FODA DEL ESTUDIO DE CASOS DE GOBIERNOS MUNICIPALES

FORTALEZAS	**OPORTUNIDADES**
F1. Creciente conciencia institucional sobre la importancia estratégica de la ciberseguridad (1,4) F2. Reconocimiento del riesgo cibernético por parte del personal de Tecnologías de la Información (TI), aun en ausencia de incidentes graves (1,4) F3. Avances iniciales en capacitación y sensibilización del recurso humano mediante talleres y campañas básicas (1,6) F4. Implementación parcial de controles de seguridad y respaldo de información como antivirus, contraseñas seguras, copias de respaldo (1,8)	O1. Fortalecimiento de la ciberseguridad mediante alianzas internacionales y el apoyo del sector privado O2. Transferencia de conocimiento con universidades y el sector privado para capacitación, desarrollo de políticas y transferencia de conocimiento. O3. Aprovechamiento de la transformación digital municipal (ciudadano digital) para integrar la ciberseguridad desde el diseño de los servicios públicos.
DEBILIDADES	**AMENAZAS**
D1. Bajo nivel general de madurez cibernética (1,2) que refleja un alto riesgo institucional. D2. Falta de políticas, procedimientos y documentación formal en temas de seguridad digital (1,2) D3. Deficiente gestión de incidentes cibernéticos, sin protocolos de detección, registro ni análisis de causas (0,4) D4. Dependencia de la voluntad política de los jerarcas municipales para impulsar acciones sostenibles (1,6)	A1. Aumento de ciberataques dirigidos a gobiernos municipales, especialmente mediante *ransomware, phishing* e ingeniería social. A2. Inestabilidad política y administrativa que interrumpe la continuidad de las políticas de ciberseguridad. A3. Pérdida de confianza ciudadana ante posibles incidentes que afecten la integridad o disponibilidad de los servicios digitales. A4. Restricciones presupuestarias y falta de personal especializado en ciberseguridad.

C. Estrategia CAME

A partir del análisis FODA realizado entre el NCSI (Tabla IV) y los gobiernos municipales (Tabla VI), se identificaron variables compartidas que afectan tanto al gobierno local como al nacional en términos de ciberseguridad, en la Tabla VII se aborda de manera integral la estrategia CAME.

TABLA VII
ESTRATEGIA CAME

ESTRATEGIAS CAME PARA EL GOBIERNO NACIONAL Y LOCAL			
		FACTORES EXTERNOS	
		AMENAZAS	**OPORTUNIDADES**
FACTORES INTERNOS	**FORTALEZAS**	**ESTRATEGIAS DEFENSIVAS** 1. Utilizar el marco legal robusto en protección de datos y fortalecer la cooperación internacional para prevenir y gestionar los ciberataques 2. Reforzar cooperación con organismos internacionales para mejorar la formación y crear equipo especializado en ciberseguridad, aprovechando la experiencia internacional. 3. Transferir capacidades del CSIRT-CR y de unidades especializadas del nivel nacional hacia gobiernos municipales mediante asistencia técnica directa para elevar su madurez operativa.	**ESTRATEGIAS OFENSIVAS** 1. Fortalecer el CSIRT-CR mediante alianzas con el sector privado y las universidades, y aprovechar su experiencia en la respuesta ante incidentes para capacitar a los gobiernos municipales en prevención y mitigación de ataques. 2. Aprovechar las capacidades del Organismo de Investigación Judicial y el Ministerio Público en la investigación de ciberdelitos para desarrollar políticas públicas y protocolos de protección digital.
	DEBILIDADES	**ESTRATEGIAS DE SUPERVIVENCIA** 1. Implementar protocolos de respuesta ante incidentes y políticas de seguridad digital claras, aprovechando la cooperación con el sector privado y organismos internacionales. 2. Crear programas de formación en ciberseguridad a nivel municipal en colaboración con universidades y empresas tecnológicas. 3. Establecer mecanismos obligatorios de continuidad operativa que garanticen la estabilidad de las políticas de ciberseguridad ante cambios políticos en los gobiernos municipales.	**ESTRATEGIAS DE REORIENTACIÓN** 1. Establecer un modelo de colaboración público-privada que permita coordinar las políticas de ciberseguridad y aprovechar los recursos externos. 2. Atraer inversiones externas para desarrollar soluciones locales de protección de infraestructuras críticas e impulsar la innovación tecnológica en las municipalidades a través de colaboración con universidades y el sector privado. 3. Impulsar programas nacionales de investigación e innovación en ciberseguridad en coordinación con universidades y sector privado para reducir la dependencia tecnológica del exterior y fortalecer la capacidad de respuesta tanto nacional como municipal. 4. Crear una autoridad nacional única de gobernanza en ciberseguridad que coordine lineamientos, políticas y estándares con todas las instituciones, incluyendo gobiernos municipales.

V. Discusión

En el análisis del NCSI y el estudio de casos de los gobiernos municipales, se observa que, aunque existen políticas, la implementación de estas medidas y, por ende, la madurez cibernética a nivel nacional y local aún requieren grandes mejoras para enfrentar la creciente sofisticación de los ciberataques. Aunque Costa Rica ha avanzado en el establecimiento de un marco legal consolidado para la ciberseguridad, como lo demuestra su calificación en protección de datos personales (100%) según el NCSI [3], persisten serias deficiencias en la implementación práctica de estas políticas y en la preparación general ante los ciberataques. Esta contradicción entre la legislación y la ejecución deficiente refleja una desconexión preocupante entre la teoría y la práctica, que limita la eficacia de los esfuerzos nacionales en la protección cibernética. Uno de los problemas más destacados es la falta de coordinación institucional y liderazgo centralizado. Si bien el Estado ha establecido marcos normativos en ciberseguridad, como la Estrategia Nacional de Ciberseguridad 2023-2027 [2], estos no se traducen en acciones efectivas debido a la fragmentación en su implementación. Ref. [24] señala la ausencia de un liderazgo claro y la coordinación entre entidades genera un vacío de poder que obstaculiza la creación de políticas consistentes y efectivas. Este vacío también limita la capacidad de respuesta ante incidentes, especialmente en los niveles locales, donde la gestión reactiva ante ciberamenazas se ha convertido en la norma debido a la falta de protocolos estandarizados y formación especializada [25]. La desorganización en la gestión cibernética, a nivel local, resulta en una incapacidad de prevenir o gestionar adecuadamente las amenazas cibernéticas.

En cuanto a la conciencia organizacional, a pesar de las campañas de concienciación sobre el uso responsable de la información y la seguridad digital [26], estas siguen siendo iniciativas aisladas sin una integración real en la cultura institucional. La escasa implementación de estas campañas dentro de las políticas y prácticas institucionales demuestra que la conciencia sigue siendo insuficiente. En lugar de convertirse en una verdadera cultura de seguridad, la conciencia sobre ciberseguridad a menudo se reduce a ejercicios puntuales sin un enfoque completo. Esto deja a las instituciones, tanto a nivel nacional como local, expuestas a ataques cibernéticos cada vez más sofisticados.

En términos de la capacidad técnica para afrontar los ciberataques, Costa Rica enfrenta una de sus mayores debilidades, la escasez de personal especializado en ciberseguridad. Según [3], el puntaje de Costa Rica en investigación y desarrollo (0%) refleja una profunda carencia en innovación tecnológica y en la creación de talento local en el campo de la ciberseguridad. Esta deficiencia podría traducirse en una de las razones por las cuales el país sigue siendo vulnerable ante ataques complejos, [10] menciona que que los ataques *ransomware* y *phishing* están dirigidos cada vez más a instituciones gubernamentales. La falta de inversión en la formación de talento especializado contribuye a un círculo vicioso de vulnerabilidad, donde la escasez de expertos limita la capacidad de detección, análisis y respuesta ante incidentes. Es fundamental implementar incentivos que fomenten la inscripción y graduación de estudiantes en programas de ciberseguridad, como becas y apoyos económicos, que ayuden a reducir barreras financieras. La conexión con el mercado laboral, mediante alianzas con empresas tecnológicas, permitirá a los estudiantes obtener experiencia práctica y mejorar sus oportunidades de empleo. Además, sensibilizar a la sociedad desde edades tempranas sobre la ciberseguridad, ayudará a reducir la brecha de talento en el país [15].

Por otra parte, a nivel local, la baja madurez cibernética es aún más alarmante. Según [4], la mayoría de las municipalidades costarricenses presentan un promedio de madurez de 1,2 sobre 4, lo que refleja un riesgo cibernético alto. Esto se debe a la falta de normativas formales de ciberseguridad, la ausencia de protocolos de respuesta ante incidentes y la dependencia de la voluntad política para implementar acciones que sean realmente sostenibles a largo plazo. Este vacío institucional hace que las municipalidades estén desprotegidas y mal preparadas para afrontar amenazas digitales, lo que puede resultar en pérdidas económicas y un daño reputacional significativo en caso de un ciberataque. Además, la creciente dependencia de tecnologías extranjeras en el ámbito gubernamental agrava la vulnerabilidad cibernética. Costa Rica, al igual que otros países de América Latina, está cada vez más expuesta a riesgos geopolíticos y de soberanía digital debido a su dependencia de servicios en la nube y plataformas tecnológicas extranjeras [26]. Este modelo, aunque rentable a corto plazo, expone al país a interrupciones de servicios críticos y a un riesgo aumentado de ataques cibernéticos externos que comprometen la infraestructura digital nacional.

En cuanto a las estrategias de colaboración, a pesar de que Costa Rica ha logrado establecer ciertos acuerdos internacionales en el ámbito de la ciberseguridad, como la cooperación en cibercrimen con organismos internacionales [2] estas iniciativas no se han materializado plenamente en acciones tangibles. La cooperación público-privada es aún insuficiente, y los canales de colaboración entre el gobierno, las universidades y el sector privado son limitados, lo que impide una respuesta eficaz y coordinada frente a las amenazas cibernéticas [27].

Finalmente, la confianza ciudadana sigue siendo un tema de interés. Cualquier incidente que afecte la integridad o disponibilidad de los servicios municipales puede destruir la confianza pública en las plataformas digitales y reducir la percepción de transparencia y eficiencia en los gobiernos municipales [28]. La resistencia al uso de herramientas electrónicas puede tener repercusiones negativas en la legitimidad de los gobiernos municipales, lo que refuerza la necesidad de acciones inmediatas para fortalecer la infraestructura de ciberseguridad y garantizar la confianza de los ciudadanos en los servicios digitales.

VI. Conclusiones

El análisis de la ciberseguridad en Costa Rica, a través del modelo FODA-CAME y los resultados obtenidos del NCSI, revela tanto avances importantes como desafíos persistentes en la protección digital del país. A pesar de contar con un marco legal robusto en protección de datos personales y una cooperación internacional activa en el combate al cibercrimen, las municipalidades y el gobierno nacional enfrentan debilidades que deben ser abordadas para mejorar la resiliencia digital y la eficacia en la respuesta ante amenazas cibernéticas.

Uno de los hallazgos más destacados es la falta de coordinación institucional y la ausencia de una autoridad centralizada que gestione de manera cohesiva las políticas de ciberseguridad a nivel nacional y local. Esta fragmentación limita la efectividad de las políticas y aumenta la vulnerabilidad ante los ciberataques. Para corregir esta debilidad, se hace urgente la creación de una estructura de gobernanza coherente, que fomente una coordinación más eficaz entre los diferentes actores del ecosistema de ciberseguridad, incluyendo gobierno, sector privado, la academia y organismos internacionales [29].

Además, la escasez de personal especializado en ciberseguridad y la falta de recursos técnicos adecuados son barreras críticas para gestionar los riesgos cibernéticos de manera efectiva [15]. Esto resalta la necesidad de fortalecer la formación técnica y la capacitación especializada a nivel local. Programas de formación en colaboración con universidades y empresas tecnológicas serán fundamentales para reducir el déficit de talento y garantizar que las municipalidades cuenten con los profesionales capacitados para enfrentar los desafíos emergentes en el campo de la ciberseguridad.

Cabe destacar, que el nivel de digitalización de los gobiernos municipales en Costa Rica presenta una gran diversidad, con avances significativos en algunos municipios, mientras que otros aún enfrentan retos considerables. La falta de recursos humanos especializados en tecnologías de la información, la dependencia de servicios externos para la digitalización y la infraestructura tecnológica insuficiente limitan la capacidad de varios gobiernos municipales para implementar políticas de ciberseguridad efectivas. Además, la capacidad administrativa y presupuestaria varía considerablemente, lo que crea una brecha entre los municipios que tienen los recursos necesarios para avanzar en la digitalización y la ciberseguridad y aquellos que enfrentan restricciones financieras y de personal.

En cuanto a las amenazas cibernéticas, la creciente sofisticación de los ataques representa un riesgo tanto para el gobierno nacional como para los gobiernos municipal. La dependencia de proveedores internacionales de infraestructuras tecnológicas aumenta la vulnerabilidad de los sistemas nacionales ante ataques dirigidos. Por ello, es crucial adoptar estrategias de reorientación, como el fomento de capacidades locales y la reducción de la dependencia tecnológica externa, para mejorar la autonomía digital de Costa Rica y proteger las infraestructuras críticas.

Las oportunidades identificadas, como la cooperación internacional y las alianzas público-privadas, son esenciales para mejorar la capacidad de respuesta y la gestión de incidentes cibernéticos. La creación de un entorno digital confiable mediante el uso de tecnologías seguras, como la firma electrónica y la identificación digital, también es una oportunidad significativa para fortalecer la confianza ciudadana en los servicios públicos digitales y promover la economía digital en el país.

En términos de estrategias para el futuro, la implementación de estrategias dinámicas y adaptativas, como las planteadas en el análisis CAME, será esencial para abordar las debilidades y amenazas de manera efectiva, al mismo tiempo que se aprovechan las fortalezas internas y las oportunidades externas. La adopción de estas estrategias permitirá a Costa Rica no solo mejorar la infraestructura de ciberseguridad, sino también fortalecer la resiliencia digital a largo plazo, adaptándose a un entorno digital cada vez más complejo y dinámico.

Es decir, para que las políticas y acciones estratégicas propuestas sean efectivas, es fundamental que exista un compromiso continuo por parte de todos los sectores involucrados: gobiernos, sector privado, universidades y organismos internacionales. Esto garantizará una respuesta efectiva ante los retos de ciberseguridad, consolidando un ecosistema digital seguro y confiable.

Finalmente, se destaca que el análisis realizado con NCSI destaca las fortalezas de Costa Rica en áreas como la legislación y la respuesta ante el cibercrimen, pero también revela brechas significativas en campos como I+D, desarrollo tecnológico y defensa cibernética militar. Sin embargo, es importante señalar que el NCSI, como cualquier indicador compuesto, presenta ciertas imperfecciones. En particular, asigna una valoración de cero en categorías como la defensa cibernética militar, debido a la ausencia de un ejército en Costa Rica. Esto no refleja necesariamente la realidad de la capacidad de defensa digital del país, pero influye directamente en la puntuación asignada. Este sesgo destaca la limitación de los indicadores compuestos, ya que la ausencia de fuerzas armadas no implica una incapacidad para enfrentar amenazas cibernéticas, sino que simplemente refleja la estructura política y de defensa única de Costa Rica.

References

[1] E. Vega, L. Picado, A. Villegas, y C. Solis, «Estado de la Ciberseguridad en Costa Rica 2024», Universidad Nacional - Sede Regional Chorotega, 2025. [En línea]. Disponible en: https://repositorio.una.ac.cr/server/api/core/bitstreams/4853e1b3-c476-4932-9452-252a257c7d4e/content

[2] MICITT, «Estrategia Nacional de Ciberseguridad 2023-2027», Ministerio de Ciencia, Tecnología y Telecomunicaciones, San Jose, Costa Rica, ENC 2023, 2023. [En línea]. Disponible en: https://www.micitt.go.cr/sites/default/files/2023-06/Estrategia-Nacional-de-Ciberseguridad-MICITT-2023-2027.pdf

[3] NCSI, «NCSI :: Costa Rica». Accedido: 30 de enero de 2026. [En línea]. Disponible en: https://ncsi.ega.ee/country/cr/

[4] F. Quiros Perez, J. Rojas-Segura, y J. Martinez-Villavicencio, «Cyber Risk and Vulnerability in Local Governments of Costa Rica: A Case Study», en Proceedings of the 5th LACCEI International Multiconference on Entrepreneurship, Innovation and Regional Development (LEIRD 2025): «Entrepreneurship with Purpose: Social and Technological Innovation in the Age of AI», Cartagena, Colombia: Latin American and Caribbean Consortium of Engineering Institutions, 2025. doi: 10.18687/LEIRD2025.1.1.239.

[5] O. Bustillos Ortega y J. Rojas Segura, «Cómo promueven los estados la ciberseguridad de las PYMEs», *Interfases*, vol. 17, n.o 1, pp. 168-186, 2023, doi: https://doi.org/10.26439/interfases2023.n017.6246.

[6] J. D. Solano, «Propuesta para mejorar la seguridad de la comunicación de datos de las organizaciones de Costa Rica a través de internet.», CENFOTEC, San Jose, Costa Rica, 2024. [En línea]. Disponible en: https://repositorio.ucenfotec.ac.cr/bitstream/handle/123456789/521/PIA02-Solano%20Romero%20Jeffry%20David_MSEG_2024.pdf?sequence=1&isAllowed=y

[7] L. Robinson et al., «Digital inequalities 3.0: emergent inequalities in the information age», *First Monday*, vol. 25, n.o 7, 2020, doi: https://doi.org/10.5210/fm.v25i7.10844.

[8] C. C. Urcuqui López., A. Navarro Cadavid, J. L. Osorio Quintero, y M. García Peña, Ciberseguridad: un enfoque desde la ciencia de datos - Primera edición. Universidad Icesi, 2018. Accedido: 30 de enero de 2026. [En línea]. Disponible en: http://hdl.handle.net/10906/84046

[9] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, P. Watters, y A. Ng, «Cybersecurity data science: an overview from machine learning perspective», *J Big Data*, vol. 7, n.o 1, p. 41, jul. 2020, doi: 10.1186/s40537-020-00318-5.

[10] H. S. Lallie et al., «Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic», *Computers & Security*, vol. 105, p. 102248, jun. 2021, doi: 10.1016/j.cose.2021.102248.

[11] A. Khalid, M. Raza, P. Afsar, R. A. Khan, M. I. Mohmand, y H. U. Rahman, «A SWOT Analysis of Software Development Life Cycle Security Metrics», *Journal of Software: Evolution and Process*, vol. 37, n.o 1, p. e2744, 2025, doi: 10.1002/smr.2744.

[12] K. Shaukat et al., «Performance Comparison and Current Challenges of Using Machine Learning Techniques in Cybersecurity», *Energies*, vol. 13, n.o 10, p. 2509, ene. 2020, doi: 10.3390/en13102509.

[13] S. Jamanbalayeva, E. Burova, A. Sagikyzy, D. Zhanabayeva, y A. Adamidi, «The paradigm of the digital society: synthesis of technocratic and socio-humanitarian approaches», *Cogent Social Sciences*, vol. 11, n.o 1, p. 2513460, dic. 2025, doi: 10.1080/23311886.2025.2513460.

[14] J. Rojas-Segura, M. Faith-Vargas, y J. Martinez-Villavicencio, «Conceptualizing digital transformation using semantic decomposition», *Tec Empresarial*, vol. 17, n.o 3, pp. 63-75, dic. 2023, doi: 10.18845/te.v17i3.6850.

[15] O. Bustillos Ortega, J. Rojas Segura, y J. Murillo-Gamboa, «Ciberseguridad y desarrollo de habilidades digitales: propuesta de alfabetización digital en edades tempranas», *Interfases*, vol. 18, n.o 2, pp. 185-205, dic. 2023, doi: 10.26439/interfases2023.n018.6626.

[16] CISCO, «Estudio de Cisco Revela Deficiencias Alarmantes en la Preparación de Seguridad», *Cisco News The Americas Network*. Accedido: 30 de enero de 2026. [En línea]. Disponible en: https://news-blogs.cisco.com/americas/es/2025/05/08/estudio-de-cisco-revela-deficiencias-alarmantes-en-la-preparacion-de-seguridad/

[17] C. A. Madrigal, M. G. García, I. M. Zumbado, T. M. Murillo, M. R. González, y V. S. Ruiz, «Un Análisis del sistema educativo costarricense: Desafío crítico para la ciberseguridad del país», *Rhombus*, vol. 3, n.o 2, sep. 2023, Accedido: 30 de enero de 2026. [En línea]. Disponible en: https://revistas.ulacit.ac.cr/index.php/rhombus/article/view/89

[18] T. Howell, J. Rojas-Segura, J. Martinez-Villavicencio, y C. Rodriguez Bravo, «Vulnerabilidades en la Seguridad Cibernética de Empresas: Un Estudio de Casos», en Proceedings of the 23rd LACCEI International Multi-Conference for Engineering, Education and Technology (LACCEI): «Engineering, Artificial Intelligence, and Sustainable Technologies in service of society», Mexico City: Latin American and Caribbean Consortium of Engineering Institutions, 2025. doi: 10.18687/LACCEI2025.1.1.1773.

[19] M. Gavrilă, M.-G. Murariu, R.-E. Ambrozie, y D. Tărniceriu, «SWOT Analysis of a Blockchain and IoT-Based System for Alcohol and Health Monitoring in Road Safety», en 2025 International Symposium on Signals, Circuits and Systems (ISSCS), jul. 2025, pp. 1-4. doi: 10.1109/ISSCS66034.2025.11105686.

[20] S. Siriwardhana, R. Moehler, y Y. Fang, «Exploring the Determinants of Construction 4.0 Implementation in Australian Construction Industry: A SWOT Analysis», en Proceedings of the International Conference on Smart and Sustainable Built Environment (SASBE 2024), A. GhaffarianHoseini, A. Ghaffarianhoseini, F. Rahimian, y M. Babu Purushothaman, Eds., Singapore: Springer Nature, 2025, pp. 830-841. doi: 10.1007/978-981-96-4051-5_80.

[21] N. González-Cancelas, J. P. C. Palacios Calzada, J. Vaca-Cabrero, y A. Camarero-Orive, «Optimizing Sustainable Port Logistics in Spanish Ports with Emerging Technologies», *Sustainability*, vol. 17, n.o 8, p. 3392, ene. 2025, doi: 10.3390/su17083392.

[22] M. J. Sánchez Pérez, «Modelo de Gestión de Calidad de los Departamentos de Orientación Educativa en los Institutos de Educación Secundaria de la Comunidad Valenciana», Universidad de Valencia, Valencia, España, 2015. Accedido: 30 de enero de 2026. [En línea]. Disponible en: http://hdl.handle.net/10550/51532

[23] R. Hernández-Sampieri y C. Mendoza, Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta, Primera Edición. Ciudad de México: Mcgraw-Hill México, 2018.

[24] M. Karpiuk, «The Local Government's Position in the Polish Cybersecurity System.», Lex Localis: *Journal of Local Self-Government*, vol. 19, n.o 3, 2021, doi: 10.4335/19.3.609-620(2021).

[25] S. T. Hossain, T. Yigitcanlar, K. Nguyen, y Y. Xu, «Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework», *Applied Sciences*, vol. 14, n.o 13, Art. n.o 13, ene. 2024, doi: 10.3390/app14135501.

[26] M. Domínguez-Dorado, F. J. Rodríguez-Pérez, J. Carmona-Murillo, D. Cortés-Polo, y J. Calle-Cancho, «Boosting Holistic Cybersecurity Awareness with Outsourced Wide-Scope CyberSOC: A Generalization from a Spanish Public Organization Study», Information, vol. 14, n.o 11, Art. n.o 11, nov. 2023, doi: 10.3390/info14110586.

[27] O. Flor-Unda, F. Simbaña, X. Larriva-Novo, Á. Acuña, R. Tipán, y P. Acosta-Vargas, «A Comprehensive Analysis of the Worst Cybersecurity Vulnerabilities in Latin America», *Informatics*, vol. 10, n.o 3, Art. n.o 3, sep. 2023, doi: 10.3390/informatics10030071.

[28] R. Shandler y M. A. Gomez, «The hidden threat of cyber-attacks – undermining public confidence in government», *Journal of Information Technology & Politics*, vol. 20, n.o 4, pp. 359-374, oct. 2023, doi: 10.1080/19331681.2022.2112796.

[29] J. Rojas-Segura et al., «How to evaluate the cyber risk of SMEs? An Academia strategy to create competitive advantages», en Proc. LACCEI int. multi-conf. eng. educ. technol., Latin American and Caribbean Consortium of Engineering Institutions, 2024. doi: 10.18687/LACCEI2024.1.1.639.Manuscript Templates for Conference Proceedings, IEEE. http://www.ieee.org/conferences_events/conferences/publishing/templates.html