Cyber Risk and Vulnerability in Local Governments of Costa Rica: A Case Study

Fabiana Quirós Pérez [1]; Javier Rojas-Segura[2]; José Martinez-Villavicencio[3]
[1, 2, 3] Tecnológico de Costa Rica, Costa Rica, *fabianaquirosp@estudiantec.cr, jarojas@tec.ac.cr, jomartinez@tec.ac.cr*

Abstract– ***Cybersecurity has become a major global concern due to its direct connection to the protection of sensitive information. However, academic research has largely focused on other sectors, overlooking local governments that also face significant challenges. This gap in the literature is precisely what this study seeks to address. The research aimed to identify the main cybersecurity vulnerabilities affecting five selected municipalities of Costa Rica, as well as to assess their current level of cybersecurity maturity using the Cybersecurity Maturity Model. A case study methodology was used, applying a fourteen-dimensional questionnaire. This approach enabled the collection of data on cybersecurity policies, practices, and resources within the municipalities. Findings revealed a low level of cybersecurity maturity, particularly in areas such as "Cybersecurity Policies," "Communications Security," and "Cybersecurity Incident Management," exposing municipalities to significant cyber risks. These results highlight the situation of digital public management, contributing to filling the academic gap on the subject.***

Keywords-- ***Cybersecurity, local governments, cyber risk, municipalities, maturity.***

Riesgo y Vulnerabilidad Cibernética en los Gobiernos Locales de Costa Rica: Un Estudio de Casos

Fabiana Quirós Pérez [1]; Javier Rojas-Segura[2]; José Martinez-Villavicencio[3]
[1, 2, 3] Tecnológico de Costa Rica, Costa Rica, *fabianaquirosp@estudiantec.cr, jarojas@tec.ac.cr, jomartinez@tec.ac.cr*

Resumen*– En la actualidad, la ciberseguridad se ha convertido en una preocupación primordial a nivel mundial debido a su relación directa con la protección de la información sensible. Sin embargo, en el contexto académico las investigaciones se han centrado en otros sectores, dejando de lado los gobiernos locales que también enfrentan grandes desafíos, y es precisamente este vacío de información lo que se busca atender. Este estudio se enfocó en identificar las principales vulnerabilidades a las que están expuestas cinco municipalidades seleccionadas de Costa Rica, así como el nivel de madurez con el que cuentan actualmente mediante la aplicación del Modelo de Madurez en Ciberseguridad. Para ello, se desarrolló la metodología de casos, donde se aplicó un cuestionario conformado por catorce dimensiones, lo que permitió obtener resultados sobre políticas, prácticas y recursos en materia de ciberseguridad de las municipalidades. Los resultados evidenciaron que el nivel de madurez en ciberseguridad de las municipalidades es bajo, particularmente en áreas como "Políticas de Ciberseguridad", "Seguridad en las Comunicaciones" y "Gestión de Incidentes de Ciberseguridad", lo cual expone a las municipalidades a riesgos cibernéticos importantes. Estos resultados no solo permiten visibilizar la realidad existente en la gestión pública digital, sino que también aportan al vacío académico en la materia.

***Palabras clave*—Ciberseguridad, gobiernos locales, riesgo cibernético, municipalidades, madurez.**

I. Introducción

Hoy en día, la ciberseguridad se ha convertido en una de las grandes preocupaciones de las organizaciones públicas y privadas [1], [2]. Sin embargo, las más afectadas son las instituciones públicas, incluidos los gobiernos locales, ya que se consideran objetivos atractivos para los ciberdelincuentes [3].

Si bien es fundamental desarrollar políticas y regulaciones que protejan su infraestructura tecnológica, los gobiernos locales en Costa Rica enfrentan muchos desafíos importantes, lo cual representa un riesgo significativo, ya que estas instituciones brindan servicios esenciales y manejan información sensible de los ciudadanos [4], [5]. De hecho, [6], [7] coinciden con lo anterior al indicar que los gobiernos locales son particularmente vulnerables frente a las ciberamenazas debido a factores como las restricciones presupuestarias, la escasez de recursos y la falta de competencias técnicas entre sus gestores.

No obstante, a pesar de estos valiosos aportes, la literatura académica aún es limitada en cuanto al caso específico de los gobiernos locales, ya que la mayoría de las investigaciones se enfocan en otras instituciones del sector público o en organizaciones del sector privado[8], [9].

Este estudio tiene como objetivo conocer el nivel de madurez en ciberseguridad de las municipalidades de Costa Rica y evaluar el nivel de riesgo cibernético al que están expuestas, mediante un análisis basado en la metodología de estudios de casos, utilizando un instrumento denominado "Modelo de Madurez en Ciberseguridad" (ECM^2) de [10], con el fin de concientizar sobre la cultura de ciberseguridad en estas organizaciones. Para orientar dicho objetivo, se plantea la siguiente pregunta: ¿Cuál es el nivel de madurez en ciberseguridad de las municipalidades de Costa Rica y cómo se relaciona con el nivel de riesgo cibernético al que están expuestas?, , ya que, esta pregunta guía a la comprensión de las deficiencias del sistema de ciberseguridad que impactan la seguridad de los servicios públicos locales.

II. Revisión de Literatura

Un municipio está constituido por el conjunto de personas vecinas residentes en un mismo cantón, que promueven y administran sus propios intereses [11]. En Costa Rica, actualmente existen 84 cantones, cada uno con su respectivo gobierno local o municipalidad.

A. Ciberseguridad y su Importancia en Gobiernos Locales

Ref. [12] define la ciberseguridad como la práctica de proteger sistemas críticos e información confidencial de ataques digitales, que involucran tecnología, personas y procesos. Es por ello por lo que se deben establecer una serie de técnicas tecnológicas y organizativas destinadas a garantizar la integridad, confidencialidad y accesibilidad de los datos, ya que, las incursiones cibernéticas pueden variar, como la extorsión a través del software de cifrado, robar información confidencial o interrumpir las actividades comerciales, lo que requiere una defensa digital robusta en todos los sectores [13]. La ciberseguridad es un tema crucial para los gobiernos locales, pues estos actúan como la principal interfaz entre los ciudadanos y los servicios públicos, gestionando infraestructuras vitales y datos sensibles [7]. En este contexto, la transformación digital se ha convertido en un tema relevante en la actualidad [14], imponiendo nuevos retos a los gobiernos locales, especialmente en la protección de la información de los ciudadanos y la integridad de los documentos administrativos, sin generar desconfianza en la población. Tal y como lo establece [15], cada vez son más los gobiernos que utilizan la gobernanza electrónica como una nueva forma de comunicación con los residentes, intercambio de información y accesibilidad con el objetivo de ofrecer mejores servicios electrónicos, mejorar la calidad de los servicios, aumentar la transparencia y reducir los costes, ya que los servicios públicos tradicionales de la sociedad actual no satisfacen las demandas de los ciudadanos; no obstante, estas autoras también advierten que, si bien es cierto la

adopción de tecnologías como el Internet de las Cosas (IoT), la inteligencia artificial (IA) y la gobernanza electrónica mejora la eficiencia de los servicios públicos, estos también conllevan nuevas amenazas en los entornos digitales. Esta situación subraya la necesidad urgente de que los municipios mantengan un equilibrio adecuado entre la innovación tecnológica y las medidas de seguridad, adoptando sistemas de protección más robustos frente a riesgos emergentes [16]. En esta misma línea, la Estrategia Nacional de Ciberseguridad destaca que la colaboración y el intercambio de información, conocimientos y recursos entre países y organizaciones internacionales ayudan a fortalecer la capacidad para prevenir, detectar y responder a incidentes cibernéticos y proteger a los usuarios en el entorno digital [12]. Además, desde una perspectiva económica, es incuestionable que los territorios competitivos y que funcionan bien ofrecen mejores condiciones para lograr otros resultados igualmente relevantes con importantes implicaciones sociales [17] así que evaluar la infraestructura digital y los riesgos cibernéticos de los municipios permite fortalecer su competitividad a nivel cantonal, vinculando directamente la seguridad informática con el desempeño territorial [17], [18]. Como consecuencia de lo anterior, es que los gobiernos locales están obligados a llevar a cabo una serie de actividades encaminadas a la detección de incidentes, el análisis de las causas de estos y la adopción de medidas correctoras [19].

B. Amenazas y Riesgos en Ciberseguridad

Durante los últimos años se ha observado una mayor sofisticación, precisión y coordinación en los ataques informáticos, representando una amenaza mucho más compleja para las autoridades locales [20]. Precisamente, son las organizaciones del sector público las que se enfrentan a mayores retos debido a la frecuencia de los ciberataques y a la probabilidad de que al menos algunos ataques tengan éxito y causen daños a los sistemas de información, no solo interrumpiendo los servicios públicos esenciales, sino también poniendo en peligro los datos y la privacidad de los ciudadanos [4], [21]. Esta tendencia junto con la vulnerabilidad inherente a las limitaciones presupuestarias y escasos recursos disponibles para las entidades gubernamentales locales los convierte en blancos atractivos para los atacantes [7]. De hecho, los ataques cibernéticos se encuentran entre los principales riesgos para los gobiernos locales, ya que, no solo afectan sistemas técnicos, sino que también tienen impactos sociales, organizacionales y económicos de alto impacto [22]. Ref. [23] menciona que en la última década, los incidentes cibernéticos se han vuelto más costosos y disruptivos, lo que incrementa aún más el riesgo para los gobiernos locales, ya que, no solo se enfrentan a la amenaza de la destrucción física de los sistemas en sí, sino a otra amenaza que puede llegar a ser inclusive más perjudicial que la anterior y es la pérdida de la confianza ciudadana en las instituciones gubernamentales, lo que puede debilitar la percepción de transparencia y eficacia del gobierno [24]. Para combatir estas amenazas de forma integral, es crucial la participación activa de todas las áreas funcionales, lo que requiere una mayor concientización holística en materia de ciberseguridad entre los equipos tácticos y operativos responsables de aplicar las medidas de seguridad [4].

C. Vulnerabilidad y Desafíos de los Gobiernos Locales

Los gobiernos locales se enfrentan a desafíos críticos en la era de la transformación digital, equilibrando la responsabilidad de salvaguardar la información de los residentes y los documentos administrativos, manteniendo al mismo tiempo la integridad de los datos y la confianza pública [16]. Ref. [25] indica que en América Latina, la falta de estándares de ciberseguridad ha favorecido un aumento de ciberataques que afectan tanto a servicios públicos como privados, ya que, cibercriminales de distintas partes del mundo han visto en los países de esta región, un blanco fácil para llevar a cabo sus actividades delictivas, aprovechando las vulnerabilidades de los gobiernos locales sin revelar su identidad. Además, diversos estudios identifican otros factores que aumentan el nivel de vulnerabilidad de los gobiernos locales en el ámbito digital. Por ejemplo, [7] menciona que una de las principales barreras a las que se enfrentan estos órganos es a la restricción presupuestaria, lo cual tiene un impacto muy significativo en su nivel de ciberseguridad que a su vez conlleva a otras limitantes como la baja conciencia en ciberseguridad, la falta de normativas, software obsoletos y brechas en infraestructuras críticas. Asimismo, [6], [8] señalan en sus investigaciones que otro de los problemas principales es que los gestores municipales no poseen los conocimientos ni las habilidades técnicas necesarias para gestionar un intercambio de datos seguro y eficaz, lo que lamentablemente los expone a riesgos cibernéticos, por lo que la formación continua de los funcionarios públicos en temas de ciberseguridad se presenta como un aspecto clave para reducir la brecha de conocimiento y mejorar la capacidad de respuesta ante incidentes. Ref. [8] mencionan en su investigación que aumentar el nivel de ciberseguridad de los municipios requiere no sólo más recursos financieros, sino también empleados más competentes, así como mejores equipos y programas informáticos.

D. Factores Tecnológicos y su Impacto

Los avances tecnológicos como el IoT y la IA pueden mejorar los servicios municipales, pero también exponen a los gobiernos locales a mayores amenazas cibernéticas [16]. Es bajo esta perspectiva, que la IA es una tecnología clave para proteger redes contra ciberataques, *malware* y accesos ilícitos, ya que puede fortalecer la ciberseguridad en gobiernos locales mediante *e-Governance* y la detección temprana de amenazas [26].

E. Gobernanza y Estrategias para la Ciberseguridad

Para abordar los desafíos evidenciados, es esencial la participación de todas las áreas funcionales mediante una

mayor concientización en ciberseguridad, así como trabajar en el fortalecimiento de un equipo especializado, la coordinación de equipos internos y externos, y la adaptación a la externalización de servicios de ciberseguridad [4]. Otra estrategia de suma importancia es contar con un marco legal unificado para garantizar interoperabilidad y un nivel de protección común en un entorno globalizado [27]. Cabe señalar que, en el caso costarricense, la autonomía política, administrativa y fiscal de los municipios, consolidada a partir de reformas legislativas de 1998, otorga a los gobiernos locales un papel central en la gestión de sus propias políticas y recursos [17]. Esta independencia, aunque fortalece la capacidad de autogobierno, también plantea el reto de que cada municipalidad defina y ejecute sus propias estrategias de ciberseguridad, generando disparidades en los niveles de preparación y protección entre cantones.

F. Tendencias y Futuro de la Ciberseguridad en Gobiernos Locales

Finalmente, si se habla de tendencias futuras en este ámbito, es fundamental señalar que cada vez más gobiernos están adoptando el *e-Governance* para mejorar la comunicación con los ciudadanos, aumentar la transparencia y reducir costos [15]. En este contexto, los datos se han convertido en un componente crítico, afectando no solo gobiernos, sino también negocios y ciudadanos [28]. Sumando el creciente protagonismo de tecnologías emergentes como la IA que tiene el potencial de fortalecer las capacidades de ciberseguridad de los Estados, los gobiernos locales y las entidades no estatales en el marco de la gobernanza electrónica [26]. Los gobiernos locales enfrentan el desafío de garantizar la seguridad de servicios públicos esenciales como el suministro de agua, salud, protección a la niñez y educación, desde infraestructuras tecnológicas comunes, que a menudo presentan limitaciones técnicas y organizativas en materia de ciberseguridad [29]. Estos retos reflejan la urgente necesidad de fortalecer las capacidades institucionales de los gobiernos locales ante un entorno digital cada vez más complejo y dinámico.

III. METODOLOGÍA

A. Enfoque de la Investigación

La presente investigación adoptó un enfoque mixto, ya que combina el análisis cuantitativo y también de percepciones u opiniones de los funcionarios. Este enfoque se sustenta en el hecho de que una gran cantidad de estudios de caso son mixtos, ya que recolectan, analizan e integran datos cuantitativos y cualitativos provenientes de diversas fuentes [30]. Esta combinación de enfoques permitió una visión más completa del estado de situación de las municipalidades en cuanto a seguridad informática, equilibrando la objetividad de los datos con el valor de las experiencias y percepciones de quienes trabajan en este ámbito.

B. Instrumento de Investigación

Desde la perspectiva cuantitativa, al igual que [31] se utilizó el instrumento ECM² de [10], que mediante una escala Likert de cinco puntos (ver Figura 1) midió el nivel de madurez en ciberseguridad de cada gobierno local permitiendo identificar las políticas, prácticas y recursos implementados en cada entidad, así como hacer comparaciones entre ellas. Para evaluar cada una de las secciones del instrumento, [10] utilizó cinco niveles que van de 0 a 4, según se detallan a continuación:

1) El nivel 0 corresponde al nivel de madurez más bajo y se utiliza cuando la evidencia sobre el control, la política o el proceso es inexistente. Esto indica que la empresa u organización es altamente vulnerable, lo cual representa un factor de riesgo muy alto en las secciones con este nivel de madurez.

2) En el nivel 1 hay evidencia de que se están creando los controles, políticas o procesos necesarios, pero aún no han sido completados. En este nivel la organización sigue siendo vulnerable y el factor de riesgo en las secciones con este nivel de madurez es alto.

3) El nivel 2 indica que la empresa cuenta con los controles, políticas y/o procesos requeridos. Sin embargo, no hay evidencia de que estos se estén aplicando correctamente, por lo tanto, hasta que estos controles no se apliquen eficientemente, la organización sigue siendo vulnerable y el factor de riesgo en las secciones con este nivel de madurez es medio.

4) En el nivel 3 la empresa no solo cuenta con los controles, políticas y/o procesos requeridos, sino que también existe evidencia de su correcta y continua implementación. Es decir, la implementación eficiente de los controles ayuda a reducir los factores de riesgo a los que está expuesta la organización, por lo que el factor de riesgo en las secciones con este nivel de madurez es bajo.

5) Finalmente, el nivel 4 indica que los esfuerzos realizados por la organización para crear, implementar y actualizar los controles, procesos y políticas son reconocidos y/o aceptados por otras empresas (o industria) como buenas prácticas en ciberseguridad. Este es el máximo nivel en el modelo y el factor de riesgo asociado es muy bajo.

Fig. 1 Escala de Niveles de Riesgo.
Tomado de [10]

Por otro lado, el enfoque cualitativo se evidenció mediante la recopilación y análisis de opiniones y perspectivas de la unidad informante, que en este estudio corresponde a los encargados de tecnologías de información (TI) de cada una de las municipalidades participantes. Para ser considerados como unidad informante, los participantes debían contar con conocimiento sobre los sistemas, políticas y prácticas de ciberseguridad de la municipalidad, así como tener responsabilidades relacionadas con la gestión o supervisión de los recursos tecnológicos. Este componente es clave para entender no solo cuáles medidas de ciberseguridad están en marcha, sino también cómo se vive y se percibe la ciberseguridad dentro de cada municipalidad, así como los principales desafíos y oportunidades a los que se enfrentan.

Para guiar la recolección de datos cualitativos, se elaboró una guía de preguntas abiertas que fue aplicada a los encargados de TI al final de la encuesta. Esta guía permitió abordar temas sobre el contexto cantonal, el uso de canales digitales, experiencias con ciberataques, la importancia percibida de la ciberseguridad y los principales retos enfrentados. La entrevista semiestructurada brindó la flexibilidad necesaria para profundizar en temas relevantes que surgieron durante la conversación, lo cual es característico de este tipo de estudios. De acuerdo con [30], en los estudios cualitativos de caso no se utilizan herramientas estandarizadas ni se establecen categorías *a priori*, ya que el objetivo principal es documentar una experiencia o evento en profundidad, entendiendo el fenómeno desde la perspectiva de quienes lo vivieron, sin buscar generalizaciones. Esto coincide con el enfoque adoptado en esta etapa de la investigación, donde se priorizó la comprensión del fenómeno desde su realidad específica. En cuanto al procesamiento de la información, las entrevistas fueron grabadas y posteriormente transcritas para facilitar su análisis. A partir de las respuestas escritas en la guía de preguntas abiertas y las transcripciones, se realizó un análisis cualitativo mediante la identificación de temas recurrentes y aspectos relevantes, seleccionados según el criterio y evaluación del equipo investigador. Las respuestas se organizaron y tabularon con el fin de estructurar y resumir los hallazgos, facilitando la integración de las opiniones recopiladas con el análisis general del estudio. La combinación de ambos enfoques permitió identificar patrones comunes y diferencias significativas entre las prácticas de ciberseguridad de los gobiernos locales estudiados, además de evaluar su preparación frente a posibles ciberataques.

C. *Diseño de la Investigación*

Se utilizó el diseño de casos múltiples, en los que, según lo articulado por [30], el marco procesal utilizado para cada caso individual se replica sistemáticamente en los demás, lo que hace que las revisiones de los casos sean análogos debido al empleo de un instrumento uniforme para la adquisición de datos y un proceso global coherente. Ref. [32] postuló que estos diseños muestran una mayor robustez y poseen una validez superior. En el contexto de múltiples estudios de casos, además del esfuerzo por descubrir patrones, se examina el nivel individual, ya que el análisis tiende a dilucidar tanto las consistencias como las discrepancias entre los casos [30].

D. *Sujeto de Estudio*

Se seleccionaron cinco municipalidades que expresaron su disposición a participar de manera voluntaria en el estudio: Acosta, Atenas, Dota, San Mateo y Tilarán. La elección de estos sujetos de estudio se basó en su compromiso y en su infraestructura cibernética para el análisis propuesto.

E. *Justificación de la Unidad de Muestra*

La selección de cinco unidades como objeto del estudio de caso se basó en múltiples consideraciones. Ref. [33] enfatizó que los estudios de casos poseen la capacidad de investigar a fondo el contexto y los elementos asociados con los acontecimientos y comportamientos humanos dentro de su entorno auténtico, esto permite la agregación de datos de diversas fuentes, lo que promueve un análisis exhaustivo y fundamentado.

Ref. [34] investigó en cinco grandes empresas del mercado venezolano, por su parte [31] investigó en cinco empresas de diversos tamaños y sectores en Costa Rica.

Ref. [30] señaló que, si bien un mayor número de casos puede mejorar la comprensión del tema abordado, la cantidad de casos debe estar en consonancia con los recursos financieros y las limitaciones de tiempo de que dispone el investigador. En este sentido, cinco gobiernos locales representaron un equilibrio factible entre profundidad y practicidad, lo que facilita un examen exhaustivo sin comprometer la integridad del estudio dada la cantidad de recursos.

IV. Resultados

Previo a presentar los resultados obtenidos, es importante enfocar el presente estudio en el grupo específico de gobiernos locales que participaron. A continuación, en la Tabla 1 se presenta una breve caracterización de cada una de ellas que incluye información importante sobre la población, presupuesto, índice de desarrollo humano cantonal (IDH-C) e índice de competitividad cantonal (ICC). Estos datos brindan una visión integral de la realidad específica de cada gobierno local, lo cual es esencial para contextualizar los resultados obtenidos en el análisis de las políticas y prácticas de ciberseguridad que se investigan.

TABLA I
DATOS CONTEXTUALES DE LOS GOBIERNOS LOCALES PARTICIPANTES

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 [35], [36], [37], [38]

Los resultados revelan diferencias en la madurez de las medidas de ciberseguridad entre las municipalidades participantes. En la dimensión de políticas de ciberseguridad, se observó que el 60% de ellas tienen políticas de ciberseguridad definidas, pero con un promedio de 0,8 queda en evidencia que la actualización de estas políticas es limitada, colocando este criterio en un nivel de riesgo alto. La difusión de estas políticas muestra un resultado más positivo, ya que, con un promedio de 2 y un 60% de las municipalidades que han logrado difundir sus políticas como mínimo de manera generalizada, se sitúa este criterio en un nivel de riesgo medio. La Figura 2 presenta el promedio de algunos criterios evaluados en las cinco municipalidades, permitiendo una visualización clara del nivel de madurez.

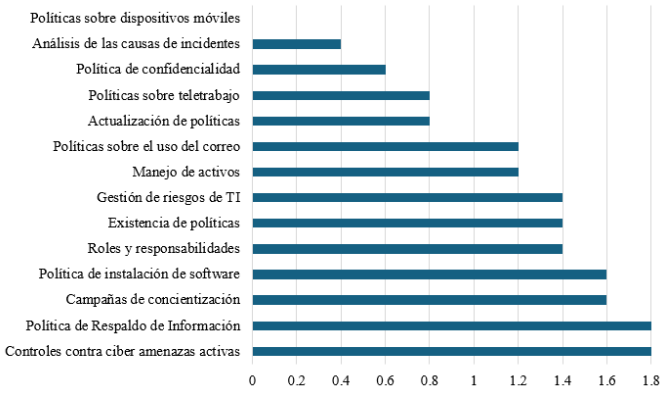

Fig. 2 Promedio de Madurez en Ciberseguridad.

En cuanto a la organización interna, solo el 60% de estas instituciones tienen roles y responsabilidades definidos para la gestión de la ciberseguridad, reflejando un promedio de 1,4 lo que indica un nivel de riesgo alto. En el rubro de políticas sobre dispositivos móviles presentan un promedio de 0 lo que refleja que las municipalidades en estudio no tienen políticas claras en esta área, lo que implica un nivel de riesgo muy alto. Además, solo el 20% de las municipalidades cuentan con una política definida sobre el teletrabajo. El 80% restante indicó que esta política está incompleta, en proceso o que no existe, lo que ubica este criterio en un nivel alto de riesgo.

Respecto al recurso humano, el promedio de 1,6 de las campañas de concientización en ciberseguridad indica que el solo el 60% de estas instituciones cuentan con un programa dedicado a campañas de sensibilización, lo que coloca este criterio en un nivel de riesgo medio. En el manejo de activos, el promedio de 1,2 refleja que solo el 20% de las instituciones tiene políticas de almacenamiento seguro de datos definidas, lo que sugiere que este es otro aspecto con un nivel de riesgo alto.

Con relación a la ciberseguridad en las operaciones de la empresa, se destaca que el promedio de 1,4 en la gestión de riesgos en TI indica que el 40% de las instituciones cuentan con un proceso documentado para este criterio, mientras que existe evidencia de la implementación y actualización continua de los controles contra ciber amenazas activas solo en el 40% de las instituciones, alcanzando un promedio de 1,8 lo que coloca este criterio en un nivel de riesgo medio. El promedio de 1,8 también refleja que el 60% de las instituciones tienen una política de respaldo de información incompleta o en proceso, lo que refleja un nivel de riesgo medio en este aspecto.

En el área de seguridad en las comunicaciones, el 40% de las instituciones no cuentan con una política de confidencialidad y no divulgación, lo que refleja un promedio de 0,6 y un nivel de riesgo alto. Además, aunque el 40% de las instituciones han establecido políticas sobre el uso del correo y los sistemas de mensajería, el promedio obtenido de 1,2 las coloca en un nivel de riesgo alto.

Por último, en la gestión de incidentes de ciberseguridad, un 40% de las instituciones tienen políticas y controles para el manejo de incidentes, con un promedio de 1,2 lo que las coloca en un nivel de riesgo alto. No obstante, el promedio de 0,4 en el análisis de las causas de los incidentes refleja que solo el 20% de las instituciones lo realizan, lo que coloca este aspecto en un nivel de riesgo muy alto. Finalmente, el promedio en el proceso de mejora continua en ciberseguridad muestra que un 40% de las instituciones no cuenta con este proceso, lo que coloca este aspecto también en un nivel de riesgo alto.

Además de los datos cuantitativos antes presentados, también se recopilaron opiniones y percepciones de las personas encargadas de los departamentos de TI de las municipalidades participantes, con el fin de obtener una visión más cercana y real sobre cómo se vive la ciberseguridad y el uso de tecnología en los gobiernos locales. A continuación, se comparten los principales hallazgos cualitativos que reflejan estas opiniones y percepciones. En cuanto al uso de canales digitales como medio de comunicación con la ciudadanía, la totalidad de las personas entrevistadas manifestó una percepción positiva. Todos coinciden en que estas herramientas son prácticas, accesibles y que han contribuido a mejorar la transparencia en la relación con los usuarios. Sin embargo, también se mencionó que su aprovechamiento podría ser mucho mayor si se invirtiera más en tecnología. Una de las frases que resume este sentir fue: "*Reconozco que nos falta mucho camino por avanzar*".

Al preguntarles si sus organizaciones han enfrentado algún incidente relacionado con ciberataques, todas las respuestas apuntaron a que no han tenido experiencias graves. Solo una persona mencionó haber detectado un intento, aunque sin consecuencias. Aun así, hay claridad sobre el riesgo que representan estas amenazas, como lo expresó uno de los encargados de TI durante la entrevista: "*El hecho de que no haya pasado no quiere decir que no pueda pasar*".

Sobre la importancia de la ciberseguridad en los gobiernos locales, hubo un consenso total: se considera un tema clave. Se mencionó la necesidad de proteger los datos sensibles, evitar fraudes y fortalecer la confianza de la ciudadanía. También se señaló que una brecha de seguridad podría afectar directamente la imagen institucional.

Finalmente, en lo referente a los desafíos, las respuestas giraron principalmente en torno a tres temas: falta de presupuesto, poca capacitación del personal y escaso apoyo hacia el área de tecnología. También se hizo referencia a la resistencia al cambio y a la necesidad de contar con lineamientos más sólidos. Algunas frases que reflejan estas dificultades son: "*Si no me dicen (sobre documentar información), no lo hago*", "*Por el cambio de administración, muchas políticas y normativas se dejan botadas porque cada alcalde va por su lado*", y "*Mientras los jerarcas sigan con una visión tan tradicional, va a ser muy difícil generar un cambio real*".

V. Discusión

El análisis de la ciberseguridad en las municipalidades de Costa Rica que se realizó mediante la aplicación del instrumento ECM², permitió identificar el nivel de preparación que tienen las municipalidades participantes para enfrentar los riesgos digitales. Con este estudio no solo se buscó conocer el estado actual de estas organizaciones en materia de seguridad cibernética, sino también evaluar el nivel de riesgo ante posibles amenazas, con la intención de generar insumos que impulsen una cultura de ciberseguridad más sólida y proactiva en los gobiernos locales.

Para iniciar, es importante comprender que tal y como lo establecen [39] la digitalización ha dado lugar al uso exponencial de tecnologías de la información y la comunicación, lo que ha generado un aumento en el riesgo de ciberataques que amenazan la cadena de suministros global, donde los más afectados son las pequeñas y medianas empresas (PYMEs) y su ecosistema, por la escasez de recursos para proteger la integridad, confidencialidad y disponibilidad de sus activos de información. Bajo esta línea, se podría decir que las municipalidades comparten algunos de estos retos con las PYMEs y el principal es la escasez de recursos económicos. Vale la pena destacar que, en algunas de las percepciones y opiniones de los encargados de TI de las municipalidades participantes, la totalidad de los encuestados hicieron referencia a la falta de presupuesto como uno de los mayores obstáculos, lo cual genera gran preocupación debido a que la seguridad de la información ciudadana debe ser una prioridad tanto para el Gobierno de Costa Rica como para las municipalidades en sí. Contrario a esto, [39] también exponen el caso del Gobierno de Japón, mismo que sirve como ejemplo para tomar acciones y mejorar en este campo. Este Gobierno promueve la transformación digital con ciberseguridad, para lo cual ha construido comunidades locales basadas en el concepto de ayuda mutua entre el gobierno, la empresa y la academia, no solo a través de asesorías con expertos, también ha integrado recursos humanos a las empresas, ha fomentado las competencias y desarrollado soluciones de seguridad regional. Además de brindar subsidios a las PYMEs para contrarrestar su falta de recursos, con esto busca fortalecer la ciberseguridad de toda la cadena de suministros, hasta sus eslabones más débiles que son los que más expuestos están a los ciberataques. También es importante destacar que otra de las grandes problemáticas que enfrentan las municipalidades es la escasez de personal capacitado, y ocasionalmente, personal poco comprometido con mantener altos niveles de seguridad digital. Lo anterior guarda relación con lo expresado por [40], donde se destaca que es un reto conseguir que el colaborador esté plenamente identificado con acciones para la protección de los datos de la organización. Además, esto también coincide con lo dicho por uno de los encargados de TI, quién expresó "*Si no me dicen (sobre documentar información), no lo hago*" lo que evidencia la falta de compromiso, proactividad e inclusive motivación de algunos colaboradores de los departamentos de TI al realizar los procedimientos necesarios para fortalecer sus sistemas. En otras ocasiones, la brecha entre la exposición, la percepción y la preparación de las PYMEs para mitigar el riesgo cibernético mencionada por [41] también toma protagonismo, ya que, aunque se reconoce la importancia que tiene la ciberseguridad en las organizaciones, es necesario seguir trabajando en las políticas y acciones preventivas que están incompletas o son totalmente inexistentes, tal como lo reconoce otro de los encargados de TI, al mencionar "*Reconozco que nos falta mucho camino por avanzar*". En este punto conviene señalar que la literatura ya ha identificado esta brecha en el sector privado, particularmente en las PYMEs, donde la falta de personal calificado en ciberseguridad agrava las limitaciones para mitigar riesgos [18]. Sin embargo, aún existe un vacío de investigación en el ámbito municipal, lo cual refuerza la relevancia de este estudio al aportar evidencia en un contexto poco explorado. Ref. [17] advierte que para evaluar con precisión las condiciones de los cantones desde múltiples ángulos, incluyendo sus infraestructuras digitales, resulta esencial generar métricas de apoyo que orienten la formulación de políticas públicas más efectivas. En este sentido, los hallazgos aquí expuestos ofrecen un insumo inicial que puede servir de base para la toma de decisiones y la definición de estrategias de ciberseguridad en los gobiernos locales costarricenses.

Asimismo, dentro de los comentarios expresados por los encargados de TI de las municipalidades, se percibió un sentimiento de abandono institucional hacia el área de tecnología. Frases como: "*Por el cambio de administración, muchas políticas y normativas se dejan botadas porque cada alcalde va por su lado*" y "*Mientras los jerarcas sigan con una visión tan tradicional, va a ser muy difícil generar un cambio real*", reflejan no solo la falta de visión a largo plazo, sino también la fragilidad con la que se gestionan los temas de ciberseguridad en el ámbito municipal. Esto resalta la importancia de contar con lineamientos y políticas públicas en

materia de ciberseguridad que trasciendan el ciclo político de los gobiernos locales y que permanezcan estables sin importar el líder en turno. En este sentido la Estrategia Nacional de Ciberseguridad 2023-2027 del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de nuestro país (MICITT) resalta la importancia de replantear la posición del Estado costarricense frente a la ciberseguridad en todos los niveles institucionales. De hecho, [12] indica que fue precisamente a raíz de los ciberataques masivos sufridos por diferentes instituciones públicas en 2022, donde incluso se declaró estado de emergencia nacional, que se estableció este marco de acción integral que incluye la armonización del marco legal y regulatorio, la creación de convenios interinstitucionales y el fortalecimiento de la gobernanza digital. Según lo establecido en la Estrategia Nacional de Ciberseguridad 2023, su objetivo no es solo prevenir y mitigar los riesgos y amenazas en el entorno digital, sino también fomentar una cultura de seguridad sólida, fortalecer la capacidad de respuesta ante incidentes y promover la resiliencia institucional, con el fin de garantizar la estabilidad del país y la confianza en el uso de los sistemas digitales [12]. Para los gobiernos locales, esto implica reconocer que la ciberseguridad no debe depender únicamente de la voluntad del jerarca de turno o de los recursos, sino ser impulsada a partir de una política pública clara, articulada y sostenible en el tiempo, que garantice recursos, seguimiento y acciones coordinadas desde el nivel nacional hasta el municipal.

Este estudio evidenció que las dimensiones con mejores resultados fueron las de “Ciberseguridad en las operaciones de la empresa” y “Ciberseguridad y el recurso humano” (Figura 3). En la primera dimensión, destacan criterios como los controles contra ciber amenazas y ciber ataques, políticas de respaldo de información o integridad de la información obtuvieron puntuaciones altas respecto a las demás dimensiones, lo que está alineado con las recomendaciones brindadas por [42], donde se establece que usar contraseñas seguras, actualizar el software, pensar antes de hacer clic en enlaces sospechosos y activar la autenticación multifactor son los fundamentos de lo que llamamos "ciberhigiene" y que mejoran drásticamente la seguridad en línea. En cuanto a la ciberseguridad y el recurso humano, sobresale el criterio de las campañas de concientización en ciberseguridad con una de las puntuaciones más altas, lo cual indica que existe un programa dedicado a la concientización sobre ciberseguridad dentro de la municipalidad. Esta situación es congruente con lo mencionado por [43], donde se explica que una vez aplicado el taller Cyberkids cuyo propósito fue la concientización de un grupo de niños y adolescentes con edades comprendidas entre 10 y 15 años, en relación con los riesgos y desafíos que conlleva el uso del ciberespacio, se reveló como una iniciativa educativa valiosa y efectiva para empoderar a la niñez y juventud digital, ofreciendo herramientas necesarias para navegar de manera segura y responsable en el entorno virtual, lo cual reafirma el impacto que tiene la concientización en los esfuerzos de la ciberseguridad.

Por otra parte, algunos de los criterios con puntuaciones más bajas corresponden a la dimensión de “Gestión de incidentes de ciberseguridad” (ver Fig. 3), donde criterios como el de políticas y controles para el manejo de incidentes de ciberseguridad, el análisis de las causas de estos incidentes y el proceso de mejora continua en ciberseguridad reflejan un alto nivel de riesgo en las municipalidades participantes, lo cual genera bastante preocupación debido a que esto refleja una frágil capacidad de respuesta ante estos incidentes que no solo ponen en riesgo los servicios básicos que ofrecen estas organizaciones, sino también la información sensible de los ciudadanos.

Fig. 3 Radar de Ciberseguridad Municipal

Además, llama la atención que la Municipalidad de Atenas fue la que obtuvo una mayor puntuación, alcanzando en muchos de los criterios evaluados puntuaciones altas. Esto resulta particularmente interesante ya que, si se toma en cuenta el IDH-C y el ICC de cada una de las municipalidades participantes, se observa que precisamente es Atenas quien cuenta con los mayores índices de todas las municipalidades evaluadas en este estudio (ver Figura 4). Contrario a esto, San Mateo cuenta con uno de los ICC más bajos del estudio; de igual manera, es una de las municipalidades con puntuación más baja en el instrumento aplicado. Lo anterior podría sugerir una relación entre estos índices [17], abriendo la posibilidad de estudiar con mayor profundidad la relación entre ambos aspectos en investigaciones futuras.

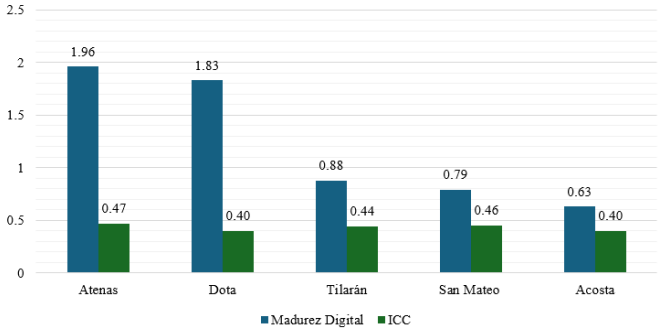

Fig. 4 Comparación entre Índice de Competitividad Cantonal e Índice de Madurez en Ciberseguridad de cada gobierno local

Como toda investigación, este estudio presentó ciertas limitantes que se deben tener presentes a la hora de interpretar la información. Las principales giraron en torno a los sujetos de estudio, ya que solamente se contó con la participación de cinco municipalidades, que además eran pequeñas, esto debido a que la elección de las municipalidades obedeció a la disponibilidad e interés que estas mostraron para formar parte del estudio. Además, algunas de las personas encargadas de los departamentos de TI no se consideraban expertas en el tema, lo cual pudo influir en el momento de contestar la encuesta. Sin embargo, aun tomando en consideración estas limitaciones, los hallazgos encontrados representan un acercamiento relevante al estado de la ciberseguridad en el contexto municipal costarricense.

VI. Conclusiones

En este capítulo se detallan las principales conclusiones a raíz del análisis realizado, con el fin de conocer el nivel de ciberseguridad de las municipalidades de Costa Rica y evaluar el nivel de riesgo cibernético al que están expuestas. Este estudio refleja que existe bajo nivel de madurez en ciberseguridad de las municipalidades, lo cual las expone a niveles de riesgo altos ante posibles ataques cibernéticos que podrían incluir pérdida de información sensible, interrupción en los servicios que brindan y pérdida de confianza por parte de los ciudadanos. La existencia de políticas que guíen el comportamiento de la organización ante los riesgos cibernéticos está rezagada, lo cual supone un gran reto ya que esto limita su capacidad de prevenir y gestionar posibles amenazas de una forma ordenada y efectiva. La seguridad de las comunicaciones y la gestión de incidentes de ciberseguridad también son de las áreas más críticas lo cual podría traducirse en fraudes, robo de información, alteración de bases de datos, etc. Ante estos resultados, es oportuno recalcar que el rol del Estado es crucial para reducir las brechas en ciberseguridad, a través de incentivos para alianzas, desarrollo de competencias, subsidios o la promoción de la investigación aplicada [39.]

Una de las principales implicaciones prácticas que deja este estudio es la importancia de la concientización tanto en las personas encargadas de los departamentos de TI como en sus superiores. Durante el proceso de entrevistas y como se expuso antes, se evidenció que en algunas ocasiones las acciones relacionadas con la ciberseguridad no se ejecutan si no hay una instrucción directa o un interés claro por parte de los mandos superiores. En algunos casos, incluso, se percibió cierta indiferencia desde la alcaldía, lo que podría generar en los encargados una actitud del tipo: "*si a mis superiores no les importa, ¿por qué debería importarme a mí?*". Esto refleja que, más allá de contar con recursos o herramientas, es fundamental que exista un compromiso real desde los niveles más altos de la organización para motivar al personal técnico y fortalecer una cultura de ciberseguridad dentro de las municipalidades.

Podría ser de mucha utilidad que en investigaciones futuras se utilice una metodología distinta al estudio de casos que permita contar con la participación de más municipalidades para que los resultados obtenidos sean representativos. Sin embargo, la metodología de estudio de casos puede aportar información muy interesante si se enfoca en otro grupo de municipalidades, por ejemplo, resultaría muy valioso analizar el nivel de ciberseguridad de las cinco municipalidades que cuentan con el mayor presupuesto a nivel país, o de forma más precisa, aquellas con mayor presupuesto por habitante, lo que permitiría explorar si existe alguna relación entre los recursos disponibles y el nivel de madurez en ciberseguridad. De la misma forma, se considera interesante contrastar el nivel de madurez en ciberseguridad con indicadores como el IDH-C o ICC para identificar si existe alguna correlación entre el desarrollo socioeconómico del cantón y las capacidades institucionales en materia de ciberseguridad. Además, futuras líneas de investigación podrían centrarse en analizar la relación entre el nivel de madurez en ciberseguridad y la frecuencia o naturaleza de los incidentes cibernéticos reportados en las municipalidades, lo que permitiría obtener información más alineada con la gestión de riesgos. Asimismo, resultaría muy valioso realizar un estudio de casos en gobiernos locales de otro país, con el objetivo de comparar los resultados obtenidos en el contexto costarricense con los de otras realidades regionales o incluso globales.

Finalmente, este estudio no solo permitió conocer el estado actual de la ciberseguridad en los gobiernos locales costarricenses e identificar áreas críticas a las que se les debe prestar especial atención para salvaguardar la información de los ciudadanos, sino también aportar al vacío de conocimiento existente en cuanto a la ciberseguridad en gobiernos locales, un tema que no ha sido tan investigado. Además, los hallazgos permiten brindar información valiosa a las municipalidades para sus procesos de mejora.

Referencias

[1] S. M. T. Toapanta, R. H. D. P. Durango, L. E. M. Gallegos, Ma. R. M. Arellano, J. A. O. Trejo, y M. M. B. Hifong, "Suitable Professional Identity Analysis to Improve Information Security Governance", en 2022 International Conference on Computer, Information and Telecommunication Systems (CITS), jul. 2022, pp. 1–4. doi: 10.1109/CITS55221.2022.9832999.

[2] R. A. Hallman, M. Major, J. Romero-Mariona, R. Phipps, E. Romero, y J. M. S. Miguel, "Return on Cybersecurity Investment in Operational Technology Systems: Quantifying the Value That Cybersecurity Technologies Provide after Integration", presentado en 5th International Conference on Complexity, Future Information Systems and Risk, 2020, pp. 43–52. Consultado: el 9 de julio de 2025. [En línea]. Disponible en: https://www.scitepress.org/Link.aspx?doi=10.5220/0009416200430052

[3] D. Fujs y I. Bernik, "Analyzing Cybersecurity Strategies of the European Union, Challenges and Opportunities for Public Administration", Elektrotehniski Vestn., vol. 91, núm. 1/2, pp. 8–20, 2024.

[4] 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, núm. 11, Art. núm. 11, nov. 2023, doi: 10.3390/info14110586.

[5] I. Skierka, "When shutdown is no option: Identifying the notion of the digital government continuity paradox in Estonia's eID crisis", Gov. Inf. Q., vol. 40, núm. 1, p. 101781, ene. 2023, doi: 10.1016/j.giq.2022.101781.
[6] M. Caldarulo, J. Olsen, y M. K. Feeney, "Oversharing: The downside of data sharing in local government", Public Adm., vol. 102, núm. 4, pp. 1647–1664, 2024, doi: 10.1111/padm.12993.
[7] S. T. Hossain, T. Yigitcanlar, K. Nguyen, y Y. Xu, "Understanding Local Government Cybersecurity Policy: A Concept Map and Framework", Information, vol. 15, núm. 6, Art. núm. 6, jun. 2024, doi: 10.3390/info15060342.
[8] A. Chodakowska, S. Kańduła, y J. Przybylska, "Cybersecurity in the Local Government Sector in Poland: More Work Needs to be Done: More work needs to be done", Lex Localis - J. Local Self-Gov., vol. 20, núm. 1, Art. núm. 1, ene. 2022, doi: 10.4335/20.1.161-192(2022).
[9] S. Ganapati, M. Ahn, y C. Reddick, "Evolution of Cybersecurity Concerns: A Systematic Literature Review", en Proceedings of the 24th Annual International Conference on Digital Government Research, en dg.o '23. New York, NY, USA: Association for Computing Machinery, jul. 2023, pp. 90–97. doi: 10.1145/3598469.3598478.
[10] C. Rodriguez Bravo, "Modelo Madurez Ciberseguridad (ECM2)". 2017. [En línea]. Disponible en: https://es.scribd.com/document/525745224/Modelo-Madurez-Ciberseguridad-Cesar-Rodriguez
[11] Código Municipal. 2008. Consultado: el 9 de julio de 2025. [En línea]. Disponible en: https://pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=64464&nValor3=0
[12] 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
[13] WEF, "Global Cybersecurity Outlook 2022", 2022. Consultado: el 4 de agosto de 2022. [En línea]. Disponible en: https://www.weforum.org/reports/global-cybersecurity-outlook-2022/
[14] J. Rojas-Segura, J. Martinez-Villavicencio, y M. Faith-Vargas, "Digital Transformation and Business Model in SMEs: a Bibliometric Analysis", en Proceedings of the LACCEI international Multi-conference for Engineering, Education and Technology, Costa Rica: Latin American and Caribbean Consortium of Engineering Institutions, 2024. doi: 10.18687/LEIRD2024.1.1.280.
[15] D. Rudyte y M. Kontrimaite, "New Public Management at Local Self-Government Institutions", en Eurasian Economic Perspectives, M. H. Bilgin, H. Danis, G. Karabulut, y G. Gözgor, Eds., Cham: Springer International Publishing, 2020, pp. 169–180. doi: 10.1007/978-3-030-40375-1_12.
[16] S. T. Hossain, T. Yigitcanlar, K. Nguyen, y Y. Xu, "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework", Appl. Sci., vol. 14, núm. 13, Art. núm. 13, ene. 2024, doi: 10.3390/app14135501.
[17] E. Lafuente, M. Araya, y J. C. Leiva, "Assessment of local competitiveness: A composite indicator analysis of Costa Rican counties using the 'Benefit of the Doubt' model", *Socioecon. Plann. Sci*., vol. 81, p. 100864, jun. 2022, doi: 10.1016/j.seps.2020.100864.
[18] 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.
[19] M. Karpiuk, "The Local Government's Position in the Polish Cybersecurity System.", Lex Localis J. Local Self-Gov., vol. 19, núm. 3, 2021, doi: 10.4335/19.3.609-620(2021).
[20] G. Ahmadi-Assalemi, H. Al-Khateeb, G. Epiphaniou, y C. Maple, "Cyber Resilience and Incident Response in Smart Cities: A Systematic Literature Review", Smart Cities, vol. 3, núm. 3, Art. núm. 3, sep. 2020, doi: 10.3390/smartcities3030046.
[21] D. F. Norris, L. Mateczun, A. Joshi, y T. Finin, "Managing cybersecurity at the grassroots: Evidence from the first nationwide survey of local government cybersecurity", J. Urban Aff., vol. 43, núm. 8, pp. 1173–1195, sep. 2021, doi: 10.1080/07352166.2020.1727295.
[22] B. Preis y L. Susskind, "Municipal Cybersecurity: More Work Needs to be Done", Urban Aff. Rev., vol. 58, núm. 2, pp. 614–629, mar. 2022, doi: 10.1177/1078087420973760.
[23] M. Dunn Cavelty y A. Wenger, "Cyber security meets security politics: Complex technology, fragmented politics, and networked science", Contemp. Secur. Policy, vol. 41, núm. 1, pp. 5–32, ene. 2020, doi: 10.1080/13523260.2019.1678855.
[24] R. Shandler y M. A. Gomez, "The hidden threat of cyber-attacks – undermining public confidence in government", J. Inf. Technol. Polit., vol. 20, núm. 4, pp. 359–374, oct. 2023, doi: 10.1080/19331681.2022.2112796.
[25] 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, núm. 3, Art. núm. 3, sep. 2023, doi: 10.3390/informatics10030071.
[26] S. A. A. Bokhari y S. Myeong, "The Influence of Artificial Intelligence on E-Governance and Cybersecurity in Smart Cities: A Stakeholder's Perspective", IEEE Access, vol. 11, pp. 69783–69797, 2023, doi: 10.1109/ACCESS.2023.3293480.
[27] J. Sanchez-Zurdo y J. San-Martín, "A Country Risk Assessment from the Perspective of Cybersecurity in Local Entities", Appl. Sci., vol. 14, núm. 24, Art. núm. 24, ene. 2024, doi: 10.3390/app142412036.
[28] M. Agbali, A. A. Dahiru, G. D. Olufemi, I. A. Kashifu, y O. Vincent, "Data Privacy and Protection: The Role of Regulation and Implications for Data Controllers in Developing Countries", en Information and Communication Technologies for Development, J. M. Bass y P. J. Wall, Eds., Cham: Springer International Publishing, 2020, pp. 205–216. doi: 10.1007/978-3-030-65828-1_17.
[29] A. Vestad y B. Yang, "Municipal Cybersecurity—A Neglected Research Area? A Survey of Current Research", en Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, C. Onwubiko, P. Rosati, A. Rege, A. Erola, X. Bellekens, H. Hindy, y M. G. Jaatun, Eds., Singapore: Springer Nature, 2023, pp. 151–165. doi: 10.1007/978-981-19-6414-5_9.
[30] 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.
[31] T. Howell, J. Rojas-Segura, J. Martinez-Villavicencio, y C. Rodriguez-Bravo, "Cybersecurity Vulnerabilities in Companies: A Case Study.", en Proceedings of the LACCEI International Multi-conference for Engineering, Education and Technology, Latin American and Caribbean Consortium of Engineering 10.18687/LACCEI2025.1.1.1773.
[32] R. K. Yin, Case Study Research and Applications. Design and Methods, Sixth Edition. Thousand Oaks, CA: SAGE Publications, Inc., 2018. [En línea]. Disponible en: https://uk.sagepub.com/en-gb/eur/case-study-research-and-applications/book250150
[33] M. L. Saavedra García, "El estudio de caso como diseño de investigación en las Ciencias Administrativas", Iberoam. Bus. J. Rev. Estud. Int., vol. 1, núm. 1, pp. 72–97, 2017, doi: https://doi.org/10.22451/3002.ibj2017.vol1.1.11005.
[34] R. Puente y M. Cervilla, "Prácticas de la gerencia de relaciones con el cliente (CRM) en empresas venezolanas: un estudio de casos", Acad. Rev. Latinoam. Adm., Consultado: el 8 de febrero de 2025. [En línea]. Disponible en: https://www.academia.edu/95936680/Pr%C3%A1cticas_de_la_gerencia_de_relaciones_con_el_cliente_CRM_en_empresas_venezolanas_un_estudio_de_casos
[35] PNUD, "Atlas de Desarrollo Humano Cantonal en Costa Rica 2024-Análisis de Resultados". Programa de las Naciones Unidas para el Desarrollo (PNUD), 2024. Consultado: el 9 de julio de 2025. [En línea]. Disponible en: https://pnud-conocimiento.cr/repositorio/atlas-resultados-2024/
[36] Contraloria General de la Republica, "Antecedentes históricos - CGR | Costa Rica". Consultado: el 28 de junio de 2023. [En línea]. Disponible en: https://www.cgr.go.cr/01-cgr-transp/antecedentes-historicos.html
[37] INEC, Estimación de Población y Vivienda 2022. Resultados Generales, vol. 1. San Jose, Costa Rica: Instituto Nacional de Estadística y Censos, 2023. [En línea]. Disponible en: https://admin.inec.cr/sites/default/files/2023-

07/rePoblacResultadosGenerales_Estimacion_poblacion_vivienda_2022.pdf
[38] UCR, "Índice de Competitividad Cantonal | Costa Rica 2022 - 2023", Universidad de Costa Rica, San Jose, Costa Rica, 2025. Consultado: el 9 de julio de 2025. [En línea]. Disponible en: https://economia.ucr.ac.cr/accion-social/ICC
[39] O. Bustillos Ortega y J. Rojas Segura, "Cómo promueven los estados la ciberseguridad de las PYMEs", Interfases, vol. 17, núm. 1, pp. 168–186, 2023, doi: https://doi.org/10.26439/interfases2023.n017.6246.
[40] O. Bustillos Ortega y J. Rojas Segura, "Protocolo básico de ciberseguridad para pymes", Interfases, vol. 16, núm. 2, pp. 168–186, dic. 2022, doi: 10.26439/interfases2022.n016.6021.
[41] J. Rojas-Segura, M. Faith-Vargas, y J. Martinez-Villavicencio, "Conceptualizing digital transformation using semantic decomposition", TEC Empres., vol. 17, núm. 3, pp. 63–75, dic. 2023, doi: 10.18845/te.v17i3.6850.
[42] Cybersecurity & Infraestructure, Security Agency CISA, "Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA", America´s Cyber Defense Agency. Consultado: el 9 de julio de 2025. [En línea]. Disponible en: https://www.cisa.gov/topics/cybersecurity-best-practices
[43] 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, núm. 2, pp. 185–205, dic. 2023, doi: 10.26439/interfases2023.n018.6626.