

Artículo Científico

# Ciberseguridad en gobierno electrónico: percepción del sector público en El Empalme

## *Cybersecurity in e-government: public sector perception in El Empalme*



Espinoza-Saldaña, Néstor Javier <sup>1</sup>



<https://orcid.org/0009-0004-3872-2655>



[nespinozas@uteq.edu.ec](mailto:nespinozas@uteq.edu.ec)



Universidad Técnica Estatal de Quevedo, Ecuador, Quevedo.



Lara-Zambrano, William Oswaldo <sup>2</sup>



<https://orcid.org/0009-0003-2081-8125>



[wlaraz@uteq.edu.ec](mailto:wlaraz@uteq.edu.ec)



Universidad Técnica Estatal de Quevedo, Ecuador, Quevedo.



Ruiz-Jara, Johan Alexander <sup>3</sup>



<https://orcid.org/0009-0006-8429-5724>



[jruizi@uteq.edu.ec](mailto:jruizi@uteq.edu.ec)



Universidad Técnica Estatal de Quevedo, Ecuador, Quevedo.



Zamora-Mayorga, Darwin Javier <sup>4</sup>



<https://orcid.org/0000-0001-5118-2519>



[dzamora@uteq.edu.ec](mailto:dzamora@uteq.edu.ec)



Universidad Técnica Estatal de Quevedo, Ecuador, Quevedo.

Autor de correspondencia <sup>1</sup>



DOI / URL: <https://doi.org/10.55813/gaea/rcym/v3/n3/62>

**Resumen:** Este estudio examina la percepción institucional de la ciberseguridad en los sistemas de gobierno electrónico del GAD El Empalme durante el periodo 2025. Surge del contexto de un nivel de digitalización del sector público local en avance rápido a nivel municipal, donde continúan existiendo algunas deficiencias técnicas, organizativas y regulatorias para garantizar la seguridad de los servicios en línea. Esta investigación utiliza un enfoque de métodos mixtos, que incluye una encuesta a usuarios, así como entrevistas con funcionarios y ciudadanos, para determinar las brechas en infraestructura, capacitación y políticas de protección de datos. Los resultados revelan que solo una pequeña fracción del personal ha recibido capacitación básica en ciberseguridad, que existen sistemas obsoletos sin copias de seguridad regulares y que hay poca confianza entre los ciudadanos en los servicios digitales. Además, la financiación asignada a la seguridad digital es mínima y hay costos significativos causados por incidentes de ciberseguridad. El estudio, sugiere crear un modelo contextualizado de ciberseguridad que integre tecnología, formación continua y participación ciudadana para fortalecer la resiliencia institucional frente a amenazas digitales.

**Palabras clave:** ciberseguridad, gobierno electrónico, percepción institucional, infraestructura, capacitación.



Check for updates

**Received:** 10/Jul/2025  
**Accepted:** 28/Jul/2025  
**Published:** 06/Ago/2025

**Cita:** Espinoza-Saldaña, N. J., Lara-Zambrano, W. O., Ruiz-Jara, J. A., & Zamora-Mayorga, D. J. (2025). Ciberseguridad en gobierno electrónico: percepción del sector público en El Empalme. *Revista Científica Ciencia Y Método*, 3(3), 98-110. <https://doi.org/10.55813/gaea/rcym/v3/n3/62>

Revista Científica Ciencia y Método (RCyM)  
<https://revistacym.com>  
[revistacym@editorialgrupo-aea.com](mailto:revistacym@editorialgrupo-aea.com)  
[info@editorialgrupo-aea.com](mailto:info@editorialgrupo-aea.com)

© 2025. Este artículo es un documento de acceso abierto distribuido bajo los términos y condiciones de la **Licencia Creative Commons, Atribución-NoComercial 4.0 Internacional**.



**Abstract:**

This study examines the institutional perception of cybersecurity in the e-government systems of the GAD El Empalme during the period 2025. It arises from the context of a rapidly advancing level of digitization of the local public sector at the municipal level, where some technical, organizational, and regulatory deficiencies continue to exist in ensuring the security of online services. This research uses a mixed-methods approach, including a user survey and interviews with officials and citizens, to identify gaps in infrastructure, training, and data protection policies. The results reveal that only a small fraction of staff have received basic cybersecurity training, that there are outdated systems without regular backups, and that there is little trust among citizens in digital services. In addition, funding allocated to digital security is minimal, and there are significant costs caused by cybersecurity incidents. The study suggests creating a contextualized cybersecurity model that integrates technology, ongoing training, and citizen participation to strengthen institutional resilience to digital threats.

**Keywords:** cybersecurity, e-government, institutional perception, infrastructure, training.

## 1. Introducción

El gobierno electrónico en Ecuador inició a finales de los años 90 como parte del proceso de modernización estatal mediante el uso de tecnologías digitales. Con el crecimiento de estas plataformas, surgió la preocupación por proteger la información gubernamental y los datos ciudadanos, en temas de tecnología aplicada al sector gobierno son de gran relevancia. En los últimos años, los países han avanzado en temas de gobierno digital e inteligencia artificial (Ospina, 2023). Lo que hizo indispensable incorporar la ciberseguridad como un componente clave. En la época de la digitalización, las administraciones locales están esforzándose por enfrentar el reto de actualizar sus servicios a través de sistemas de administración electrónica, que aseguran mejorar la eficiencia, transparencia y accesibilidad a un nivel diferente.

En el GAD El Empalme, Ecuador, es donde existen precauciones críticas de ciberseguridad debido a la falta de infraestructura técnica y capacitación del personal. Según Abarca (2017) en todos los niveles o departamentos de trabajo requerían de capacitación para poder desarrollar su labor de forma eficiente. Este gobierno enfocó sus esfuerzos en implementar un sistema de gobierno electrónico, pero la carencia de protocolos de seguridad sobre riesgos cibernéticos mutados para el entorno crítico en el que los servidores públicos se hallan transforma a sus organizaciones en un objetivo sencillo de asaltos diseñados para poner en peligro información delicada y el funcionamiento interno de las entidades gubernamentales.

Este estudio se centra en analizar las percepciones del sector público del GAD El Empalme sobre la ciberseguridad en sus sistemas de gobierno electrónico, la implementación de sistemas promete optimizar la eficiencia, transparencia y accesibilidad a un nivel diferente. Según Tabarquino (2018) un Estado dinámico e inclusivo para la prestación del servicio público de internet y digitalización Ecuador, y en particular el GAD El Empalme, no es la excepción, donde existen precauciones críticas de ciberseguridad debido a la falta de infraestructura técnica y capacitación del personal.

Este GAD El Empalme enfocó sus esfuerzos en implementar un sistema de gobierno electrónico, pero la carencia de protocolos de seguridad sobre riesgos cibernéticos, el entorno crítico en el que los empleados del gobierno hacen que sus organizaciones sean objetivos sencillos para agresiones que buscan poner en riesgo información confidencial y el correcto funcionamiento de las entidades gubernamentales. Según Sánchez (2019) la “democracia electrónica”, vincula todos los trámites por parte del ciudadano, como usuario del Sistema Público en la aparición de las nuevas tecnologías.

El problema adquiere relevancia ante el aumento de ciberamenazas a instituciones públicas en Latinoamérica, donde ataques como phishing o ransomware han paralizado servicios esenciales y erosionado la confianza ciudadana. En GAD El Empalme, esto se agrava por la brecha digital entre la población y la escasa retroalimentación ante incidentes reportados. Así, el estudio no solo evalúa vulnerabilidades técnicas, sino también el intercambio de información entre los organismos de Gobierno, Según Varela (2022) uno de los aspectos más decisivos para reconsiderar sería los modos de gestión del sector público van a ser el cambio del entorno.

Metodológicamente, se adoptó un enfoque mixto (cualitativo-cuantitativo). Mediante encuestas a 70 usuarios y entrevista a director del departamento administrativo, identificamos patrones de percepción, brechas de capacitación y protocolos ausentes. Los resultados revelan no solo las debilidades actuales, sino también oportunidades para diseñar estrategias adaptadas a un cantón con características rural-urbanas, donde la confianza en lo digital es frágil pero necesaria para el desarrollo, para eso el gobierno electrónico se proyectó para optimizar la eficiencia del gobierno y mejorar los servicios estatales en todas las esferas de gobierno (Choez-Calderón & Aldo-Patricio, 2025).

El objetivo es analizar el impacto de la implementación del Gobierno Electrónico en la eficiencia operativa y los niveles de transparencia en la gestión pública, asegurando que la modernización del GAD El Empalme sea segura, inclusiva y sostenible. Este trabajo aporta evidencia empírica para políticas públicas en gobiernos locales con realidades similares, destacando que, en la digitalización, la seguridad, la transparencia consiste en llevar a cabo prácticas y estrategias que posibiliten la divulgación pública de actividades, resultados o faltas.

## 2. Materiales y métodos

La investigación adoptó un enfoque mixto que integró métodos cualitativos y cuantitativos para obtener una comprensión integral del funcionamiento del presupuesto participativo en el GAD El Empalme. Esta complementariedad metodológica permitió combinar la profundidad interpretativa del análisis cualitativo con la rigurosidad estadística del enfoque cuantitativo, respondiendo así a la naturaleza compleja del objeto de investigación.

El componente cualitativo profundizó en las problemáticas sociales asociadas a la participación ciudadana, considerando las particularidades del contexto local. Se empleó la investigación documental como técnica principal, mediante la recopilación, selección y análisis de información proveniente de libros, artículos científicos, documentos oficiales, actas y memorias institucionales. Según Ávila-Coello (2024) Las TIC pasaron de ser consideradas como simples sistemas computacionales a constituirse en herramientas fundamentales que apoyan el desarrollo virtual de un sinnúmero de las actividades. Adicionalmente, se realizó una entrevista semiestructurada a un funcionario de la Dirección de Planificación y Participación Ciudadana del GAD El Empalme para profundizar en las dinámicas internas del proceso participativo. Como señala Quecedo et al. (2002). Las técnicas cualitativas pueden utilizarse de forma complementaria, para incrementar la fiabilidad o validez de un diseño cuantitativo.

El componente cuantitativo se enfocó en la recolección de datos empíricos para establecer relaciones de causa-efecto asociados a la percepción ciudadana sobre el presupuesto participativo. Se aplicaron encuestas estructuradas a una muestra aleatoria de 70 usuarios y director del departamento administrativo del GAD El Empalme, estas encuestas cuantificaron variables como nivel de conocimiento, frecuencia de participación, percepción de transparencia y efectividad en la asignación de recursos. De acuerdo con Babativa (2017) la investigación cuantitativa se basa en hallazgos replicables que permiten abordar fenómenos sociales mediante análisis estadístico.

Los datos obtenidos fueron procesados y tabulados en una hoja de cálculo Excel para organizar la información y facilitar la identificación de tendencias. El análisis se complementó con un enfoque descriptivo para caracterizar las situaciones, costumbres y actitudes predominantes en la comunidad respecto al presupuesto participativo. Se destaca que la investigación descriptiva busca detallar con exactitud las propiedades de los fenómenos observados, proporcionando una visión clara y contextualizada de la realidad estudiada.

### 3. Resultados

Los resultados obtenidos en el estudio evidencian una situación crítica respecto a la preparación institucional del GAD El Empalme frente a los desafíos de ciberseguridad en su modelo de gobierno electrónico. A través de un análisis mixto, se identificaron deficiencias tanto técnicas como estructurales: entre ellas, el uso de sistemas obsoletos, la ausencia de respaldos periódicos de información y debilidades organizacionales en cuanto a la gestión de la seguridad digital.

El estudio revela que el personal cuenta con escasa capacitación en temas de ciberseguridad, que no existen protocolos formalizados para la atención de incidentes, y que se destina un presupuesto insuficiente al fortalecimiento de la infraestructura tecnológica. Asimismo, se detectó una percepción generalizada de inseguridad digital entre funcionarios y usuarios, lo que repercute de manera negativa en la confianza de la ciudadanía.

Entre los hallazgos más relevantes se encuentra que el 70% de los sistemas digitales del GAD El Empalme operan con software obsoleto, afectando cultura institucional en cuanto a actualización tecnológica y gestión del riesgo digital. Según Ramos-Secaira (2023) las TIC abordan y generan cambios socioeconómicos, políticos y culturales, dando posibilidades de incremento económico e impacto en sus propios indicadores sociales que favorece la implicación activa de la comunidad al reconocer el valor público de esta cultura tecnológica.

Desde la dimensión humana, los resultados mostraron que solo el 15% del personal administrativo ha recibido capacitación básica en ciberseguridad, y que existe un amplio desconocimiento sobre amenazas comunes como el phishing o la suplantación de identidad. Las entrevistas realizadas revela la improvisación por parte del personal no especializado frente a incidentes técnicos, reforzando la relación entre la baja preparación del talento humano y la percepción de inseguridad digital.

En cuanto a la percepción ciudadana, la encuesta aplicada a usuarios mostró que únicamente el 28% confía plenamente en los servicios digitales del GAD El Empalme. Este resultado se relaciona con la falta de visibilidad de respuestas institucionales ante incidentes pasados y con la ausencia de campañas educativas sobre protección de datos y uso seguro de plataformas digitales. Además, el 43% de los encuestados manifestó preocupación por la seguridad de su información personal, lo que podría limitar el uso futuro de servicios en línea. Según Llasacce-Orosco (2024) las nuevas tecnologías fomentan innovación y cambios en la sociedad, al cual sus habitantes deben adoptarse si quieren progresar y estar de la mano con el avance de las nuevas tecnologías.

**Tabla 1**

*Principales indicadores técnicos y organizacionales del GAD El Empalme en ciberseguridad (2023)*

Indicador	Valor Reportado
Plataformas operando con software obsoleto	70%
Personal administrativo con capacitación en ciberseguridad	15%
Sistemas con respaldo regular de datos	Solo 40%
Incidentes de seguridad reportados en 2023	23 casos (35% acceso no autorizado• 26% phishing 17% DoS)
Confianza ciudadana plena en los servicios digitales	28%
Costo estimado de incidentes anuales	\$45,000 USD (equivale al 15% del presupuesto de TI)

*Nota:* GAD El Empalme

El GAD El Empalme tiene serios problemas de ciberseguridad: el 70% de sus sistemas usan softwares obsoletos y solo el 15% del personal está capacitado. Solo el 40% hace respaldos de datos, lo que aumenta el riesgo. En 2023 hubo 23 incidentes, muchos por accesos no autorizados y phishing. La baja confianza ciudadana (28%) y el alto costo de los ataques (\$45,000) muestran que se necesita mejorar urgentemente

Los datos confirman la existencia de una brecha significativa entre la digitalización de los servicios públicos y las prácticas de seguridad institucional. Esta situación se agrava con la escasa formación de los funcionarios y la inexistencia de protocolos formales de gestión de incidentes, lo que expone al GAD El Empalme a vulnerabilidades técnicas y riesgos operativos.

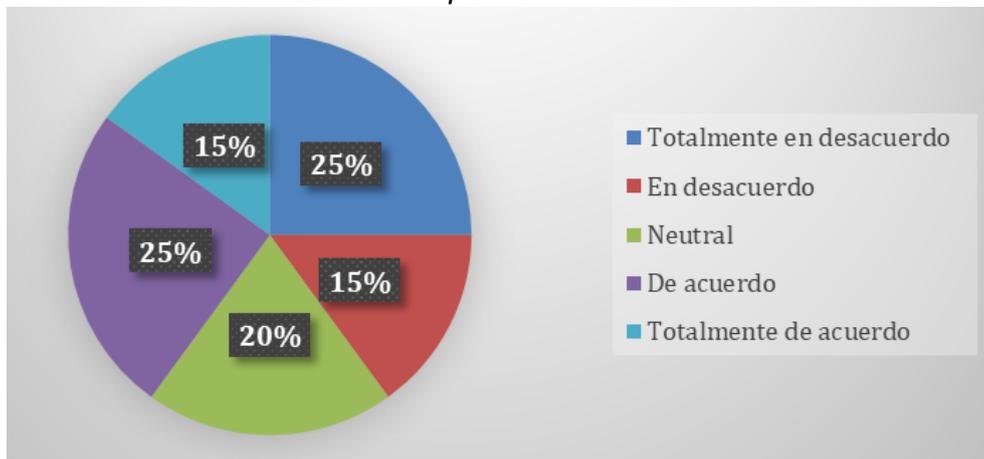
En términos presupuestarios, el estudio destaca la baja inversión en ciberseguridad: apenas el 3.2% del presupuesto anual se destina a tecnología, y solo el 15% de ese valor se orienta a medidas de seguridad digital. La ineficiencia en la ejecución presupuestaria también representa un factor de riesgo: los procesos de adquisición tecnológica toman en promedio ocho meses, afectando la capacidad de respuesta institucional ante amenazas emergentes. Además, se identificó una alta rotación del personal técnico, lo cual debilita la continuidad de las políticas de seguridad.

La discusión de estos hallazgos, desde los marcos conceptuales Ciberseguridad y la norma ISO 27001, permite concluir que el GAD El Empalme se encuentra en una etapa incipiente de madurez digital. No basta con disponer de infraestructura básica; es imprescindible fortalecer el componente organizacional, implementar protocolos normativos y fomentar una cultura institucional de protección de la información.

La recolección de datos ayuda a demostrar que la sensación de vulnerabilidad en el entorno digital no es únicamente personal ni aislada, sino que es un reflejo de una administración fragmentada y reaccional. La ausencia de indicadores de retorno de inversión en tecnología, la falta de políticas de retroalimentación a los ciudadanos y el incumplimiento de estándares mínimos de seguridad son elementos que configuran un entorno de baja resiliencia institucional.

Estos resultados subrayan la urgencia del manejo de la ciberseguridad contextualizado, con enfoque centrado en las personas, que articule inversión sostenida, desarrollo de competencias y gobernanza clara. Tal enfoque permitiría transitar desde una cultura de respuesta hacia una cultura de prevención, favoreciendo la confianza ciudadana y la sostenibilidad del proceso de transformación digital local.

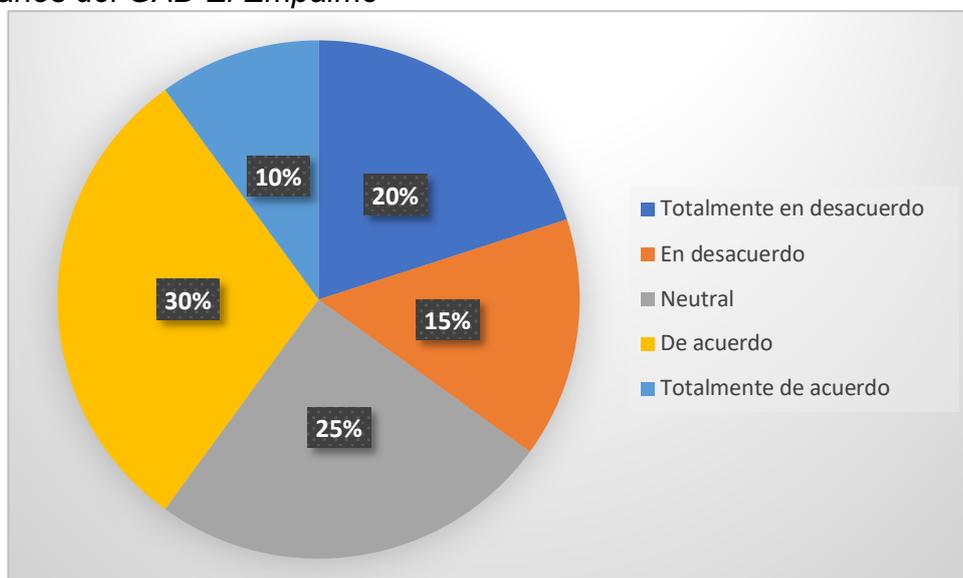
**Figura 1**  
*Tramites electrónicos en el GAD El Empalme*



Nota: Encuestas ciudadanía (Autores, 2025).

Un 25% de los encuestados expresó que "totalmente en desacuerdo" con la afirmación de que sus datos personales están seguros. Este dato es preocupante, ya que refleja una desconfianza significativa en la capacidad del GAD El Empalme para proteger la información personal. Un 15% adicional se mostró en desacuerdo, mientras que un 45% se posicionó en una postura neutral o de acuerdo.

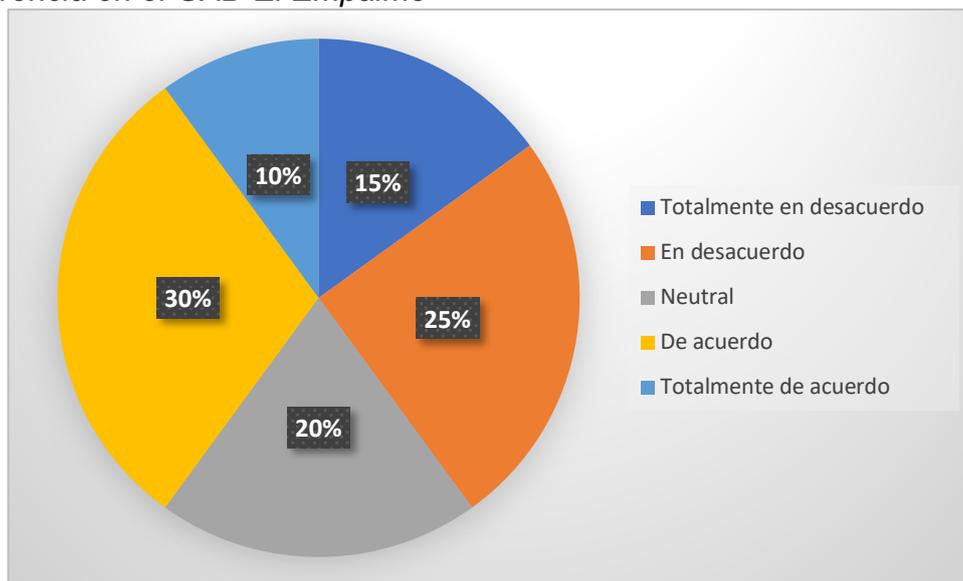
**Figura 2**  
*Funcionarios del GAD El Empalme*



Nota: Encuestas ciudadanía (Autores, 2025).

En relación con la capacitación de los funcionarios para garantizar la seguridad digital, un 20% se mostró "totalmente en desacuerdo" y un 15% "en desacuerdo". Solo un 55% de los encuestados se mostró positivo y neutral sobre la competencia de los funcionarios. Este resultado indica que, a pesar de la inversión en tecnología, la percepción de la competencia del personal es un área de mejora. Es crucial que el GAD El Empalme desarrolle programas de formación continua para su personal, asegurando que estén al día con las mejores prácticas en ciberseguridad y atención al ciudadano.

**Figura 3**  
*Transparencia en el GAD El Empalme*



Nota: Encuestas Ciudadanía (Autores, 2025).

La percepción de transparencia en el manejo de los datos personales arrojó resultados mixtos. Un 15% de los encuestados se mostró "totalmente en desacuerdo" con la afirmación de que hay transparencia en el uso de sus datos, y un 25% "en desacuerdo". Sin embargo, un 50% se mostró neutral o de acuerdo.

**Tabla 2**  
*Datos obtenidos por encuesta a la ciudadanía en el cantón El Empalme*

Preguntas	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Confío en que mis datos personales están seguros al realizar trámites electrónicos en el GAD El Empalme.	Totalmente en desacuerdo	5	25	25,0
	en desacuerdo	3	15,0	40,0
	neutral	4	20,0	60,0
	de acuerdo	5	25,0	85,0
	totalmente de acuerdo	3	15,0	100,0
Creo que los funcionarios del GAD El Empalme están	Totalmente en desacuerdo	20	100,0	100,0
	en desacuerdo	4	20,0	20,0
	en desacuerdo	3	15,0	35,0
	neutral	5	25,0	60,0
	de acuerdo	6	30,0	90,0
				100,0

capacitados para garantizar la seguridad digital.	totalmente de acuerdo		2	10,0	10,0	
	total		20	100,0	100,0	
Siento que hay transparencia por parte del GAD El Empalme	Totalmente en desacuerdo	en	3	15,0	15,0	15,0
	neutral		5	25,0	25,0	40,0
	de acuerdo	desacuerdo	4	20,0	20,0	60,0
	total		6	30,0	30,0	90,0
sobre cómo se utilizan y protegen mis datos.	de acuerdo		2	10,0	10,0	100,0
	totalmente de acuerdo		20	100,0	100,0	

*Nota:* Encuestas Ciudadanía (Autores, 2025).

Los resultados de la encuesta sobre la percepción del Gobierno Electrónico en el GAD El Empalme revelan una notable desconfianza ciudadana respecto a la seguridad de los datos y la capacitación de los funcionarios. Un 25% de los encuestados siente que sus datos no están seguros, lo que indica una barrera significativa para la adopción de servicios electrónicos. Además, un 20% considera que los funcionarios no están adecuadamente preparados para garantizar la seguridad digital, lo que refuerza la necesidad de invertir en formación continua. Por otro lado, aunque un 40% percibe cierta transparencia en la gestión de datos, un 40% adicional se muestra neutral, lo que sugiere oportunidades para mejorar la comunicación y aumentar la confianza. En conjunto, estos hallazgos subrayan la importancia de implementar estrategias de capacitación y comunicación efectivas para fortalecer la confianza y la participación ciudadana en el ámbito del Gobierno Electrónico.

#### 4. Discusión

La ciberseguridad en el gobierno electrónico constituye un eje fundamental para garantizar la integridad, confidencialidad y disponibilidad de los servicios digitales ofrecidos por los gobiernos locales. En el caso del GAD El Empalme, la investigación evidencia una brecha considerable entre el proceso de digitalización institucional y la capacidad técnica y organizativa para proteger los sistemas y datos manejados, comprometiendo seriamente la confianza ciudadana y la resiliencia institucional. Aunque se han realizado esfuerzos por implementar plataformas electrónicas, persisten múltiples deficiencias estructurales que limitan su eficacia como instrumento de modernización administrativa.

Los principales retos en materia de ciberseguridad radican en una infraestructura tecnológica vulnerable (70% de software obsoletos), una débil formación del personal (solo el 15% de los funcionarios ha recibido capacitación en seguridad digital) y una percepción generalizada de inseguridad (43% de la ciudadanía manifiesta preocupación por sus datos personales). Estos datos no solo muestran debilidades técnicas, sino que revelan barreras organizativas, económicas y culturales que obstaculizan la consolidación de un ecosistema digital seguro y confiable. Según

Boné-Andrade et al., (2023) La mayoría de las administraciones públicas concentran sus esfuerzos en darle prioridad a las necesidades del día a día de los ciudadanos.

En este sentido, (Vinueza & Jiménez, 2019) menciona que las amenazas que han ganado terreno, los ciberataques destacan como una herramienta cada vez más utilizada, ya sea para la represión política o para desafiar al Estado, de manera directa o encubierta. El GAD El Empalme no cuenta con protocolos de gestión de incidentes, ni con políticas de retroalimentación ciudadana tras vulneraciones de seguridad. A esto se suma una baja inversión presupuestaria, donde menos del 5% del gasto en tecnologías de la información se destina a seguridad digital, lo cual impide adoptar estándares como la norma ISO 27001 o marcos como el del NIST (Instituto Nacional de Estándares y Tecnología), fundamentales para una gestión integral del riesgo.

El análisis revela desafíos sustanciales en términos de transparencia institucional y percepción ciudadana. La encuesta evidencia que solo el 28% de los usuarios confía plenamente en los servicios digitales del GAD El Empalme, mientras que un 25% se muestra totalmente en desacuerdo con la afirmación de que sus datos están seguros. Además, el 35% de los encuestados cuestiona la capacitación del personal, lo que refuerza la percepción de desprotección frente a amenazas como el phishing, accesos no autorizados o suplantación de identidad. Este entorno refuerza un círculo de deslegitimación institucional, donde la ciudadanía se distancia progresivamente del uso de servicios digitales ante la falta de garantías mínimas.

Los resultados muestran una digitalización fragmentada y expuesta, con limitada capacidad de respuesta institucional y bajo compromiso ciudadano. A diferencia de experiencias exitosas en otras jurisdicciones locales que integran formación continua, inversión tecnológica y participación social, en el GAD El Empalme exhibe una estrategia reactiva, con adquisiciones lentas y alta rotación de personal técnico, lo cual debilita la sostenibilidad de cualquier avance tecnológico. Esto evidencia que la tecnología por sí sola no transforma la administración pública, si no se acompaña de políticas públicas sólidas y una cultura institucional orientada a la seguridad y la transparencia.

Respecto al fortalecimiento del vínculo entre gobierno y ciudadanía, los indicadores son claros: la confianza es baja, la percepción de transparencia limitada (40% se declara neutral o en desacuerdo con la gestión de sus datos), y no existen mecanismos efectivos de comunicación sobre las medidas de seguridad implementadas. Tal como plantea (Morán et al., 2024) empoderar a los ciudadanos, mejorar la entrega de servicios, fortalecer la responsabilidad, incrementar la transparencia y mejorar la eficiencia gubernamental.

La ciberseguridad, entonces, no solo debe entenderse como un componente técnico del gobierno electrónico, sino como una herramienta estratégica de fortalecimiento institucional y reconstrucción de la legitimidad pública. Sin embargo, para que esto sea posible, es indispensable superar las barreras técnicas, organizativas y

presupuestarias que actualmente limitan su implementación en territorios como El Empalme.

Como señala (Ospina, 2023), las tecnologías de la Información y las comunicaciones para incrementar la eficiencia y efectividad de la función pública, donde se reconozca al ciudadano no solo como usuario, sino como agente activo en la transformación digital del Estado. El caso del GAD El Empalme evidencia la distancia entre el diseño tecnológico y la capacidad institucional para gestionarlo, subrayando la necesidad urgente de desarrollar un modelo contextualizado de ciberseguridad que articule inversión sostenida, competencias humanas y participación ciudadana informada.

## 5. Conclusiones

El proceso de digitalización emprendido por el GAD El Empalme marca un progreso de una infraestructura tecnológica poco robusta y la limitación de estrategia eficiente de seguridad informática. La adopción de servicios digitales no ha sido acompañada por una inversión proporcional en protección informática ni por la actualización oportuna de sistemas, lo cual ha generado importantes riesgos operativos e institucionales.

Uno de los hallazgos más significativos del estudio es la baja capacitación del personal municipal en temas de seguridad digital, con solo un 15% de los funcionarios administrativos que ha recibido formación básica. Esta carencia se traduce en prácticas vulnerables, respuestas improvisadas ante incidentes y una débil capacidad de respuesta institucional frente a amenazas, como ataques de phishing o accesos no autorizados. Esto confirma que el factor humano sigue siendo el eslabón más frágil en la cadena de ciberseguridad.

Desde la perspectiva ciudadana, la baja confianza en los servicios electrónicos del municipio refleja una percepción de inseguridad digital arraigada. La limitada comunicación institucional ante fallos de seguridad y la falta de transparencia sobre la protección de los datos personales afectan negativamente la legitimidad del gobierno electrónico y su aceptación por parte de la comunidad. Esta percepción representa una barrera clave para la consolidación de un ecosistema digital participativo y resiliente.

A nivel normativo, el estudio confirma la existencia de vacíos regulatorios y una débil aplicación de estándares internacionales, como los establecidos por la norma ISO 27001 o el marco de ciberseguridad del NIST. Según (Zamora et al., 2025) El Gobierno Electrónico en Ecuador no solo busca optimizar los procesos internos del sector público, sino también abrir nuevas vías de interacción con la sociedad civil. La falta de protocolos definidos y la ausencia de auditorías periódicas específicas en materia de seguridad digital dificultan una gestión proactiva de riesgos. De igual manera, la limitada asignación de recursos presupuestarios, representando menos del 5% del

gasto en tecnologías de la información destinado a ciberseguridad, dificulta la aplicación adecuada de acciones preventivas y correctivas.

La investigación confirma que la visión institucional respecto a la ciberseguridad se encuentra directamente relacionada con los aspectos técnicos, el recurso humano y el marco normativo vigente en el GAD El Empalme. Se vuelve imprescindible la transparencia de ciberseguridad adaptado al contexto local, que no solo fortalezca la infraestructura digital, sino que también promueva una cultura organizacional orientada a la prevención, la capacitación continua y la transparencia ciudadana. Solo así será posible avanzar hacia un gobierno electrónico confiable, inclusivo y sostenible.

## CONFLICTO DE INTERESES

“Los autores declaran no tener ningún conflicto de intereses”.

## Referencias Bibliográficas

- Abarca Amador, Y. (2017). Procesos de capacitación ayudados por TIC en el ámbito laboral. *Revista De Lenguas Modernas*, (25). <https://doi.org/10.15517/rm.v0i25.27710>
- Ávila-Coello, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. *Journal of Economic and Social Science Research*, 4(2), 140–156. <https://doi.org/10.55813/gaea/jessr/v4/n2/96>
- Babativa Novoa, C. (2017). Investigación cuantitativa. Bogotá : Fundación Universitaria del Área Andina, 2017. <https://dijitk.areandina.edu.co/handle/areandina/3544>
- Boné-Andrade, M. F., Pinargote-Bravo, V. J., & Bonilla-Fierro, L. F. (2023). Estrategias de ciberseguridad en entornos de trabajo híbridos y remoto. *Revista Científica Ciencia Y Método*, 1(4), 31-43. <https://doi.org/10.55813/gaea/rcym/v1/n4/21>
- Choez-Calderón, C. J., & Aldo-Patricio, M. O. (2025). La ciberseguridad como prioridad empresarial dentro de marcos los regulatorios y normativos internacionales. *Revista Científica Ciencia Y Método*, 3(3), 14-27. <https://doi.org/10.55813/gaea/rcym/v3/n3/38>
- Llasacce-Orosco, U. (2024). El gobierno electrónico en la labor fiscal del Ministerio Público, Perú. *IUSTITIA SOCIALIS*, 9(16), 1–16. <https://doi.org/10.35381/racji.v8i16.3151>
- Morán Chilan, J. H., & Faubla Bravo, C. N. (2024) GOBIERNO ELECTRÓNICO EN LOS PROCESOS DE RECAUDACIÓN DE IMPUESTO DEL GAD JIPIJAPA, *Ciencia y Desarrollo. Universidad Alas Peruanas*, 27(3), 181-193

- Muñoz. (2025). Impacto del Gobierno Electrónico en la Eficiencia y Transparencia de la Gestión Pública. *Revista Veritas de Difusão Científica*, 6(1), 659–682. <https://doi.org/10.61616/rvdc.v6i1.426>
- Ospina. (2023). Gobierno digital e inteligencia artificial, una mirada al caso colombiano. *Administración & Desarrollo*, 53(1). <https://doi.org/10.22431/25005227.vol53n1.2>
- Quecedo Lecanda, R., & Castaño Garrido, C. (2002). *Introducción a la metodología de investigación cualitativa*. *Revista de Psicodidáctica*, 14, 1–36. <https://www.redalyc.org/pdf/175/17501402.pdf>
- Ramos-Secaira, F. M. (2023). Seguridad Cibernética en Empresas Ecuatorianas: Prácticas y Retos Actuales. *Revista Científica Zambos*, 2(3), 16-28. <https://doi.org/10.69484/rcz/v2/n3/47>
- Sánchez. (2019). Transformación digital en el acceso a la Atención Especializada: Aplicación Cita Web AE. *3C TIC: Cuadernos de Desarrollo Aplicados a Las TIC*, 8(2). <https://doi.org/10.17993/3ctic.2019.82.28-53>
- Tabarquino-Muñoz, R. A. (2018). El servicio público de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia 2010-2018. *Entramado*, 14(2), 166-181. <https://doi.org/10.18041/1900-3803/entramado.2.4752>
- Varela. (2022). Uso de las Tecnologías de la Información y su aporte a la calidad de servicio en instituciones públicas. *Revista Científica Sinapsis*, 2(21). <https://doi.org/10.37117/s.v2i21.677>
- Vinueza Miller, D. A., & Jiménez, R. P. (2019). Ciberataques como Estrategia Política: Un Análisis de su Impacto en la Libertad de Expresión Durante los Periodos de Inestabilidad Política del Ecuador (2019 -2024). *Revista Enfoques de la Comunicación*, 13, 261–295. <https://revista.consejodecomunicacion.gob.ec/index.php/rec/article/view/254>
- Zamora Mayorga, D. J., Andrade López, G. E., & Olmedo Izquierdo, E. A. (2025). Implementación del Gobierno Electrónico en la Democratización de la Administración Pública del Ecuador. *Revista Veritas De Difusão Científica*, 6(1), 1187–1202. <https://doi.org/10.61616/rvdc.v6i1.454>