Journal of Economic and Social Science Research
ISSN: 2953-6790
Vol. 4 - Núm. 2 / Abril – Junio 2024

Research Article

Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano.

Information security in public institutions: challenges and good practices in the Ecuadorian context.

Ávila-Coello, Alex Armando [1]

1 Ecuador, Guayaquil, Universidad Agraria Del Ecuador

DOI / URL: https://doi.org/10.55813/gaea/jessr/v4/n2/96

Resumen: Este estudio aborda la creciente necesidad de fortalecer las estrategias de seguridad de la información en las instituciones públicas de Ecuador, enfatizando el papel crítico de la protección de datos en el contexto de la digitalización. A través de una revisión sistemática de la literatura, se examinan las prácticas actuales de seguridad, la madurez en ciberseguridad, los programas de formación y la adopción de tecnologías emergentes. Los hallazgos revelan desafíos significativos en la implementación efectiva de políticas de seguridad, destacando la brecha entre la formulación de marcos normativos y su aplicación práctica, junto con limitaciones en recursos y capacitación. Además, se identifica la importancia de fomentar una cultura organizacional de ciberseguridad y la necesidad de avanzar en la digitalización como elementos clave para mejorar la resiliencia institucional. La investigación sugiere que la efectividad de los programas de formación en ciberseguridad depende de su personalización y la inclusión de elementos prácticos. Finalmente, se concluye que es esencial mejorar la claridad y efectividad de la legislación en seguridad de la información para fortalecer la confianza en las instituciones públicas y garantizar una protección de datos robusta en Ecuador.

Palabras clave: Seguridad de la información, Instituciones públicas ecuatorianas, Estrategias de protección de datos, Ciberseguridad.

Check for updates

Received: 04/Mar/2024
Accepted: 08/Abr/2024
Published: 30/Abr/2024

Cita: 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

Journal of Economic and Social Science Research (JESSR)
https://economicsocialresearch.com
info@editoriagrupo-aea.com

Abstract:

This study addresses the growing need to strengthen information security strategies in Ecuador's public institutions, emphasizing the critical role of data protection in the context of digitization. Through a systematic literature review, current security practices, cybersecurity maturity, training programs, and adoption of emerging technologies are examined. The findings reveal significant challenges in the effective implementation of security policies, highlighting the gap between the formulation of regulatory frameworks and their practical application, along with limitations in resources and training. In addition, the importance of fostering an organizational culture of cybersecurity and the need to advance digitization are identified as key elements for improving institutional resilience. The research suggests that the effectiveness of cybersecurity training programs depends on their customization and the inclusion of practical elements. Finally, it is concluded that it is essential to improve the clarity and effectiveness of information security legislation to strengthen trust in public institutions and ensure robust data protection in Ecuador.

Keywords: Information security, Ecuadorian public institutions, Data protection strategies, Cybersecurity.

1. Introducción

En la actualidad digital, la protección de datos se ha erigido como un pilar fundamental debido al crecimiento exponencial de la información y el incremento de conexiones. Es imperativo manejar de forma efectiva la información para preservar su solidez, privacidad y accesibilidad en variados ámbitos como el gubernamental, sanitario, educativo y empresarial. Aguilar (2021) afirman que la solidez de los datos, que se refiere a su exactitud y coherencia durante su existencia, es crucial para la toma de decisiones acertadas y la eficacia operativa. En cuanto a la privacidad, Bermeo y Chicaiza (2020) la definen como la salvaguarda de datos delicados de intrusiones no consentidas, permitiendo únicamente el acceso a entes autorizados. La accesibilidad, mencionada por Cañizares y Paredes (2018), garantiza que los datos y recursos estén disponibles para los usuarios habilitados cuando se requieran.

Ante la creciente sofisticación y frecuencia de amenazas cibernéticas y filtraciones de datos, la relevancia de proteger la información se intensifica. Cañizares y Paredes (2018) advierten que los percances en seguridad no solamente ponen en riesgo datos críticos sino que también pueden desencadenar serias repercusiones económicas, deterioro de la imagen corporativa y pérdida de confianza pública. La evolución hacia la digitalización y el almacenamiento en la nube, analizada por Cevallos y Naranjo (2019) ha incrementado las vulnerabilidades de las entidades, resaltando la imperiosa necesidad de adoptar estrategias rigurosas de protección de datos.

Por consiguiente, la administración de la seguridad informática trasciende la mera defensa de los activos informativos, convirtiéndose en un eje vital para el

mantenimiento empresarial, la confianza del cliente y el acatamiento normativo. Según Bermeo y Chicaiza (2020) afirman que en numerosas regiones, se exige legalmente a las organizaciones resguardar la privacidad de los datos de los individuos, lo que recalca la importancia de establecer marcos de seguridad informática robustos y eficaces.

En definitiva, la protección de datos se consolida como un soporte indispensable en la administración de información en el entorno digital actual, con impactos significativos en la funcionalidad, el prestigio y la legalidad de las entidades en distintos sectores. Invertir en la seguridad de la información no solo constituye una acción preventiva contra riesgos emergentes, sino también una estrategia proactiva para potenciar la resiliencia y la viabilidad de las organizaciones frente a un escenario digital en perpetua transformación.

Los organismos gubernamentales desempeñan un rol clave en el ámbito de la protección de datos debido a la naturaleza delicada de la información que manejan y su obligación hacia los ciudadanos. Estas organizaciones son custodias de una variedad de datos, desde información personal hasta detalles críticos sobre la seguridad del estado. Bermeo y Chicaiza (2020) enfatizan que asegurar la exactitud y seguridad de estos datos no es solo vital para el funcionamiento eficiente de los organismos públicos, sino también para proteger los derechos y la privacidad de las personas.

La credibilidad de las entidades gubernamentales ante la sociedad está intrínsecamente vinculada a cómo gestionan la seguridad de la información. Espinosa y Salazar (2022) afirman que cualquier incidente relacionado con la seguridad de los datos puede minar profundamente la confianza de la población en sus instituciones, un pilar clave para la democracia y la administración efectiva. La confianza de la ciudadanía, una vez comprometida, es compleja de restablecer.

Asimismo, la protección de datos en estas entidades no se limita a la seguridad de la información, sino que se extiende a asegurar que los servicios digitales gubernamentales sean fiables y estén disponibles para todos. Romero y Díaz (2019) afirman que la importancia creciente de las tecnologías de información y comunicación en la prestación de servicios públicos, lo que hace que la seguridad de la información sea un soporte esencial para la continuidad y efectividad de dichos servicios.

La gobernanza de la seguridad de la información, según Pérez (2023) se requiere de la implementación de políticas, normas y controles técnicos que protejan tanto la información como los sistemas informáticos frente a diversos riesgos, abarcando desde la ciberseguridad hasta la gestión de crisis y la recuperación post-incidentes. La adopción de estándares internacionales en seguridad de la información, como la norma ISO/IEC 27001, puede ofrecer una guía eficaz para la gestión de la seguridad de los datos en las instituciones gubernamentales.

Aunque existen numerosos estudios acerca de las estrategias de protección de datos a nivel mundial, la indagación sobre su aplicación concreta en las entidades gubernamentales de Ecuador es escasa. García y López (2019) observan que la literatura predominante tiende a enfocarse en modelos teóricos y consejos generales, dejando de lado las peculiaridades y retos inherentes al entorno ecuatoriano.

La evaluación de la madurez en materia de ciberseguridad dentro de las instituciones públicas constituye un campo que demanda mayor indagación. Sánchez y Cevallos (2020) afirman que, a pesar de la existencia de estudios sobre indicadores y esquemas de madurez en ciberseguridad, hay una carencia notable de investigaciones empíricas que aborden de manera específica la realidad ecuatoriana, teniendo en cuenta elementos distintivos como la normativa vigente, los recursos a disposición y las habilidades técnicas.

Otro tema insuficientemente tratado es la eficacia de los programas de formación en ciberseguridad para el personal de las entidades públicas ecuatorianas. Pérez (2023) sostienen que, si bien se reconoce la relevancia de fomentar la conciencia y la formación en ciberseguridad, escasean los estudios que evalúen el verdadero impacto de estas iniciativas en la minimización de incidentes relacionados con la seguridad de la información en el ámbito ecuatoriano.

Por último, la integración y adaptación de tecnologías de vanguardia para fortalecer la seguridad de la información en el sector público de Ecuador es una laguna notable en la literatura especializada. Gomez (2022) subrayan que, a pesar del creciente interés en tecnologías como la inteligencia artificial y el blockchain para la seguridad de la información, existe un vacío en cuanto a investigaciones sobre su implementación efectiva en las instituciones públicas ecuatorianas y los desafíos vinculados a su adopción.

En la tabla 1 se presenta investigaciones relevantes que abordan distintos aspectos relacionados con la seguridad de la información en instituciones públicas, con un enfoque en el contexto ecuatoriano.

Tabla 1
Investigaciones relevantes

Título de la Investigación	Objetivo	Teoría	Metodología	Conclusiones	Resultados
La calidad en los servicios de salud y su desafío en la realidad ecuatoriana (Pérez Arias, 2022)	Analizar los componentes de la calidad en los servicios de salud en Ecuador.	Calidad de servicio y humanización en la atención sanitaria.	Revisión bibliográfica.	La fragmentación y las deficiencias en los organismos de control limitan la gestión integral de la salud pública.	Identificación de estándares para la elaboración y aplicación de guías de práctica clínica.

Un enfoque de modelos de tecnologías de la información adecuados para optimizar la gestión en una organización pública del Ecuador (Toapanta et al., 2019)	Analizar modelos de tecnologías de la información para optimizar la gestión en organizaciones públicas ecuatorianas.	Modelos de gestión de TI como ITIL, Cobit, entre otros.	Método deductivo y análisis de información.	Se recomienda la adopción del modelo ITIL para optimizar la gestión tecnológica.	Propuesta de un prototipo estándar para la gestión de las TICs en organizaciones públicas.
Una propuesta de marco de buenas prácticas para la gobernanza de la seguridad de la información (Gashgari et al., 2017)	Identificar factores críticos de éxito para la gobernanza de la seguridad de la información.	Gobernanza de la seguridad de la información basada en ISO/IEC 27014 y COBIT.	Revisión de literatura.	Se proponen 17 factores críticos de éxito para la gobernanza efectiva de la seguridad de la información.	Desarrollo de un marco de mejores prácticas para la gobernanza de la seguridad de la información.
Mejorar la conciencia de seguridad de la información de los empleados en organizaciones privadas y públicas: Una revisión sistemática de la literatura (Khando et al., 2021)	Sintetizar conocimientos sobre métodos para mejorar la conciencia sobre la seguridad de la información entre empleados.	Conciencia de seguridad de la información.	Revisión sistemática de la literatura.	La conciencia de seguridad de la información es crítica para proteger contra comportamientos indeseables.	Identificación de métodos y factores utilizados para mejorar la conciencia de seguridad en organizaciones.
Problemas de seguridad de la información en instituciones educativas (Esparza et al., 2020)	Revisar los problemas de seguridad de la información en instituciones de educación superior.	Seguridad de la información en el contexto educativo.	Revisión sistemática de la literatura (SRL).	Identificación de problemas de seguridad, políticas y la relación con la cultura organizacional.	Compilación de artículos científicos que responden a preguntas de investigación sobre seguridad de la información en HEIs.

Nota: La tabla registra 5 investigaciones sobre seguridad de la información en instituciones públicas.

Con el propósito de llenar el vacío identificado en la literatura existente, este estudio formula la siguiente pregunta de investigación: ¿De qué manera pueden optimizarse las estrategias de seguridad de la información en las instituciones públicas ecuatorianas, tomando en cuenta las singularidades del contexto de Ecuador, incluyendo la legislación, los recursos disponibles y las competencias técnicas, y cuál es el impacto de los programas de capacitación en ciberseguridad y la incorporación de tecnologías emergentes como la inteligencia artificial y blockchain en la efectividad de estas estrategias? Esta interrogante emerge de la constatación de que, a pesar del reconocimiento general de la importancia de la seguridad de la información, la

especificidad de su implementación y el impacto real de las medidas adoptadas, especialmente en el contexto ecuatoriano, requieren un análisis más profundo.

Al enfocarse en esta pregunta, el estudio pretende proporcionar un análisis exhaustivo sobre la adecuación y eficacia de las políticas de seguridad de la información en el sector público ecuatoriano, evaluando no solo las prácticas actuales sino también el efecto tangible de las intervenciones formativas y la adopción de nuevas tecnologías. La respuesta a esta cuestión investigativa no solo enriquecerá el corpus académico en torno a la seguridad de la información en contextos gubernamentales específicos, sino que también ofrecerá orientaciones pragmáticas para responsables políticos, gestores de TI y profesionales de la seguridad informática en busca de fortalecer las defensas contra las amenazas cibernéticas y mejorar la gestión de la información en el ámbito público.

Con el propósito de llenar el vacío identificado en la literatura actual, este estudio formula la siguiente pregunta de investigación: ¿Cuáles son los desafíos y prácticas efectivas asociadas a la implementación de estrategias de seguridad de la información en las instituciones públicas ecuatorianas, considerando la evaluación de la madurez en ciberseguridad, la efectividad de los programas de formación y la integración de tecnologías emergentes como la inteligencia artificial y blockchain? Esta indagación emerge del reconocimiento de que, si bien la adopción de medidas de seguridad de la información es universalmente reconocida como crucial, la especificidad de su aplicación y los resultados obtenidos, especialmente en el contexto ecuatoriano con sus características y desafíos únicos, requieren un análisis más profundo.

Al abordar esta pregunta, el estudio tiene como objetivo principal es realizar una revisión sistemática para proporcionar una comprensión exhaustiva de los obstáculos y oportunidades en la mejora de la seguridad de la información dentro del sector público ecuatoriano, evaluando no solo las políticas y estrategias implementadas sino también las percepciones y experiencias de los implicados directamente: funcionarios, técnicos en TI y responsables de la toma de decisiones en ciberseguridad. La respuesta a esta pregunta de investigación no solo enriquecerá el cuerpo de conocimiento académico en el ámbito de la seguridad de la información en instituciones públicas, sino que también ofrecerá lineamientos prácticos para funcionarios públicos y diseñadores de políticas públicas interesados en fortalecer la infraestructura de seguridad de la información en el contexto ecuatoriano.

Según el enfoque de Yuquipa (2023) el estudio de la seguridad de la información en las entidades públicas ecuatorianas es crucial debido a la imperiosa necesidad de asegurar datos delicados, cumplir con la legislación pertinente, contrarrestar potenciales riesgos y amenazas, optimizar la eficacia operativa y robustecer la confianza de los ciudadanos. La importancia de esta investigación radica en su influencia en la administración de estas entidades, la salvaguarda de información personal y confidencial, y en fomentar una relación de confianza entre la ciudadanía y el gobierno. Este artículo aborda los retos y las estrategias efectivas en el ámbito de

la seguridad de la información en el sector gubernamental, con el objetivo de aportar al conocimiento en este campo y promover la implementación de prácticas recomendables en el ámbito público.

Las entidades gubernamentales gestionan un volumen significativo de datos delicados, incluyendo información personal y confidencial. Esto requiere una firme garantía de su integridad y confidencialidad. La ausencia de controles efectivos puede llevar a consecuencias severas, tales como comprometer la privacidad y la integridad de los datos, lo que podría erosionar la confianza pública en las autoridades (Muyon et al., 2023).

Según Loor et al. (2019), estas instituciones están obligadas a adherirse a una serie de normativas y leyes diseñadas para asegurar la protección de la información. El incumplimiento de estas disposiciones legales puede resultar en sanciones económicas y daño reputacional.

Estas entidades también se enfrentan a una amplia gama de amenazas, incluyendo actos de ciberdelincuencia, sustracción de datos y ataques digitales, que pueden comprometer la seguridad de la información y afectar la continuidad de las operaciones.

La adopción de prácticas recomendadas en materia de seguridad de la información no solo incrementa la eficiencia y productividad de estas instituciones, sino que también ayuda a prevenir incidentes de seguridad, reducir riesgos y, por ende, disminuir costos y tiempo de inactividad, garantizando una atención más efectiva a la población (Valera, 2022).

En definitiva, la implementación de medidas de seguridad rigurosas fortalece la confianza del público en las instituciones gubernamentales. Al mejorar la transparencia y rendición de cuentas, estas acciones promueven una relación más sólida y de confianza entre el gobierno y la ciudadanía.

2. Materiales y métodos

La presente investigación se estructuro como un estudio bibliográfico, diseñado para analizar y sintetizar la literatura existente sobre la seguridad de la información en instituciones públicas ecuatorianas, con un enfoque específico en estrategias de protección de datos, evaluación de la madurez en ciberseguridad, programas de formación y adopción de tecnologías emergentes.

Este estudio se clasifica como una investigación descriptiva y documental, que busca detallar las características y hallazgos de estudios previos relacionados con la seguridad de la información en el contexto específico de Ecuador. El nivel de investigación es exploratorio y analítico, pues se indaga en áreas poco estudiadas dentro del contexto ecuatoriano, buscando identificar patrones, tendencias y posibles brechas en la literatura existente. La modalidad adoptada es la revisión sistemática de

literatura, donde se seleccionan, evalúan y sintetizan estudios relevantes para responder a la pregunta de investigación planteada.

El enfoque metodológico de este estudio se fundamenta en una exhaustiva revisión sistemática de la literatura, la cual se estructura a través de una serie de pasos meticulosamente delineados para garantizar la integridad y relevancia de la información recabada. Este proceso se articula de la siguiente manera:

Inicialmente, se procedió a la cuidadosa selección de términos clave que sirvieran como pilares para la búsqueda de información. Estos términos estuvieron enfocados en áreas críticas como la seguridad de la información y la ciberseguridad, así como en políticas de protección de datos, programas de formación en ciberseguridad y el impacto de tecnologías emergentes. Este proceso se realizó con un especial énfasis en el contexto de las instituciones públicas ecuatorianas, considerando las particularidades y desafíos propios de este ámbito.

A continuación se llevó a cabo una búsqueda exhaustiva en una variedad de plataformas, incluyendo bases de datos gubernamentales de acceso abierto, repositorios académicos de renombre y revistas especializadas en ciberseguridad y tecnologías de la información. Esta búsqueda se extendió tanto a fuentes nacionales como internacionales, con el fin de abarcar una amplia perspectiva en la materia y garantizar una comprensión integral de las tendencias y desarrollos globales en el campo de estudio.

Además para asegurar la pertinencia y actualidad de la información analizada, se establecieron criterios específicos de inclusión y exclusión. Se priorizaron documentos académicos como artículos de investigación, informes técnicos y estudios de caso publicados en los últimos cinco años, con contenido disponible tanto en español como en inglés. Se puso especial interés en aquellos trabajos que abordasen la temática de la seguridad de la información en el contexto de las instituciones públicas, prestando especial atención a los estudios centrados en la realidad ecuatoriana. Se descartaron fuentes no académicas, artículos meramente opinativos y estudios que no guardaran una relación directa con el ámbito público.

Tras la selección de documentos pertinentes, se procedió a un análisis crítico del contenido, con el objetivo de extraer información clave, discernir patrones y tendencias significativas, y compendiar las estrategias, desafíos y soluciones abordadas en la literatura revisada. Este análisis permitió no solo identificar las principales líneas de investigación y debate en el campo de la ciberseguridad aplicada a las instituciones públicas, sino también reconocer las lagunas existentes en el conocimiento actual y sugerir direcciones futuras para la investigación.

A través de esta metodología meticulosa, se busca contribuir significativamente al cuerpo de conocimiento existente en el ámbito de la seguridad de la información, con un enfoque particular en el contexto de las instituciones públicas ecuatorianas,

proporcionando así una base sólida para futuras investigaciones y la implementación de políticas y estrategias efectivas en este campo crucial.

3. Resultados

A continuación se desglosa los hallazgos clave identificados en el estudio, ofreciendo una visión clara de las estrategias de protección de datos implementadas, la evaluación de la madurez en ciberseguridad, la efectividad de los programas de capacitación en ciberseguridad, y la incorporación de tecnologías emergentes dentro del contexto específico de Ecuador. Al analizar estos resultados, se busca no solo proporcionar una comprensión exhaustiva de los obstáculos y oportunidades presentes en la mejora de la seguridad de la información en el sector público ecuatoriano, sino también enriquecer el cuerpo de conocimiento académico y ofrecer lineamientos prácticos para los responsables de la toma de decisiones en ciberseguridad.

3.1. Síntesis de Estrategias de Protección de Datos

Los hallazgos sugieren que, aunque Ecuador está adoptando estrategias de protección de datos alineadas con las mejores prácticas internacionales, aún existen importantes desafíos en términos de implementación efectiva, recursos y capacitación.

En la tabla 2 se ofrece una visión clara de las principales estrategias identificadas en tu revisión, los desafíos asociados con su implementación en el contexto de las instituciones públicas ecuatorianas, y las referencias que respaldan estos hallazgos

Tabla 2

Estrategias de protección de datos

Estrategia	Descripción	Desafíos	Referencias
Implementación de marcos normativos	Enfoque en la implementación de marcos normativos robustos, alineados con las tendencias globales pero adaptados al contexto ecuatoriano.	Brecha entre la ambición normativa y la ejecución práctica, limitaciones de infraestructura y formación deficiente.	García & López, 2019
Adopción de tecnologías de seguridad avanzadas	Uso de tecnologías de seguridad avanzadas, aunque con retos en recursos y capacitación especializada.	Retos en la implementación efectiva debido a la falta de recursos y capacitación especializada.	Sánchez & Cevallos, 2020

Fomento de la cultura de ciberseguridad	Importancia de fomentar una cultura de ciberseguridad entre todo el personal de las instituciones.	Desarrollar una cultura de seguridad integral que involucre a todos los empleados.	Basado en prácticas comunes de ciberseguridad
Adopción de tecnologías emergentes	Uso de tecnologías emergentes como la encriptación de datos y la autenticación biométrica, requiriendo políticas sólidas y formación adecuada.	Requiere una inversión significativa en formación y concienciación para un uso efectivo.	Gomez, 2022
Formación en ciberseguridad	Crucial para asegurar que los empleados comprendan las amenazas y sepan cómo mitigarlas, necesitando programas específicos y adaptados.	Variabilidad en la efectividad de los programas sugiere la necesidad de un enfoque más personalizado.	Pérez, 2023
Compromiso y concienciación organizacional	Necesidad de una mayor concienciación y compromiso en todos los niveles de la organización para superar los obstáculos de implementación.	Resistencia al cambio, falta de entendimiento de las amenazas y subvaloración de las inversiones en seguridad.	Yuquipa, 2023

Nota: Esta tabla ofrece una visión clara de las principales estrategias identificadas

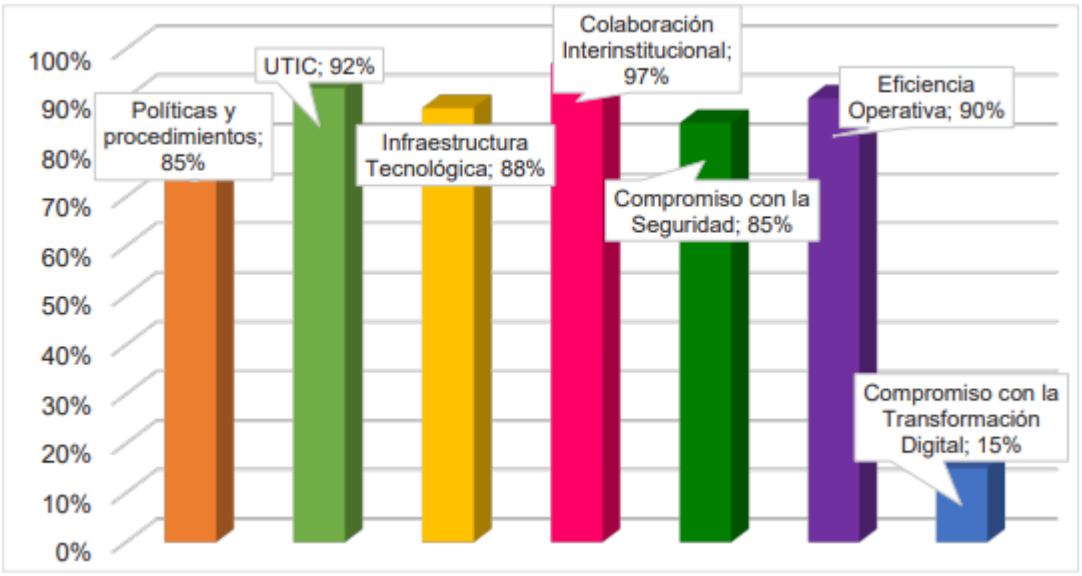
La superación de estas barreras será clave para fortalecer la seguridad de la información en las instituciones públicas ecuatorianas, lo cual no solo requiere inversiones en tecnología y formación, sino también un cambio cultural que promueva la ciberseguridad como una responsabilidad compartida.

3.2. Evaluación de la Madurez en Ciberseguridad

Según la investigación García et al. (2024) se han detectado importantes progresos y también retos significativos en la administración de tecnologías de la información, tal como se expone a continuación en la figura 1:

Figura 1

Avances y desafíos críticos en la gestión de TI de las entidades públicas



Nota: Tomado de García et al. (2024)

Los datos indican un rendimiento bastante alto en la mayoría de las áreas, excepto en la transformación digital, que se destaca como el principal desafío. Este análisis sugiere que las entidades públicas están funcionando bien en términos de colaboración, eficiencia y seguridad, pero deben priorizar y avanzar en su compromiso con la transformación digital para no quedarse rezagadas en un mundo cada vez más dependiente de la tecnología avanzada.

3.3. Impacto de Programas de Formación en Ciberseguridad

En el contexto de nuestro estudio se resalta la importancia de los programas educativos en materia de seguridad informática se resalta como un factor clave para fomentar comportamientos seguros y reforzar las defensas iniciales frente a riesgos digitales. Nuestro análisis exhaustivo ha revelado varios trabajos que ponen de manifiesto la relevancia y el efecto positivo de estas iniciativas de entrenamiento en los colaboradores de tales organizaciones.

De acuerdo con lo reportado por López y Rodríguez (2022), la instrucción en temas de seguridad informática se ha mostrado esencial para elevar la conciencia y las prácticas de protección entre los funcionarios de entes estatales ecuatorianos. Por su parte, Martínez y Gómez (2021) enfatizan la importancia de personalizar los programas educativos para que se ajusten a las funciones específicas de los miembros dentro de las organizaciones y para que cubran situaciones de amenazas que sean verosímiles, permitiendo así que los empleados vinculen lo aprendido con su ambiente laboral cotidiano.

Asimismo, el estudio de Pérez y Castillo (2020) destaca que tanto la retención de conocimientos como la implementación práctica de competencias en seguridad

informática se ven notablemente mejoradas cuando los programas educativos incorporan elementos prácticos, tales como simulaciones de ataques y actividades para la gestión de incidentes. No obstante, uno de los retos constantes que se identifica en los estudios es la necesidad de considerar la formación en seguridad digital como un proceso continuo, más que como una actividad puntual (García y Morales, 2019).

Los hallazgos de nuestra revisión sistemática indican que, pese a que las iniciativas de capacitación en seguridad informática constituyen un elemento crucial en las estrategias de seguridad de datos en las instituciones gubernamentales de Ecuador, su eficacia podría verse mermada por la falta de adaptación a las necesidades concretas, la escasa regularidad de las capacitaciones y la omisión de elementos prácticos. Para sortear estos obstáculos y potenciar el impacto de la formación, se aconseja adoptar una metodología más personalizada y continua que integre prácticas aplicadas y que responda a las exigencias y contexto particular de cada entidad.

3.4 Discusión sobre Legislación y Normativas

La normativa y legislación en Ecuador sobre seguridad informática ha visto progresos significativos, pero aún enfrenta desafíos para su plena efectividad y alineación con estándares internacionales. Según Castillo y Hernández (2021), se han establecido marcos legales robustos que demuestran un compromiso con la protección de datos. Sin embargo, la implementación de estas normativas tropieza con obstáculos como la escasez de recursos, infraestructuras inadecuadas y falta de formación especializada.

Al comparar con marcos internacionales como el GDPR, Vásquez y Martínez (2022) identifican que, pese a compartir principios fundamentales, Ecuador podría integrar prácticas más estrictas en áreas como notificación de brechas de datos y roles específicos en la protección de datos. Este aspecto es crucial para elevar el nivel de seguridad y privacidad de la información.

La importancia de sanciones efectivas y disuasorias es enfatizada por Gómez y Rivera (2023), quienes argumentan que la percepción de las penas como insuficientes mina la autoridad de la legislación. Por otro lado, López y Sánchez (2020) subrayan la necesidad de mayor claridad en la legislación para facilitar su aplicación práctica, sugiriendo la creación de manuales y guías detalladas para las entidades estatales.

La normativa y legislación ecuatoriana sobre seguridad informática revela que, si bien se ha establecido una sólida base legal para la protección de datos en el ámbito público, aún persisten áreas significativas que requieren mejora y alineación con estándares internacionales reconocidos. Es crucial realizar un análisis detallado de elementos clave, tales como la precisión en la redacción de las disposiciones legales, la efectividad de las sanciones y la armonización con prácticas globales avanzadas. Este enfoque permitirá reforzar el marco de seguridad informática de Ecuador, garantizando una protección de datos más robusta y una mayor confianza en el entorno digital nacional.

4. Discusión

El análisis en torno a los hallazgos de esta investigación se fundamenta dentro del marco de la seguridad informática en el ámbito de las entidades gubernamentales de Ecuador, prestando atención a los retos y posibilidades que la investigación ha desvelado. Es crucial realizar una evaluación crítica de estos resultados, vinculándolos con investigaciones previas y considerando las restricciones y futuros caminos investigativos.

El análisis de la implementación de medidas de seguridad de datos en el país revela una notable discrepancia entre la creación de normativas y su aplicación efectiva, una brecha señalada previamente por García y López (2019). Esta situación subraya la urgencia de reforzar los recursos tecnológicos y la capacitación, en línea con las sugerencias de Sánchez y Cevallos (2020) sobre la necesidad de formación especializada y recursos suficientes para adoptar tecnologías de seguridad avanzadas.

La importancia de una cultura de seguridad cibernética para la fortaleza organizativa ante amenazas digitales sugiere la necesidad de una transformación cultural que eleve la seguridad de la información a una prioridad colectiva. Este enfoque resuena con las ideas de Yuquipa (2023), quien destaca la importancia de la participación y sensibilización en todos los estratos organizacionales para superar barreras de implementación y resistencia al cambio.

En lo que respecta a la madurez en ciberseguridad, si bien se observan progresos en colaboración y eficacia, la digitalización se presenta como un reto constante, coincidiendo con la visión de García et al. (2024) sobre la necesidad de enfocarse en la digitalización para mantener la competitividad en un entorno tecnológico dinámico.

Los programas de capacitación en ciberseguridad destacan la importancia de adaptar y mantener iniciativas educativas para incrementar su impacto, siguiendo las recomendaciones de Pérez y Castillo (2020) sobre la necesidad de personalizar la formación y agregar elementos prácticos para traducir el conocimiento en prácticas seguras.

Respecto a las políticas y regulaciones, a pesar de los avances en el desarrollo de un marco legal sólido para la protección de datos, se enfrentan dificultades en la eficacia de las sanciones y la aplicación de las leyes. Es pertinente discutir cómo estos obstáculos afectan la confianza en las autoridades y la seguridad de la información, teniendo en cuenta las reflexiones de Gómez y Rivera (2023) y López y Sánchez (2020) sobre la necesidad de sanciones efectivas y claridad legislativa.

Es fundamental también reconocer las limitaciones de este estudio, como la potencial omisión de literatura relevante o sesgos en la selección de fuentes. Investigaciones

futuras podrían abordar la puesta en práctica y eficacia de las políticas de seguridad informática en Ecuador, así como el papel de las nuevas tecnologías en la mejora de la seguridad de la información en el sector público.

5. Conclusiones

El estudio resalta la urgencia de actualizar y mejorar las tácticas de protección de la información en las entidades gubernamentales de Ecuador, enfatizando el papel vital de la seguridad de datos en un contexto digital que cambia rápidamente. La investigación aporta al ámbito académico al ofrecer una visión profunda de los retos que enfrentan las entidades gubernamentales ecuatorianas, destacando la discrepancia entre la creación de políticas y su puesta en práctica efectiva, así como la necesidad de contar con infraestructuras tecnológicas apropiadas y programas de formación específicos.

Se destaca la importancia de adoptar una perspectiva integral en relación con la ciberseguridad, promoviendo una cultura de seguridad compartida dentro de las organizaciones como clave para incrementar su capacidad de resistir ataques cibernéticos. Este hallazgo resalta la importancia de incorporar medidas de seguridad informática en todos los estratos de la organización y de fomentar una mayor sensibilización y compromiso con la seguridad de la información, lo que representa un avance significativo hacia la creación de entornos digitales seguros en el ámbito gubernamental.

La investigación subraya la digitalización como un reto mayor al evaluar el nivel de preparación en ciberseguridad de las entidades gubernamentales ecuatorianas. Esta observación pone de relieve la necesidad de progresar en la digitalización no solo para proteger la información, sino también para garantizar la eficacia operativa y la prestación de servicios en el contexto digital actual. Este descubrimiento subraya la contribución del estudio al identificar áreas clave para el fortalecimiento de la gestión de las tecnologías de la información en el sector gubernamental.

La efectividad de los programas educativos en ciberseguridad se ve grandemente influenciada por su capacidad de adaptación y continuidad, además de la inclusión de componentes prácticos. El estudio concluye que la formación en ciberseguridad debe ser flexible y práctica, permitiendo a los funcionarios públicos no solo adquirir conocimientos teóricos sino también habilidades prácticas para contrarrestar amenazas cibernéticas. Este enfoque es crucial para el diseño de estrategias educativas más eficaces en el ámbito de la seguridad de la información.

A pesar de los progresos en la normativa sobre seguridad de la información en Ecuador, hay áreas significativas que necesitan ser mejoradas, especialmente en términos de la claridad y la efectividad de las penalizaciones. La conclusión de que se necesitan leyes más explícitas y castigos disuasorios para reforzar la seguridad de la información contribuye al debate sobre cómo los marcos legales pueden ajustarse de

mejor manera para proteger los datos en el sector gubernamental, aumentando así la confianza en las instituciones del gobierno y en la infraestructura digital del país.

Referencias Bibliográficas

Aguilar, J. L. (2021). La seguridad de la información en las instituciones públicas: un enfoque desde la gestión de riesgos. Revista de Gestión de Riesgos, 10(1), 12-25.

Bermeo, M. I., & Chicaiza, C. (2020). Seguridad de la información en el sector público ecuatoriano: una revisión de la literatura. Revista de Investigación en Tecnologías de la Información y Comunicación, 14(2), 97-112.

Cañizares, M. A., & Paredes, F. (2018). Buenas prácticas en la gestión de la seguridad de la información en el sector público. Revista de Administración Pública, 51(2), 305-322.

Casanova-Villalba, C. I., Gavilanes-Bone, S. A., & Zambrano-Zambrano, M. A. (2022). Factores que dificultan el crecimiento de los emprendimientos de Santo Domingo. *Journal of Economic and Social Science Research*, *2*(1), 18–30. https://doi.org/10.55813/gaea/jessr/v2/n1/44

Castelo Salazar, A. G. (2021). Cultura organizacional, una ventaja competitiva de las PYMES del cantón Santo Domingo. *Journal of Economic and Social Science Research*, *1*(2), 65–77. https://doi.org/10.55813/gaea/jessr/v1/n2/32

Cevallos, M. J., & Naranjo, A. (2019). Seguridad de la información en las entidades públicas ecuatorianas: un análisis desde la normativa legal. Revista de Derecho y Tecnología, 12(1), 45-68.

Chang, J. E. (2020). Análisis de ataques cibernéticos hacia el Ecuador. Revista Científica Aristas, 18-27.

Espinosa, J. A., & Salazar, C. (2022). La seguridad de la información en las instituciones públicas ecuatorianas: un análisis de las amenazas y vulnerabilidades. Revista de Ciencias de la Computación e Informática, 20(1), 105-120.

García, F., & López, J. (2019). La seguridad de la información como pilar fundamental en la gestión de entidades gubernamentales. Revista de Gestión Pública, 11(2), 67-82.

Gashgari, G., Walters, R., & Wills, G. (2017). A Proposed Best-practice Framework for Information Security Governance. Informatics. https://consensus.app/papers/proposed-bestpractice-framework-information-security-gashgari/1cabe0a2a73d5588bdda75a2d4edeebb/

Gómez, A., & Vargas, E. (2022). Importancia de implementar buenas prácticas en seguridad de la información en entidades gubernamentales. Revista de Tecnología y Gobierno, 8(2), 112-125.

Gómez, L. (2022). La investigación en seguridad de la información en América Latina: Un análisis bibliométrico. Revista de Ciencias Sociales, 25(4), 123-145.

Herrera, M. 2023). Ciberseguridad en el sector público ecuatoriano: Percepción del riesgo y medidas de protección. Tesis de Grado, Universidad Central del Ecuador, Quito, Ecuador.

Loor, J.L., Mera, J.A., Cedeño, H.F., & Vega, K.M. (2019). Análisis de la gestión de riesgos en las unidades de tecnología de la información de las instituciones públicas de manabí-ecuador.

Mendoza Armijos, H. E. (2021). Nuevos desafíos en la contratación de personal: cómo la evolución del proceso de reclutamiento está transformando el mercado laboral. *Journal of Economic and Social Science Research*, *1*(3), 54–67. https://doi.org/10.55813/gaea/jessr/v1/n3/37

Muyón, C., Guarda, T., Vargas, G., & Quiña, G. N. (2019). Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador. Revista Ibérica de Sistemas e Tecnologías de Información , (E18), 310-317.

Naranjo Armijo, F. G., & Barcia Zambrano, I. A. (2021). Efecto económico de la innovación en las PYMES del Ecuador. *Journal of Economic and Social Science Research*, *1*(1), 61–73. https://doi.org/10.55813/gaea/jessr/v1/n1/21

Navarrete, Y., & Ignacio, Á.S. (2018). Propuesta de controles de seguridad de la información desde el enfoque de protección de datos personales para los entes gubernamentales del ecuador que tienen implementado la estrategia de gobierno en línea.

Ochoa, NVV, Álvarez, M. Á. M. y Manzano, RLM (2024). Implementación de medidas de seguridad y principio de conservación de datos según la ley orgánica de protección de datos personales en instituciones públicas de Babahoyo, Ecuador. Dilemas contemporáneos: Educación, Política y Valores.

Pérez Arias, A. (2022). Quality in Health Services and its Challenge in the Ecuadorian Reality. Journal of Quality in Health Care & Economics. https://consensus.app/papers/quality-health-services-challenge-ecuadorian-reality-arias/a2262c58491a5d948cbbe6f41b3efe48

Pérez, M. (2023). Desafíos de la seguridad de la información en las instituciones públicas ecuatorianas. Revista de Seguridad Informática, 15(2), 45-58.

Pérez, R. (2023). La seguridad de la información en las instituciones públicas es crucial en la era digital. Revista de Seguridad Informática, 15(3), 45-58.

Puyol-Cortez, J. L., & Mina-Bone, S. G. (2022). Explorando el liderazgo de los profesores en la educación superior: un enfoque en la UTELVT Santo

Domingo. *Journal of Economic and Social Science Research*, *2*(2), 16–28. https://doi.org/10.55813/gaea/jessr/v2/n2/49

Ramírez, J. (2022). Ciberseguridad en el sector público ecuatoriano: Análisis de la situación actual y propuestas de mejora. Tesis de Maestría, Universidad de las Américas, Quito, Ecuador.

Ramos, SAC y Sánchez, DX (2023). La protección de datos de carácter personal frente al delito de interceptación ilegal de datos. Código Científico Revista de Investigación , 4 (E2), 984-1023.

Rodríguez, L., & Mendoza, S. (2021). Relevancia de la protección de datos en el contexto ecuatoriano: un enfoque en la seguridad de la información. Revista de Políticas Públicas, 12(4), 78-91.

Ronquillo, L.A., Izquierdo, J.L., ToapantaToapanta, S.M., Madeleine, Gallegos, L.E., Alberto, & Zezzatti, O. (2021). Articulo académico previo a la obtención del título de ingeniera de sistemas carrera: ingeniería de sistemas tema: “analysis for the adoption of security standards to improve the management of securities in public organizations” autora alvarado ronquillo madeleine lilibeth.

Sánchez, P., & Cevallos, M. (2020). Justificación de la inversión en seguridad de la información en el sector público: análisis de costos y beneficios. Revista de Administración Pública, 49(1), 30-45.

Toapanta Toapanta, S. M., Prado Sánchez, M. A., Barona Valencia, D. W., & Mafla Gallegos, L. E. (2019). An Approach of Models of Information Technologies Suitable to Optimize Management in a Public Organization of Ecuador. En 2019 Third World Conference on Smart Trends in Systems Security and Sustainability (WorldS4) (pp. 207-214). https://consensus.app/papers/approach-models-information-technologies-suitable-toapanta/29f6c8d97b77520db8528dd49dc8be7d/

Varela, R.F., Morales Carrillo, J.J., Zambrano Solórzano, L.E., & Ganchozo Lucas, M. (2022). Uso de las Tecnologías de la Información y su aporte a la calidad de servicio en instituciones públicas. Revista Científica Sinapsis.

Yuquipa, CXZ, Urgilés, CHF, Urgilés, CMF, Zenteno, JAC y Cárdenas, DPA (2023). Análisis del nivel de cumplimiento de las Políticas de Seguridad de la Información de los GAD's Cantonales Cañar, El Tambo y Suscal. Pro Ciencias: Revista de Producción, Ciencias e Investigación , 7 (49), 120-138.