RELIGACIÓN
REVISTA

Modelo de madurez de seguridad de información de Sistemas Integrales de Gestión de Riego y Drenaje

Information Security Maturity Model for Integrated Irrigation and Drainage Management Systems

Jennifer Jomaira Loayza Castro, Daniel Jacobo Andrade Pesántez

Resumen

En un contexto global de creciente digitalización, la protección de los datos personales y la gestión segura de la información se han convertido en ejes fundamentales para garantizar la confianza ciudadana, la transparencia institucional y el cumplimiento normativo. En Ecuador, la aplicación de la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) enfrenta aún limitaciones en su implementación práctica, especialmente en los Gobiernos Autónomos Descentralizados (GAD), donde los sistemas informáticos carecen de marcos integrales de gestión de seguridad. Ante esta problemática, la presente investigación tuvo como objetivo diseñar un modelo de madurez aplicado a la gestión de seguridad de la información para el Sistema Integral de Gestión de Riego y Drenaje del GAD Provincial de El Oro, alineado con la LOPDP, la norma ISO/IEC 27001:2022 y el Esquema Gubernamental de Seguridad de la Información (EGSI) en su versión 3, utilizando la integración del modelo de madurez de capacidades (CMMI por sus siglas en Inglés), con un diseño transversal de investigación se permitió durante un periodo de tiempo, estudiar una muestra delimitada geográfica y sistemática de 12 personas, bajo un enfoque mixto, que emplearon tres instrumentos: el primero, una lista de verificación sobre los controles de la ISO/IEC 27001:2022, el segundo, una encuesta aplicada al personal técnico y administrativo, y tercero, entrevistas a persona por perfiles profesionales. Los resultados indicaron un bajo nivel de cumplimiento y conocimiento de la LOPDP (niveles 1 y 2 del CMMI) del modelo guía, caracterizados por una incipiente etapa inicial de implementación de un EGSI, continuando, con una falta de documentación metodológica así como la escasez de políticas institucionales que integralmente rijan la seguridad de la información, terminando, con la ausencia de capacitación y formación al personal institucional, se detectaron también, deficiencias en control de accesos, gestión de riesgos, respuesta a incidentes y capacitación del personal. Estos hallazgos reflejan una limitada articulación entre la LOPDP, el EGSI v3, el CMMI y los procesos internos. En este sentido, se logra identificar las falencias que tiene el sistema de riego, la reciente inserción institucional en materia de la LOPDP. El modelo propuesto pretende ser una herramienta estratégica para mejorar la gestión de seguridad de la información en la institución cuidando aspectos técnicos, legales y administrativos que promuevan la confidencialidad, integridad y disponibilidad de los datos. Así mismo, plasma un aporte metodológico replicable en otros sistemas informáticos de la institución. Por último, abre caminos a futuras investigaciones orientadas a verificar los niveles de madurez de sistemas informáticos, así también, fomenta alternativas de implementación del EGSI para los GAD's y posibilita el desarrollo de investigaciones o auditorías en la gestión de la ciberseguridad pública.

Palabras clave: datos; personales; sistemas; riego; drenaje.

Jennifer Jomaira Loayza Castro
Universidad Católica de Cuenca | Cuenca | Ecuador | jennifer.loayza.46@est.ucacue.edu.ec
https://orcid.org/0009-0003-6885-941X
Daniel Jacobo Andrade Pesántez
Universidad Católica de Cuenca | Cuenca | Ecuador | dandradep@ucacue.edu.ec
https://orcid.org/0000-0003-0586-4038

http://doi.org/10.46652/rgn.v11i49.1589
ISSN 2477-9083
Vol. 11 No. 49, enero-marzo, 2026, e2601589
Quito, Ecuador

Enviado: julio 30, 2025
Aceptado: septiembre 04, 2025
Publicado: noviembre 26, 2025
Publicación Continua

Abstract

In a global context of increasing digitalization, the protection of personal data and the secure management of information have become fundamental pillars to ensure public trust, institutional transparency, and regulatory compliance. In Ecuador, the implementation of the Organic Law on Personal Data Protection (LOPDP, 2021) still faces limitations in its practical application, particularly within Decentralized Autonomous Governments (GADs), where information systems lack comprehensive information security management frameworks. In response to this issue, the present research aimed to design a maturity model applied to information security management for the Integrated Irrigation and Drainage Management System of the Provincial GAD of El Oro, aligned with the LOPDP, ISO/IEC 27001:2022, and the Governmental Information Security Scheme (EGSI), version 3. The study integrated the Capability Maturity Model Integration (CMMI) framework and adopted a cross-sectional research design, allowing for the analysis of a geographically and systematically delimited sample of 12 participants over a defined period. A mixed-methods approach was employed using three instruments: first, a checklist based on the ISO/IEC 27001:2022 controls; second, a survey administered to technical and administrative personnel; and third, interviews conducted with professionals according to their profiles. The results revealed a low level of compliance and awareness of the LOPDP (corresponding to levels 1 and 2 of the CMMI reference model), characterized by an incipient initial stage in the implementation of an EGSI, a lack of methodological documentation, and a scarcity of institutional policies that comprehensively govern information security. Additionally, there was an absence of institutional training and awareness programs, as well as deficiencies in access control, risk management, incident response, and staff training. These findings reflect a limited articulation among the LOPDP, EGSI v3, CMMI, and internal institutional processes. In this regard, the study identifies key weaknesses within the irrigation system and highlights the institution's recent adoption of the LOPDP framework. The proposed model is intended to serve as a strategic tool to enhance information security management within the institution, addressing technical, legal, and administrative aspects that promote data confidentiality, integrity, and availability. Moreover, it provides a methodological contribution that can be replicated in other institutional information systems. Finally, it opens avenues for future research aimed at assessing the maturity levels of information systems, promoting alternatives for EGSI implementation across GADs, and fostering the development of studies or audits related to public cybersecurity management.

Keywords: data; personal; systems; irrigation; drainage.

Introducción

En un entorno global caracterizado por la acelerada digitalización de los servicios y la creciente dependencia de las Tecnologías de la Información (TI), la gestión segura de los datos personales constituye un eje estratégico para garantizar la confianza ciudadana, la eficiencia institucional y el cumplimiento normativo. Tanto en Europa como en América Latina se han establecido marcos regulatorios para fortalecer la soberanía digital y la protección de la privacidad (Barros et al., 2025).

El Reglamento General de Protección de Datos (GDPR) en la Unión Europea ha marcado un precedente internacional, influyendo en la formulación de legislaciones nacionales en países como Brasil, Argentina, México y Colombia. Sin embargo, la región latinoamericana enfrenta aún desafíos significativos en materia de implementación, supervisión y concientización ciudadana en lo que se refiere a la protección de los datos del usuario (Villacres, 2024).

En Ecuador, la promulgación de la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021), representó un avance sustantivo hacia la consolidación de un marco jurídico que garantice

los derechos de los titulares y establezca obligaciones claras para quienes gestionan información personal. No obstante, diversos estudios académicos y técnicos, tales como: Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales: ¿Tendencia en América Latina? (Albornoz, 2022), Responsabilidad médica administrativa, Manejo de datos personales relativos a la salud, Ecuador, 2023 (Heredia & Santacruz, 2023), 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 (Vinueza et al., 2024), han identificado que la aplicación de esta normativa sigue siendo incipiente, especialmente en instituciones públicas descentralizadas y en sistemas importantes de servicios públicos. Dichas brechas generan riesgos de vulneración de la confidencialidad, integridad y disponibilidad de la información, pilares fundamentales de la seguridad de la información (ISO 27001:2022).

Figura 1. Pilares de seguridad de la Información

Fuente: elaboración propia

Según el reporte n° 10 AVANCE DE LA IMPLEMENTACIÓN del Esquema Gubernamental de Seguridad de la Información (EGSI) (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2022) muestra el porcentaje total de avance de cumplimiento de 112 instituciones de la Administración Pública Central en la implementación de un esquema de gestión de seguridad de la información en las instituciones públicas. El problema se acentúa en el ámbito de los Gobiernos Autónomos Descentralizados (GAD), responsables de gestionar datos sensibles vinculados a servicios comunitarios y territoriales. En particular, el Gobierno Autónomo Descentralizado Provincial de El Oro carece de un modelo robusto de gestión de la seguridad de la información que articule políticas, procesos y controles alineados con la LOPDP y estándares internacionales (Gallardo, 2018). Esta situación se refleja en sistemas informáticos institucionales especialmente en los más críticos como el Sistema Integral de Gestión de Riego y Drenaje, que contiene la información de los usuarios de los sistemas de dotación de agua (riego) y mantenimiento de

los suelos de productividad agrícola (drenaje); el sistema está dividido en 6 módulos: Módulo Catastro De Usuarios De Riego, Módulo De Cálculo De Consumo De Agua, Módulo De Emisión Y Recaudación, Modulo Administrativo De Trámite De Usuario, Administración y Módulo GIS - Online que concierne a los cantones: Machala, El Guabo, Pasaje y Santa Rosa.

La ausencia de medidas estandarizadas de seguridad en el sistema integral expone a la institución a riesgos de ciberataques, interrupciones importantes en la operatividad, accesos no autorizados y pérdida de información sensible, comprometiendo derechos ciudadanos y la continuidad de la operación (Vinueza et al., 2024).

La literatura académica reciente ha abordado casos similares en sectores educativos (Guamán, 2024) y en el gobierno electrónico ecuatoriano, evidenciando que las principales vulnerabilidades derivan de la falta de cultura organizacional en seguridad, políticas obsoletas y ausencia de marcos de gestión basados en normas internacionales como ISO 27001. Esta norma establece lineamientos para implementar un Sistema de Gestión de Seguridad de la Información (SGSI), estructurado sobre el ciclo de mejora continua Planificar-Hacer-Verificar-Actuar (PDCA) (Muyón et al., 2019), lo que permite garantizar la confidencialidad, integridad y disponibilidad de los datos en cualquier tipo de organización. Sin embargo, aún existen vacíos de aplicación en entornos locales y subnacionales, donde no se han desarrollado metodologías específicas que adapten el marco ISO 27001 a sistemas de gestión operativa como el sistema integral de riego y drenaje.

En este sentido, también se ha analizado e incorporado los modelos de madurez como herramientas estratégicas para evaluar el grado de desarrollo de los procesos organizacionales. Por tanto, también se ha analizado los modelos de madurez como herramientas estratégicas para evaluar el grado de desarrollo de los procesos institucionales. Por un lado se tiene COBIT que de forma general se enfoca en la gobernanza TI sin embargo el modelo NIST CSF (Verdugo, 2023), se encamina en la gestión de riesgos cibernéticos mientras que CMMI se centra en la mejora continua de procesos siendo un referente metodológico aplicable a la seguridad de la información; el cual tiene mayor aplicabilidad al objeto de estudio permitiendo medir la madurez de los procesos en cinco niveles (Inicial, Gestionado, Definido, Cuantitativamente Gestionado y Optimizado) (ver figura 2), orientando a las organizaciones hacia la mejora continua mediante la evaluación sistemática de sus capacidades (Morales et al., 2014).

Figura 2. Niveles de madurez, siguiendo la lógica del CMMI (Modelo Integrado de Madurez de Capacidades)

Nivel	Denominación	Descripción general	Objetivo principal
Nivel 1: Inicial (Reactivo)	Ausencia de políticas formales. La gestión de seguridad depende de esfuerzos individuales.	Se gestionan incidentes de manera reactiva sin documentación ni monitoreo.	Reconocer la existencia de vulnerabilidades y la necesidad de controles formales.
Nivel 2: Gestionado (Formalización básica)	Existencia de políticas iniciales de seguridad y controles parciales.	Se definen roles, responsabilidades y se implementan medidas básicas de protección de datos personales.	Establecer políticas, procedimientos y roles básicos.
Nivel 3: Definido (Estandarizado)	Políticas y procesos institucionalizados, documentados y socializados.	Se gestiona la seguridad de manera coordinada, con auditorías internas y capacitación regular.	Alinear la gestión institucional con la LOPDP y la ISO/IEC 27001.
Nivel 4: Gestionado Cuantitativamente	Procesos medidos y controlados mediante indicadores.	Se usan métricas para evaluar la eficacia de los controles, riesgos y cumplimiento.	Implementar una gestión basada en datos y evidencias.
Nivel 5: Optimizado (Mejora continua)	Cultura institucional de seguridad y cumplimiento continuo.	Se promueve la innovación en la protección de datos y la mejora constante del SGSI.	Lograr un sistema resiliente y sostenible de seguridad de la información.

Fuente: elaboración propia

De este modo, la integración del CMMI como modelo de madurez guía en la presente investigación permitió establecer niveles de avances en la implementación de políticas, controles y procesos de seguridad de la información dentro del Sistema Integral de Gestión de Riego y Drenaje.

En este contexto, el presente artículo tiene como objetivo diseñar un modelo de madurez aplicado a la gestión de seguridad de la información para el Sistema Integral de Gestión de Riego y Drenaje del GAD Provincial de El Oro, alineado en la normativa nacional vigente (LOPDP), en la norma internacional ISO/IEC 27001:2022 y guiado en el EGSI en su versión 3; a partir del análisis de las políticas de ciberseguridad relacionados a la privacidad de los datos personales que tuvieren en el Gobierno Autónomo Descentralizado Provincial de El Oro; demostrando la vinculación que tienen las normativas en la figura 3.

Figura 3. Dominios del CMMI adaptadas a la ISO 27001

Área de Proceso	Descripción	Norma / Marco de referencia
1. Gestión de Políticas y Cumplimiento	Desarrollo y aplicación de políticas de seguridad, conforme a LOPDP y EGSI.	ISO 27001: cláusulas 5 y 6
2. Gestión de Riesgos de Seguridad	Identificación, análisis y mitigación de riesgos.	ISO 27005, EGSI v3
3. Control de Accesos y Autenticación	Implementación de medidas técnicas y administrativas para el acceso seguro al sistema.	ISO 27002:2022 – Control 5.15
4. Gestión de Incidentes y Continuidad Operativa	Registro, respuesta y lecciones aprendidas ante incidentes de ciberseguridad.	ISO 22301, LOPDP art. 45
5. Protección de Datos Personales	Cumplimiento de principios de tratamiento, consentimiento y derechos ARCO.	LOPDP (2021)
6. Capacitación y Concienciación	Formación del personal en buenas prácticas de seguridad.	ISO 27001, control 6.3
7. Monitoreo, Auditoría y Mejora Continua	Seguimiento del SGSI, revisión de métricas y retroalimentación.	Ciclo PDCA – ISO 27001

Fuente: elaboración propia

Por tanto, se busca responder a preguntas de investigación orientadas a: ¿cuáles son las políticas y normativas de ciberseguridad adoptadas por el GADPEO para garantizar la protección de datos personales en el sistema?, ¿cuáles son las principales vulnerabilidades y riesgos presentes en el sistema integral?

Además, la relevancia de este estudio radica en que sus resultados no solo permitirán fortalecer la gestión de seguridad de la información institucional del sistema de riego en el GAD Provincial de El Oro, sino que también se espera aportar evidencia metodológica para replicar en otros sistemas informáticos de la institución; así como también generar un marco de referencia para otros GAD del Ecuador que dispongan de un sistema informático de características similares que enfrenten problemáticas en la implementación de un modelo de gestión de seguridad de la información. Asimismo, la propuesta contribuye a la literatura sobre ciberseguridad en el sector público al integrar marcos regulatorios nacionales con estándares internacionales, generando un modelo replicable y ajustado al contexto ecuatoriano.

Además, es necesario reconocer que la falta de cultura en seguridad de la información en los gobiernos locales responde también a limitaciones de recursos técnicos, financieros y humanos. La ausencia de personal especializado, la inexistencia de manuales de procedimiento y la débil articulación entre la normativa nacional y la gestión cotidiana generan escenarios donde la información se administra de manera fragmentada y poco segura. Esta brecha institucional pone en riesgo no solo la protección de los datos personales, sino también la credibilidad y legitimidad de las instituciones públicas frente a la ciudadanía.

Por otra parte, el estudio cobra relevancia en el marco de los compromisos internacionales de Ecuador en materia de gobierno electrónico, transparencia y protección de datos. La implementación de un modelo de gestión de seguridad de la información en sistemas como el de riego y drenaje no solo permitirá cumplir con la LOPDP, sino que también se alinea con estándares internacionales como el GDPR sobre privacidad y protección de datos personales en las Américas. Con ello, se busca fortalecer la interoperabilidad, confianza digital y sostenibilidad institucional en el uso de las tecnologías de la información (Guamán, 2024).

Este trabajo se propone llenar un vacío en la investigación aplicada en el contexto ecuatoriano: la adaptación de la norma ISO 27001 al sistema informático específico institucional. A diferencia de estudios previos centrados en instituciones educativas o entidades nacionales, este artículo plantea una propuesta metodológica ajustada a la gestión operativa del sistema, con el fin de establecer un marco integral de seguridad que pueda ser replicado y evaluado en distintos sistemas informáticos institucionales y por qué no en escenarios del sector público.

Por último, éste artículo se organiza de la siguiente manera: en la primera sección se presenta la introducción sobre seguridad de la información, normativa ecuatoriana y la norma ISO 27001 así como un breve preámbulo del objetivo del sistema; en la segunda sección se expone la metodología utilizada para el análisis del sistema en estudio; en la tercera se propone el modelo de gestión de seguridad de la información para el Sistema Integral de Gestión de Riego y Drenaje; y en la cuarta sección se discuten los resultados, conclusiones derivadas de la investigación.

Metodología

El presente estudio diseñó un modelo de madurez aplicado a la gestión de seguridad de la información para el Sistema Integral de Gestión de Riego y Drenaje del GAD Provincial de El Oro, alineado con la Ley Orgánica de Protección de Datos Personales y la norma ISO/IEC 27001:2022 y tomando como guía el EGSI, con el fin de fortalecer la protección de datos personales, reducir vulnerabilidades cibernéticas y mejorar la eficiencia institucional del sistema.

El estudio se desarrolló bajo un enfoque aplicado, con un diseño de investigación de tipo transversal y alcance descriptivo, puesto que se buscó analizar y proponer un modelo de madurez práctico de gestión de seguridad de la información en un momento específico del tiempo. La elección de este diseño permitió identificar vulnerabilidades, revisar el grado de cumplimiento normativo y plantear lineamientos de mejora continua al modelo de gestión de seguridad de la información generado en alineación tanto a la Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) como a la norma internacional ISO/IEC 27001:2022. Esta investigación es coherente al contexto institucional, ya que no sólo consistió en el análisis de la situación actual ni en la medición de los niveles alcanzados (ver tabla 1), sino más bien busca generar un aporte referencial para su futura implementación a otros sistemas.

Tabla 1. Análisis de madurez (CMMI) aplicado en el Sistema de Riego y Drenaje

Área de Proceso	Nivel Actual (Evaluado)	Evidencia	Brecha Principal
Políticas y cumplimiento	2	Existen lineamientos dispersos	Falta política integral SGSI
Gestión de riesgos	2	No hay matriz formal	No se actualizan riesgos
Control de accesos	3	Roles definidos parcialmente	Falta autenticación robusta
Incidentes y continuidad	1	No hay plan de respuesta formal	Falta plan de contingencia
Protección de datos personales	2	Desconocimiento de LOPDP	Capacitación insuficiente
Capacitación y concienciación	2	Charlas aisladas	Falta plan de formación anual
Monitoreo y mejora	1	Sin indicadores ni auditorías	No hay seguimiento periódico

Fuente: elaboración propia

El uso del CMMI en el desarrollo metodológico investigativo como marco guía para la estructuración del modelo propuesto permitió establecer niveles evolutivos de madurez dentro del desarrollo institucional en materia de seguridad de la información en el sistema integral y aplicabilidad de la LOPDP. Su aplicación metodológica se realizó transversalmente en la identificación de brechas, categorización de controles, cumplimiento de normativa legal y priorización de acciones de mejora. Así, cada nivel del CMMI fue adaptado al contexto del GAD Provincial de El Oro, integrando los requisitos técnicos de la ISO/IEC 27001:2022, los artículos de la LOPDP y el esquema vigente gubernamental lo cual posibilitó la formulación de un modelo de madurez contextualizado al sistema de estudio. El uso del CMMI, por tanto, no se limitó a una referencia teórica, sino que sirvió como instrumento analítico para definir indicadores de avance,

criterios de evaluación y mecanismos de retroalimentación para su adaptación a otros sistemas informáticos institucionales

La investigación se llevó a cabo en el GAD Provincial de El Oro, específicamente en la Dirección de Recursos Hídricos. El objeto de estudio estuvo constituido por el Sistema Integral de Gestión Riego y Drenaje, que es un sistema informático que centraliza procesos sensibles como el catastro, la gestión de fichas técnicas, el control de turnos de riego, la administración de usuarios, la gestión de contratos y la transferencia de dominios. La selección de este sistema respondió a su relevancia crítica para la prestación de servicios a la ciudadanía y a la alta exposición de datos personales vinculados a usuarios finales y funcionarios.

Para realizar el proceso investigativo, se considera que inicialmente es fundamental conocer el nivel de conocimiento que los usuarios del sistema integral tienen respecto a la Ley Orgánica de Protección de Datos Personales (LOPDP), la Norma ISO/IEC 27001:2022 y el EGSI dado por el Ministerio de Telecomunicaciones, por tanto, previo los permisos respectivos se procedió a aplicar 3 instrumentos de recolección de información. Se considera que la población de interés estuvo conformada por funcionarios del GAD con responsabilidades y perfiles directos en la administración del sistema integral y en la supervisión de procesos relacionados con el sistema. Se incluyó tanto a personal técnico, con perfil de inspectores, encargados de la operación de la plataforma como a personal administrativo-recaudador vinculado con la gestión y la planificación institucional adicionalmente se incluyó a los funcionarios GIS, con perfil de analistas. Se excluyó a funcionarios sin acceso al sistema informático, así como a personal temporal o en capacitación, con el fin de garantizar la pertinencia de las respuestas y la confiabilidad de la información obtenida.

Por proximidad geográfica y facilidad de acceso el tamaño muestral se definió mediante un muestreo no probabilístico por conveniencia, tomando en consideración que el total de la población es 50 funcionarios que usan el sistema de gestión de riego y drenaje por lo que se considera la muestra de 12 participantes clave. Este procedimiento permitió acceder a personal con experiencia directa en el manejo de los sistemas y en la aplicación de políticas de seguridad de la información. Aunque esta técnica limitó la generalización de los hallazgos para los demás sistemas institucionales, aseguró la obtención de información relevante y específica para el caso de estudio, sin embargo, crea un marco de referencia para su aplicabilidad en los demás sistemas informáticos institucionales.

En aplicación de la LOPDP, se procedió a analizar y explicar en algunos casos el consentimiento informado a los participantes; previo a la aplicación de instrumentos para la recolección de datos, los 3 instrumentos usados fueron: en primer lugar, se utilizó una lista de chequeo basada en los 93 controles conforme a la ISO/IEC 27001: 2022, la cual permitió evaluar el nivel de conocimiento y cumplimiento de buenas prácticas en seguridad de la información. En segundo lugar, se aplicó una encuesta dirigida al personal técnico, administrativo-recaudador y a los técnicos GIS del sistema validada por el Jefe de la Unidad Tics, diseñado para medir el grado de conocimiento y aplicación de los principios de la LOPDP en sus actividades cotidianas en el uso del sistema. Finalmente, se desarrolló una entrevista aplicada a un funcionario por perfil, inspectores, técnicos

GIS, secretaria-recaudador, orientada a profundizar en los criterios de gestión, la identificación de riesgos y las estrategias institucionales de protección de datos.

Considerando que la hipótesis indica que: *La implementación efectiva de las políticas de ciberseguridad en las entidades gubernamentales de Ecuador influye positivamente sobre la privacidad de los datos personales, fortaleciendo el cumplimiento de la Ley de Protección de Datos Personales en el GADPEO;* se determina que las variables analizadas se agruparon en tres categorías: (a) nivel de cumplimiento de la LOPDP (VD), medido en una escala ordinal de bajo a alto; (b) nivel de madurez en la gestión de seguridad de la información (VD), aplicado a la gestión de seguridad; y (c) la identificación de brechas en políticas, procedimientos y controles (VI), clasificadas de manera nominal en categorías como ausencia de políticas, controles insuficientes o deficiencias en la capacitación. Esta combinación de variables permitió obtener una visión integral del estado de la gestión de la información en la institución.

Para ejecutar el procedimiento de recolección de datos con los instrumentos mencionados se socializó el consentimiento informado a todos los participantes, garantizando la confidencialidad y el anonimato de la información recopilada. Adicionalmente se tomó como fuentes de información secundaria la revisión documental de varios artículos, revistas, tesis, leyes, esquemas gubernamentales, guías y diseños que convergieron en tomar como base fundamental el EGSI conforme a la normativa vigente en el Acuerdo Ministerial No. 0003-2024 (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2024).

Dentro del estudio se presentó limitaciones relacionadas con el sesgo de selección, derivado del muestreo no probabilístico lo cual fue superado con la determinación de la población objetivo, al conocer la base de los usuarios del sistema y la muestra a ser seleccionada, lo que impidió generalizar los resultados a todos los sistemas informáticos institucionales puesto que la cantidad total de usuarios por sistema varía en función de las direcciones que los usan; sin embargo se acentúa el antecedente dentro de la institución. Una limitación técnica adicional fue la dependencia de la disponibilidad del personal para participar en el estudio debido a las ocupaciones propias del perfil. Estas limitaciones fueron reconocidas y abordadas, reduciendo su impacto en la validez de los hallazgos.

Finalmente se puede indicar que la metodología adoptada permitió obtener una visión integral y aplicada sobre el estado de la seguridad de la información en el sistema objeto de estudio del GAD Provincial de El Oro, analizando lineamientos normativos internacionales y nacionales. El uso combinado de encuestas, entrevistas y listas de chequeo basadas en ISO 27001:2022 posibilitó identificar tanto las fortalezas como las brechas en la gestión institucional, proporcionando una base empírica sólida para que impulse el diseño del modelo de gestión de seguridad de la información propuesto en este estudio para el sistema integral de riego y drenaje.

Resultados

El análisis realizado en el Sistema Integral de Gestión de Riego y Drenaje del GAD Provincial de El Oro evidenció un bajo nivel de cumplimiento de la Ley Orgánica de Protección de Datos Personales. Las encuestas aplicadas al personal mostraron un conocimiento limitado sobre principios de protección de datos y gestión de la seguridad de la información. La lista de chequeo basada en la ISO/IEC 27001:2022 identificó deficiencias en políticas de acceso, clasificación de la información y controles de seguridad. Asimismo, las entrevistas confirmaron la ausencia de procedimientos estandarizados, lo que incrementa la exposición a vulnerabilidades cibernéticas y riesgos operativos.

Por tanto, se identificó que para establecer un modelo de madurez de seguridad de información para el sistema integral de riego y drenaje es importante realizar a primera instancia un reconocimiento de la institución y en especial de la Dirección que usa el sistema integral proponiendo establecer un levantamiento de información general.

Seguidamente, se procedió a realizar el respectivo análisis de riesgo determinando que el Sistema Integral es de importancia crítica dentro de la institución puesto que su fallo representa un impacto significativo en los objetivos institucionales, operacionales y financieros; por lo que los riesgos a los que está expuesto el sistema van desde lo estratégico hasta lo político como se representa en la figura 4.

Figura 4. Identificación del riesgo

R1	Riesgo Estratégico
R2	Riesgo de Imagen
R3	Riesgo Operativos
R4	Riesgos Financieros
R5	Riesgos Incumplimiento
R6	Riesgos de Tecnologia
R7	Riesgos Legales
R8	Riesgos Políticos

Fuente: elaboración propia

Al analizar el sistema integral se pudo determinar los siguientes activos circundantes al mismo, que se plasmaron en la figura 5 conforme al formato referencial dado en el EGSI v2 del Ministerio de Telecomunicaciones:

Figura 5. Activos de Información identificados

Activos de Información Identificados			
N°	**Tipo**	**Activo**	**Descripción**
1	Información física	Documentación	Corresponde a todos los documentos físicos, como actas, acuerdos, circulares, informes, planes, entre otros.
2	Información digital	Documentación	Corresponde a este tipo los archivos de datos digitales, archivados electrónicamente: Correos electrónicos, Copias de seguridad, Base de datos, entre otros.
3	Software	Sistema Integral	Corresponde al Software de aplicación, software del sistema, herramientas de desarrollo y utilidades, entre otros.
4	Software	Sistemas Operativos	Corresponde al sistema operativo que usan los equipos de cómputo de los funcionarios.
5	Hardware	Servidores, equipos de computo	Corresponde a todos los dispositivos y periféricos en lo que se apoya el sistema integral.
6	Servicios	Sistema Integral	Corresponde a los servicios tecnológicos que ayudan a la administración o flujo de información generada por los procesos de la institución, tales como el correo electrónico, otros softwares de la institución.
7	Humanos	Usuarios del sistema	Corresponde a los funcionarios que usan el sistema
8	Humanos	Ciudadanía	Corresponde a la ciudadanía en general que se benefician del servicio de riego y drenaje
9	Infraestructura	Red LAN	Corresponde a la infraestructura que compone la red local

Fuente: elaboración propia

Una vez examinado el sistema integral se identifica, conforme al catálogo de amenazas y vulnerabilidades comunes propuesto por el EGSI v3 se identifica aquellas que también se tienen en la institución como se detalla en la Tabla 2.

Tabla 2. Listado de Controles EGSI v3.0 asociados a la LOPDP

Listado de Controles EGSI v3.0 asociados a la LOPDP									
Artículo LOPDP	**N° Control EGSI v3**	**Nombre del Control**	**Tipo de control**	**Propiedades de seguridad información**	**Conceptos de ciberseguridad**	**Capacidades operativas**	**Dominio de seguridad**	**Amenaza asociada**	**Vulnerabilidad relacionada**
Art. 37. Seguridad de datos personales	1.7	Inteligencia de amenazas	#Preventivo #Detectivo #Correctivo	CID	#Identificar #Detectar #Responder	#Gestión_de_Amenazas_ y Vulnerabilidades	#Defensa #Resiliencia	Ingeniería Social	Formación en seguridad insuficiente
Art. 37. Seguridad de datos personales	1.12	Clasificación de la información	#Preventivo	CID	#Identificar	#Información_protección	#Protección #Defensa	Tratamiento sin autorización expresa de datos personales	Procedimientos para el manejo de información clasificada no desarrollados
Art. 37. Seguridad de datos personales	1.16	Gestión de Identidad	#Preventivo	CID	#Proteger	#Gestión_de_identidad_ acceso	#Protección	Robo de identidad o credenciales digitales	Proceso formal de autorización de información disponible públicamente no desarrollado
Art. 37. Seguridad de datos personales	1.17	Información de autenticación	#Preventivo	CID	#Proteger	#Gestión_de_identidad_ acceso	#Protección	Corrupción de datos	Poca conciencia de seguridad

Listado de Controles EGSI v3.0 asociados a la LOPDP									
Artículo LOPDP	**N° Control EGSI v3**	**Nombre del Control**	**Tipo de control**	**Propiedades de seguridad información**	**Conceptos de ciberseguridad**	**Capacidades operativas**	**Dominio de seguridad**	**Amenaza asociada**	**Vulnerabilidad relacionada**
Art. 37. Seguridad de datos personales	1.18	Derechos de acceso	#Preventivo	CID	#Proteger	#Gestión_de_identidad_ acceso	#Protección	Robo de identidad o credenciales digitales	Poca conciencia de seguridad
Art. 44. Acceso a datos personales para atención a emergencias e incidentes informáticos	1.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	#Correctivo	CID	#Responder #Recuperar	#Gestión_de_eventos_ de_seguridad_de la_Información	#Defensa	Violación de la mantenibilidad del sistema de información	Procedimientos para informar debilidades de seguridad ineficaz en su implementación
Art. 44. Acceso a datos personales para atención a emergencias e incidentes informáticos, Art. 46. Notificación de vulneración de seguridad al titular	126	Respuesta a incidentes de seguridad de la información	#Correctivo	CID	#Responder #Recuperar	#Gestión_de_eventos_ de_seguridad_de_ la_Información	#Defensa	Violación de la mantenibilidad del sistema de información	Falta de copias de seguridad o copias de seguridad incompletas
Art. 43. Notificación de vulneración de seguridad	4.8	Gestión de vulnerabilidades técnicas	#Preventivo	CID	#Identificar #Proteger	#Gestión_de_amenazas_ y_vulnerabilidades	#Gobernanza_ y_Ecosistema#Protección #Defensa	Violación de la mantenibilidad del sistema de información	Formación en seguridad insuficiente
Art. 37. Seguridad de datos personales	4.12	Prevención de fuga de datos	#Preventivo #Detectivo	C	#Proteger #Detectar	#Información_protección	#Protección #Defensa	Divulgación de información	Arquitectura de red insegura
Art. 39. Protección de datos personales desde el diseño y por defecto	4.26	Requisitos de seguridad de la aplicación	#Preventivo	CID	#Proteger	#Seguridad_del_sistema_ y_red #Seguridad_aplicación	#Protección #Defensa	Denegación de acciones	Asignación inadecuada de responsabilidades de seguridad de la información

Listado de Controles EGSI v3.0 asociados a la LOPDP									
Artículo LOPDP	**N° Control EGSI v3**	**Nombre del Control**	**Tipo de control**	**Propiedades de seguridad información**	**Conceptos de ciberseguridad**	**Capacidades operativas**	**Dominio de seguridad**	**Amenaza asociada**	**Vulnerabilidad relacionada**
Art. 39. Protección de datos personales desde el diseño y por defecto	4.27	Arquitectura del sistema seguro y principios de ingeniería	#Preventivo	CID	#Proteger	#Seguridad_del_sistema_y_red #Seguridad_aplicación	#Protección	Ataque de repetición (ataque de playback), ataque de hombre en el medio	Pruebas de software inexistentes o insuficientes
Art. 39. Protección de datos personales desde el diseño y por defecto	4.28	Codificación Segura	#Preventivo	CID	#Proteger	#Seguridad_del_sistema_y_red #Seguridad_aplicación	#Protección	Corrupción de datos	Especificaciones poco claras o incompletas para desarrolladores
Art. 39. Protección de datos personales desde el diseño y por defecto	4.29	Pruebas de seguridad en desarrollo y aceptación	#Preventivo	CID	#Detectar	#Seguridad_del_sistema_y_red #Seguridad_aplicación #Seguridad_de_información	#Protección	Manipulación de software	Pruebas de software inexistentes o insuficientes
Art. 39. Protección de datos personales desde el diseño y por defecto	4.30	Desarrollo subcontratado	#Preventivo #Detectivo	CID	#Identificar #Proteger #Detectar	#Seguridad_del_sistema_y_red #Seguridad_aplicación #Seguridad_de_las_Relaciones_con_los_proveedores	#Gobernanza_ y_Ecosistema #Protección	Robo de soportes o documentos	Ausencia de personal
Art. 39. Protección de datos personales desde el diseño y por defecto	4.31	Separación de los entornos de desarrollo, prueba y producción	#Preventivo	CID	#Proteger	#Seguridad_del_sistema_y_red #Seguridad_aplicación	#Protección	Falta de recursos	Pruebas de software inexistentes o insuficientes
Art. 39. Protección de datos personales desde el diseño y por defecto	4.33	Información de pruebas	#Preventivo	CI	#Proteger	#Protección_de_la Información	#Protección	Error en uso	Documentación insuficiente o faltante

Fuente: elaboración propia

Así mismo, parte del proceso investigativo para generar un modelo propio de madurez de seguridad de información para el sistema integral de riego y drenaje consistió en realizar varios

cuestionamientos, que mediante la aplicación de los instrumentos de investigación se logró identificar el dominio y el indicar para cada interrogante presentada, por tanto basados en la información de la tablas anteriores se ha construido un modelo para medir el modelo de madurez del sistemas integral tal como se observa en la Tabla 3.

Tabla 3. Preguntas para ver la madurez de seguridad de información

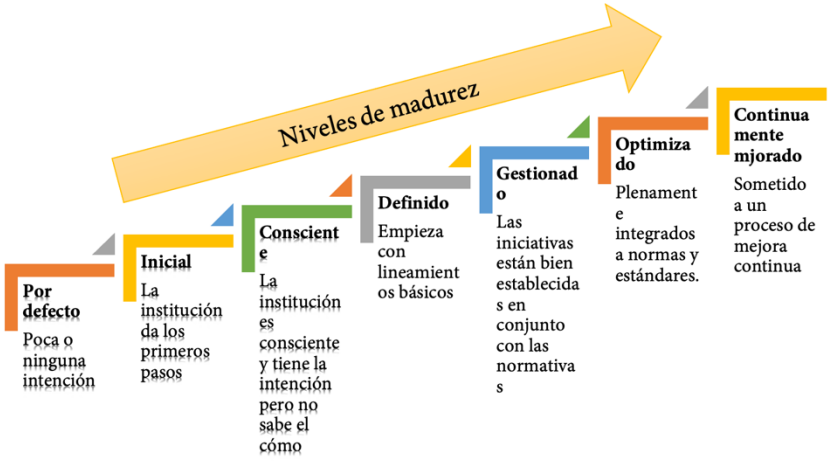
Dominio	Indicador	Pregunta	Respuesta Si/No
Gestión de Seguridad	Políticas de Seguridad	¿Existen políticas de seguridad de la información de aplicación en el sistema de riego?	
Gestión de Seguridad	Políticas de Seguridad	¿Están estas políticas pertinentemente comunicadas?	
Gestión de Seguridad	Políticas de Seguridad	¿Existe un responsable de seguridad de la información institucional?	
Gestión de Seguridad	Políticas de Seguridad	¿La seguridad de las comunicaciones de red es protegida o tienes algún proceso de cifrado?	
Gestión de Seguridad	Concienciación del personal	¿El personal recibe formación periódica en seguridad?	
Gestión de Seguridad	Gestión de activos	¿Los activos de información están inventariados y clasificados?	
Gestión de Seguridad	Gestión de activos	¿Existe las medidas de protección tanto físicas como ambientales al hardware de la infraestructura tecnológica institucional?	
Control de Accesos	Control de usuarios	¿Se controla el acceso según roles y privilegios mínimos?	
Control de Accesos	Control de usuarios	¿Existen controles para la gestión de usuarios y sus respectivos accesos?	
Control de Accesos	Gestión de contraseñas	¿Se aplican políticas de contraseñas seguras y su renovación periódica?	
Protección de Datos	Cifrado de información	¿La información sensible se cifra durante el almacenamiento y transmisión?	
Protección de Datos	Privacidad de datos	¿Se garantiza la protección de datos personales conforme a la normativa?	
Protección de Datos	Privacidad de datos	¿Existe un responsable de protección de datos personales?	
Gestión de Incidentes	Registro de incidentes	¿Se registran y analizan los incidentes de seguridad?	
Gestión de Incidentes	Plan de respuesta ante incidentes	¿Existe un plan documentado de respuesta ante incidentes?	
Gestión de Incidentes	Plan de respuesta ante incidentes	¿Cómo se asegura la continuidad del servicio del sistema integral?	
Gestión de Incidentes	Plan de respuesta ante incidentes	¿Existe una gestión adecuada de los respaldos de información?	
Cumplimiento Legal	Cumplimiento normativo	¿El software cumple con la legislación vigente en materia de seguridad?	
Cumplimiento Legal	Revisión legal periódica	¿Se revisan periódicamente las obligaciones legales y contractuales?	

Dominio	Indicador	Pregunta	Respuesta Si/No
Cumplimiento Legal	Revisión legal periódica	¿Se tiene la respectiva hoja de control del sistema integral?	
Mantenimiento Seguro	Actualización segura	¿Las actualizaciones se aplican de forma controlada y segura?	
Mantenimiento Seguro	Pruebas de seguridad	¿Se realizan pruebas de seguridad antes de la implementación?	
Mantenimiento Seguro	Pruebas de seguridad	¿Se realiza los mantenimientos reglamentarios a efecto de detectar vulnerabilidades en el sistema periódicamente?	
Desarrollo Seguro	Seguridad de información	¿Existió una adecuada gestión de seguridad de la información durante el desarrollo del sistema integral?	
Evaluación de Riesgos	Identificación de amenazas	¿Se identifican amenazas de forma continua?	
Evaluación de Riesgos	Evaluación de impacto	¿Se evalúan los impactos de las vulnerabilidades detectadas?	
Auditoría Interna	Auditorías planificadas	¿Se planifican auditorías internas de seguridad?	
Auditoría Interna	Gestión de hallazgos	¿Se da seguimiento a los hallazgos hasta su resolución?	
Capacitación	Nivel de conocimiento	¿Hay un plan de capacitación y actualización de conocimientos en materia de seguridad de la información a los usuarios del sistema integral?	

Fuente: elaboración propia

El objetivo del modelo de madurez para el sistema integral es identificar el progreso de la gestión de seguridad de la información en el Sistema Integral de Gestión de Riego y Drenaje del GAD Provincial de El Oro, alineado en la normativa nacional vigente (LOPDP), en la norma internacional ISO/IEC 27001:2022 y guiado en el EGSI en su versión 3; por lo que se resalta que después de haber evaluado los diferentes modelos de madurez basados en CMMI, se llegó a la conclusión que no existe un modelo de madurez que se ajuste al sistema institucional por tanto se propone el siguiente tal como se puede apreciar en la Figura 6; cuyo posicionamiento dependerá de las respuestas a la, preguntas mostradas en la Tabla 3 para ver la madurez de seguridad de información para la cual se ha identificado el intervalo porcentual equivalente para cada nivel como se detalla en la Tabla 4 Intervalo porcentual equivalente para cada nivel de madurez.

Figura 6. Modelo de madurez propuesto basado en CMMI



Fuente: elaboración propia

Tabla 4. Intervalo porcentual equivalente para cada nivel de madurez

Nivel	Nombre del Nivel	Descripción	Intervalo porcentual	% de respuestas positivas requeridas	Respuestas positivas esperadas (de 35)	Respuestas negativas (de 35)
1	Por defecto	Poca o ninguna intención de gestión o control de seguridad.	0 – 14 %	0 – 14 %	0 – 5	30 – 35
2	Inicial	La institución da los primeros pasos, pero sin procedimientos formales.	15 – 28 %	15 – 28 %	6 – 10	25 – 29
3	Consciente	La institución es consciente y tiene la intención de mejorar, pero aún no sabe cómo.	29 – 42 %	29 – 42 %	11 – 15	20 – 24
4	Definido	Se empieza a trabajar con lineamientos básicos e infraestructura mínima.	43 – 57 %	43 – 57 %	16 – 20	15 – 19
5	Gestionado	Las iniciativas están bien establecidas en conjunto con las normativas.	58 – 71 %	58 – 71 %	21 – 25	10 – 14
6	Optimizado	Los procesos están plenamente integrados a normas y estándares.	72 – 85 %	72 – 85 %	26 – 30	5 – 9
7	Continuamente mejorado	El sistema está sometido a un proceso de mejora continua.	86 – 100 %	86 – 100 %	31 – 35	0 – 4

Fuente: elaboración propia

Por lo tanto, una vez desarrollado e implementado el modelo de madurez propuesto aplicado a la gestión de la seguridad de la información del Sistema Integral de Riego y Drenaje, se impulsa que este instrumento sea de utilidad para evaluar y fortalecer dicho sistema, además de convertirse en un marco de referencia estratégico que pueda ser replicado y adaptado en los demás sistemas informáticos del Gobierno Autónomo Descentralizado Provincial, de tal manera, que se promueva la gestión homogénea, eficiente y sostenible de la seguridad de la información en toda la institución.

Discusión

El análisis de los resultados obtenidos en el Sistema Integral de Gestión de Riego y Drenaje del GAD Provincial de El Oro evidencia una baja madurez institucional en la gestión de la seguridad de la información, confirmando la hipótesis planteada sobre la existencia de brechas significativas en el cumplimiento de la LOPDP (2021) y la aplicación de la norma ISO/IEC 27001:2022 en un área determinada. Este hallazgo coincide con estudios previos que han señalado que, en Ecuador, la implementación de la LOPDP en instituciones públicas continúa siendo incipiente y fragmentada, especialmente en los Gobiernos Autónomos Descentralizados (Vinueza Ochoa et al., 2024; UISek, 2022).

El limitado conocimiento del personal sobre los principios de protección de datos y la ausencia de políticas estandarizadas confirman que la gestión de seguridad en el GAD Provincial de El Oro se encuentra en un nivel inicial de madurez, equivalente a los niveles 1 o 2 del modelo CMMI adaptado, es decir, con procesos reactivos y no institucionalizados. Este resultado guarda relación con lo expuesto por Gallardo (2020), quien identifica que los gobiernos locales ecuatorianos enfrentan serias dificultades para incorporar marcos normativos internacionales debido a la falta de cultura organizacional en seguridad, escasa asignación presupuestaria y dependencia de actores externos para la gestión tecnológica.

Asimismo, la aplicación de la lista de chequeo basada en la ISO/IEC 27001:2022 permitió identificar deficiencias críticas en controles como la gestión de accesos, clasificación de información, respuesta a incidentes y continuidad operativa. Estas brechas no solo exponen vulnerabilidades técnicas para el sistema integral o para la infraestructura tecnológica, sino que reflejan un vacío estructural en la gobernanza de la seguridad de la información en la institución. En términos comparativos, Martins y Oliveira (2019), plantean que las instituciones públicas tienden a adoptar los marcos regulatorios de protección de datos de manera simbólica o superficial, sin transformarlos a la práctica operativa cotidiana. Este fenómeno se evidencia también en la presente investigación, donde la LOPDP se reconoce de forma normativa, sin embargo, carece de mecanismos en la aplicación efectiva.

Los resultados también permiten establecer una correspondencia directa entre la madurez de aplicabilidad de la LOPDP, la Norma ISO/IEC 27001:2022 y el grado de cumplimiento normativo. En instituciones donde existen manuales, responsables designados y seguimientos internos, el nivel de cumplimiento de la LOPDP tiende a subir proporcionalmente, lo que respalda el planteamiento de Angela Jomaira et al. (2025), quienes resaltan que el fortalecimiento de la cultura en ciberseguridad es determinante para la sostenibilidad institucional y fortalecer la confianza ciudadana en los entornos digitales del GAD Provincial de El Oro.

Un hallazgo relevante identificado en esta investigación es que la desarticulación entre las políticas internas y los estándares internacionales generan esfuerzos duplicados y desalineación estratégica. El reporte del Ministerio de Telecomunicaciones (2022), demuestra esta problemática,

al indicar que sólo 48% de las instituciones públicas evaluadas cumplían parcialmente con el EGSI. En el contexto, la realidad del GAD Provincial de El Oro coincide con la tendencia nacional, mostrando avances limitados y ausencia de mecanismos de evaluación continua.

Otro hallazgo significativo corresponde a la percepción de los funcionarios sobre la seguridad de la información. Las entrevistas demostraron que, aunque existe conciencia sobre la importancia de proteger los datos, persisten prácticas inadecuadas como el uso de contraseñas débiles, almacenamiento de información en medios no cifrados y falta de registro de incidentes. Este resultado coincide con los encontrados por Almache et al. (2024) y Ávila-Coello (2024), donde se menciona que en América Latina los desafíos de implementación de políticas de protección de datos se deben menos a la falta de normativas y más a la carencia de capacitación y sensibilización del personal operativo.

Los resultados más importantes de este estudio, en orden de relevancia, son: (1) la confirmación de una brecha significativa entre el marco normativo y su aplicación práctica; (2) la identificación de un bajo nivel de madurez institucional en la gestión de la seguridad de la información; y (3) la necesidad de implementar un modelo integral que combine controles técnicos, administrativos y legales bajo la estructura de la norma ISO/IEC 27001:2022 (Bolaños, 2024). Estos hallazgos no solo respaldan los fundamentos teóricos del modelo propuesto, sino que también proporcionan evidencia empírica que confirma su adecuación al contexto de los GAD provinciales del Ecuador.

Desde la práctica, la implementación del modelo propuesto puede servir como hoja de ruta para la transición de la institución hacia niveles superiores de madurez (CMMI 3 y 4), fomentando la estandarización de procesos, la creación de un Comité de Seguridad de la Información y la articulación del marco LOPDP con el EGSI versión 3.0. En concordancia con las directrices de la ISO/IEC (2022), se sugiere implementar un ciclo de mejora continua (PDCA) a los procesos organizaciones que ejecuta la dirección (Jevelin & Faza, 2023), así como al sistema integral para garantizar de alguna manera la eficacia del sistema apoyado en evaluaciones internas con el seguimiento respectivo y procesos de capacitación frecuentes.

Conclusión

El presente estudio permitió evidenciar que el Sistema Integral de Gestión de Riego y Drenaje del GAD Provincial de El Oro carece de un modelo estructurado de gestión de seguridad de la información alineado con la Ley Orgánica de Protección de Datos Personales (LOPDP). Esta carencia se refleja en la débil implementación de políticas, procedimientos y controles, así como en el limitado conocimiento del personal sobre la normativa y las buenas prácticas de ciberseguridad, lo que incrementa la exposición a riesgos legales, operativos y tecnológicos.

La evaluación realizada con base en la norma ISO/IEC 27001:2022 permitió identificar de manera ordenada las brechas más críticas, especialmente en lo relacionado con la clasificación de la información, los accesos, la gestión de incidentes y la continuidad de los servicios. A partir de

estos hallazgos, se diseñó un modelo de gestión orientado no solo al cumplimiento normativo, sino también al fortalecimiento de la cultura organizacional en términos de seguridad de la información y a la reducción de vulnerabilidades técnicas u operativas en sistemas que administran datos sensibles de la ciudadanía tal es el caso del sistema integral.

El modelo planteado representa un aporte significativo que integra aspectos técnicos, legales y administrativos necesarios para garantizar los pilares fundamentales de la seguridad de la información, confidencialidad, integridad y disponibilidad. Además, constituye una oportunidad estratégica para el GAD Provincial de El Oro en su camino hacia la madurez de sus procesos organizativos y de ingeniería de software, consoliden la confianza ciudadana y mejoren la eficiencia institucional. Finalmente, este trabajo se orienta a ser replicado en otros sistemas informáticos de la institución, contribuyendo al fortalecimiento de la ciberseguridad institucional, al cumplimiento normativo y a la protección de los derechos personales de los ciudadanos y de los funcionarios en el sector público en general. A partir de este estudio, se sientan las bases para el desarrollo de futuras investigaciones orientadas a evaluar el nivel de madurez en seguridad de la información, la efectividad de los controles implementados y la adaptabilidad del modelo propuesto en diferentes contextos institucionales en especial siguiendo la línea de estudio, los sistemas informáticos institucionales.

En cuanto a las limitaciones del estudio, se reconoce que el uso de un muestreo no probabilístico restringe la generalización de los resultados a otros sistemas informáticos del GAD o de otras instituciones. Sin embargo, al enfocarse en un sistema crítico como el de riego y drenaje —que concentra datos personales, técnicos y financieros—, los hallazgos adquieren alta relevancia práctica. Además, la dependencia de la disponibilidad de los funcionarios y la falta de registros documentales actualizados constituyeron limitaciones operativas que podrían ser superadas mediante futuras investigaciones longitudinales.

Finalmente, es importante que en futuras investigaciones se profundice en el impacto que la implementación del modelo de gestión de seguridad de la información podría tener en la eficiencia institucional. También sería pertinente comparar el grado de madurez de los GAD provinciales tiene con relación a los GAD municipales o demás instituciones públicas que ya tienen un porcentaje de implementación avanzado, para identificar patrones comunes, diseñar políticas públicas e identificar controles normativos que fortalezcan la ciberseguridad en dichas instituciones.

Referencias

Albornoz, M. M. (2022). Expansión del ámbito territorial de aplicación de la ley en materia de protección de datos personales: ¿Tendencia en América Latina? *Latin American Law Review*, 9, 139–160. https://doi.org/10.29263/lar09.2022.08

Almache, E. L. R., Bustamante, J. L. R., & Espinoza, J. J. S. (2024). Implementación y desafíos de los principios de la Ley Orgánica de Protección de Datos Personales en Ecuador, Un enfoque de revisión sistemática. *Pro Sciences: Revista de Producción, Ciencias e Investigación*, *8*(54), 47-67.

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.

Barros, A., Flores, A., Jinez, M., & Zamora, D. (2025). La Protección de Datos Personales en el Gobierno Electrónico y Desafíos para la Gestión Pública. *Revista Veritas de Difusão Científica*, *6*(1), 1029–1046. https://doi.org/10.61616/rvdc.v6i1.447

Bolaños Coto, S. (2025). *Fortalecimiento de la seguridad de la información, con un enfoque en controles físicos en el área de infraestructura tecnológica a través de la ISO/IEC 27002: 2022, en el Banco Solidez en San José de Costa Rica en el año 2024* [Tesis de maestría, Universidad de Costa Rica].

Gallardo, M. (2018). *Elaboración de una política de seguridad de la información para una institución pública basado en el esquema gubernamental de seguridad de la información* [Tesis de pregrado, Universidad Internacional SEK].

Guamán, F. (2024). *Desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) utilizando la norma ISO/27001 para la protección de datos en la Unidad Educativa La Inmaculada de la ciudad de Ambato* [Tesis de maestría, Universidad Técnica de Ambato].

Heredia, L., & Santacruz, M. (2023). Responsabilidad médica administrativa, Manejo de datos personales relativos a la salud, Ecuador, 2023. *Revista Religación*, *8*(38). https://doi.org/10.46652/rgn.v8i38.1102

Jevelin, J., & Faza, A. (2023). Evaluation the information security management system: A path towards ISO 27001 certification. *Journal of Information Systems and Informatics*, *5*(4), 1240-1256.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2022). *Avance de la implementación Esquema Gubernamental de Seguridad de la Información (EGSI Versión 2.0)*. Gobierno Electrónico Ecuador.

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2024). *Esquema Gubernamental de Seguridad de la Información v3*. Registro Oficial No. 509.

Muyón, C., Guarda, T., Vargas, G., & Ninahualpa Quiña, G. (2019). Esquema Gubernamental de Seguridad de la Información EGSI y su aplicación en las entidades públicas del Ecuador. *Revista Ibérica de Sistemas e Tecnologias de Informação*, (19), 258-271.

Verdugo, G. (2023). *Propuesta de un modelo de madurez de ciberseguridad para Ecuador* [Tesis de maestría, Universidad Católica de Cuenca].

Villacres, O. (2024). *Falta de normativas y desafíos en la protección de datos personales y la ciberseguridad en el ordenamiento jurídico ecuatoriano* [Tesis de pregrado, Universidad Regional Autónoma de los Andes].

Vinueza, N., Macías, M., & Maldonado, R. (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. *Revista Científica Arbitrada de Investigación en Comunicación, Marketing y Empresa*, *5*(2), 112-130.

Autores

Jennifer Jomaira Loayza Castro. Ingeniera en Sistemas, Analista de Tecnología de la Información y Comunicación 1
Daniel Jacobo Andrade Pesántez. Universidad Católica de Cuenca

Declaración

Conflicto de interés
No tenemos ningún conflicto de interés que declarar.
Financiamiento
Sin ayuda financiera de partes externas a este artículo.
Nota
El artículo es original y no ha sido publicado previamente.