Effective information risk management. Review of a model for the Municipal Decentralized Autonomous Government of the Biblián Cantón

Gestión eficaz de riesgos de la información. Revisión de un modelo para el Gobierno Autónomo Descentralizado Municipal del Cantón Biblián

Autores:

Sacoto-Maldonado, Fernando Eduardo
UNIVERSIDAD CATÓLICA DE CUENCA
Independiente
Cuenca – Ecuador

fernando.sacoto.32@ucacue.edu.ec

https://orcid.org/0009-0006-0907-2774

Álvarez-Vera, Manuel Salvador
UNIVERSIDAD CATÓLICA DE CUENCA
Independiente
Cuenca – Ecuador

malvarezv@ucacue.edu.ec

https://orcid.org/0000-0002-2521-0042

Fechas de recepción: 25-ENE-2025 aceptación: 25-FEB-2025 publicación: 15-MAR-2025

https://orcid.org/0000-0002-8695-5005
http://mqrinvestigar.com/

Resumen

El presente artículo aborda la gestión de riesgos de la información en el Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Biblián, identificando las brechas en la implementación de políticas de seguridad a pesar de contar con un marco legal robusto. El problema central radica en la falta de recursos, capacitación y un sistema de monitoreo efectivo, lo que limita la capacidad del GAD para proteger sus activos de información. El objetivo es proponer un modelo de gestión de riesgos que se adapte a las necesidades específicas del GAD y cumpla con estándares internacionales, fortaleciendo la seguridad de la información y la confianza pública. Para ello, se revisaron literatura científica y técnica y documentos normativos nacionales e internacionales. Se identificaron deficiencias en la clasificación de activos, la capacitación del personal y la ausencia de un oficial de seguridad de la información, tal como exige el Acuerdo Ministerial No. 003-2024. El principal resultado revela que, aunque existe un marco legal sólido, la implementación es deficiente. La carencia de auditoría y monitoreo continuo impide la detección oportuna de fallas, exponiendo al GAD a riesgos significativos. Además, la falta de un oficial de seguridad limita la respuesta ante incidentes. La principal conclusión es que se requiere un modelo de gestión de riesgos más completo, cuyo sistema basado en estándares internacionales mejore la protección de la información y refuerce la confianza ciudadana.

Palabras clave: Gestión de riesgos; seguridad de la información; Gad Municipal; marco legal; capacitación del personal

Abstract

This article addresses information risk management in the Decentralized Autonomous Government (GAD) of the Municipal Canton of Biblián, identifying gaps in security policy implementation despite having a robust legal framework. The core problem lies in the lack of resources, training, and effective monitoring, which hinders the GAD's ability to protect its information assets. The goal is to propose a risk management model adapted to the GAD's specific needs that complies with international standards, thereby strengthening information security and public trust. A review of scientific and technical literature, along with national and international regulatory documents, was conducted. Deficiencies were found in asset classification, staff training, and the absence of an information security officer, as required by Ministerial Agreement No. 003-2024. The main finding reveals that although there is a solid legal framework, implementation remains weak. The lack of continuous auditing and monitoring impedes timely detection of failures, exposing the GAD to significant risks. In addition, the absence of a security officer restricts the institution's capacity to respond to incidents. The key conclusion is that a more comprehensive risk management model is needed, featuring a system aligned with international standards to enhance the protection of information and reinforce public confidence.

Keywords: Risk management; information security; MUNICIPAL GAD; legal framework; staff training

Introducción

La gestión eficaz del riesgo de la información se ha convertido en un componente esencial para las instituciones públicas, especialmente en los Gobiernos Autónomos Descentralizados (GAD). En el caso del GAD Municipal del Cantón Biblián, se maneja una gran cantidad de datos históricos y actuales, tanto físicos como digitales, relacionados con los servicios que se ofrecen a la ciudadanía. Conforme a la Ley Orgánica de Transparencia y Acceso a la Información Pública, la gestión adecuada de esta información es crucial para asegurar la eficiencia operativa y aumentar la confianza de los ciudadanos en las instituciones públicas (LOTAIP, 2024). La creciente digitalización de los entornos de trabajo ha incrementado la necesidad de implementar mecanismos sólidos para proteger la información contra riesgos de pérdida, alteraciones o acceso no autorizado (MINTEL, 2024).

El marco adecuado para gestionar estos riesgos se proporciona un nivel nacional a través del Esquema Gubernamental de Seguridad de la Información (EGSI). Las instituciones del sector público, incluidos los GAD, están obligadas a implementar estrategias que protejan la confidencialidad, integridad y disponibilidad de la información, conforme a las regulaciones vigentes. Según el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003, este plan promueve un enfoque organizado y estructurado que, siguiendo las normas internacionales de gestión de riesgos, fortalece las defensas de los activos informáticos en las organizaciones públicas (MINTEL, 2024).

El GAD del Cantón Biblián, como entidad local con diversas funciones y procesos administrativos, enfrenta desafíos únicos en la protección y manejo de la información. La constante evolución de las tecnologías de la información, junto con la presión creciente por adoptar políticas de transparencia y rendición de cuentas, intensifican estos desafíos (LOTAIP, 2024). En este contexto, la implementación de un modelo de gestión de riesgos de la información es crucial para garantizar que los procesos y operaciones del GAD estén protegidos contra amenazas tanto internas como externas.

Este estudio propone la creación de un modelo de gestión de riesgos de información para el GAD del Cantón Biblián. Este modelo no solo cumplirá con las necesidades de protección de datos importantes, sino que también se alineará con las políticas de seguridad de la información a nivel nacional e internacional, fomentando una cultura organizacional

proactiva y consciente de la importancia de la custodia de la información. El objetivo es que el modelo fortalezca la reputación del GAD como una institución al identificar, evaluar y reducir los riesgos en la gestión de información pública. Como lo sugiere Mitnick (2022), en muchos casos, el eslabón más débil en la seguridad de la información no radica en las tecnologías empleadas, sino en el comportamiento humano.

El objetivo principal es proporcionar un marco estructurado y efectivo para identificar, evaluar y mitigar los riesgos asociados a la información generada por el GAD Municipal, adaptable a sus necesidades y factibilidades. Se busca ofrecer procedimientos prácticos y aplicables que fortalezcan la seguridad de la información y promuevan una cultura de gestión proactiva del riesgo en el ámbito del manejo adecuado de la custodia de la información. La confiabilidad de la ciudadanía en los procedimientos y servicios ofrecidos por el GAD Municipal es un componente esencial de este proceso. La confianza de los usuarios aumenta cuando se puede mantener y proteger la información en tiempo real, lo que resulta en una mejor gestión de la información.

Por otro lado, el Acuerdo Ministerial No. 004-2024 tiene como objetivo promover la participación ciudadana a través de medios digitales, facilitar el acceso a la información pública y fomentar la interacción entre la población y el gobierno. La adopción de este marco puede beneficiar al GAD Municipal de Biblián al aumentar la transparencia y la confianza pública en sus procedimientos, lo cual es esencial para un manejo seguro y eficiente de la información (MINTEL, 2024).

Material y métodos

Este estudio utilizó una metodología cualitativa, descriptiva y exploratoria, enfocándose en comprender y analizar la gestión de riesgos de información en el GAD Municipal del Cantón Biblián. La complejidad de la seguridad de la información y la implementación de un modelo de gestión adaptado a las necesidades institucionales se abordan mediante este enfoque. En la primera etapa de la investigación, se realizó una revisión exhaustiva de la literatura científica y técnica, buscando documentos de organismos nacionales e internacionales relacionados con la seguridad de la información. Una de las principales fuentes de regulación fue el Esquema Gubernamental de Seguridad de la Información (EGSI), creado por el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). El análisis

del Acuerdo Ministerial No. 003-2024 permitió comprender cómo se organizan los sistemas de evaluación y gestión de riesgos en las instituciones públicas y cómo se adaptan a las necesidades del GAD de Biblián.

En la segunda fase del estudio, se revisaron manuales funcionales, incluyendo el Manual de Funciones, que establece las responsabilidades del personal encargado de la gestión de seguridad de la información. Se examinaron las responsabilidades de los comités de seguridad y los oficiales de seguridad de la información dentro del marco institucional para garantizar que cumplen con los estándares establecidos. Este análisis fue crucial para asegurar que las prácticas de seguridad de la información estuvieran alineadas con las normativas vigentes y las necesidades específicas del GAD.

Además, se incorporan normas internas de la Contraloría General del Estado, especialmente en lo que respeta a la tecnología de la información, como la Norma 410. Esta norma establece los estándares que deben cumplir las instituciones en el ámbito de la seguridad informática. La guía proporcionada por esta norma fue fundamental para comprender los estándares aplicables en la gestión de los activos de información, así como los procedimientos de auditoría necesarios para garantizar que el manejo de la información fuera transparente y responsable.

Finalmente, se revisó la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), actualizada en mayo de 2024, en el contexto de este estudio. LOTAIP establece los derechos y obligaciones del acceso a la información pública, lo cual es un componente esencial de la gestión de la seguridad de la información en el GAD. Esta ley ayudó a asegurar una gestión pública eficiente y responsable, garantizando que los procesos de gestión de riesgos cumplan con las normas de transparencia y acceso a la información.

Resultados

El estudio del marco legal en el Gobierno Autónomo Descentralizado (GAD) Municipal del Cantón Biblián reveló que la gestión de riesgos de la información estaba regulada por una serie de normativas nacionales e internacionales destinadas a garantizar la seguridad y la integridad de la información. En Ecuador, varias leyes y regulaciones resultaron esenciales para implementar un modelo efectivo de gestión de riesgos de información (Lozano y Andrade, 2020).

La Constitución de la República del Ecuador estableció principios fundamentales en cuanto a la protección de datos y privacidad, los cuales debían ser respetados y asegurados por todas las instituciones públicas (Constitución de la República del Ecuador, 2008, pp. 88-90). El numeral 19 del artículo 66 subrayó el derecho a la protección de datos personales, obligando a los GAD a tomar las medidas necesarias para garantizar la seguridad de la información de los ciudadanos.

El marco legal también incluyó la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP), establecida en 2004. Esta ley sentó las bases para la gestión adecuada de la información pública al promover la transparencia y el acceso a la información, imponiendo obligaciones sobre la protección y el manejo adecuado de datos sensibles.

Los GAD debían implementar políticas y procedimientos para garantizar la confidencialidad, integridad y disponibilidad de la información en este contexto (Acuerdo de la Contraloría General del Estado, 2014). Además, la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, aprobada en 2002, introdujo normas para el uso de firmas electrónicas y la gestión de información digital, siendo fundamental para establecer sistemas de gestión de riesgos de la información en los GAD (Rodríguez et al., 2008).

La evaluación del Sistema de Gestión de Riesgos de Información, en el marco de la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI), reveló una serie de desafíos y oportunidades importantes. Uno de los hallazgos más significativos fue la necesidad de una mayor integración de las políticas de seguridad de la información con la participación ciudadana a través de medios electrónicos, tal como se inició en el Acuerdo Ministerial No. 004-2024. Este acuerdo promovió el uso de tecnologías digitales no solo para la gestión de la información, sino también para que la ciudadanía pudiera acceder y participar activamente en los procesos públicos.

El análisis del Acuerdo Ministerial No. 003-2024, que regula el EGSI, destacó la necesidad de implementar medidas específicas para proteger la confidencialidad, integridad y disponibilidad de los datos procesados por las entidades públicas. Se descubrió que el sistema actual del GAD Municipal de Biblián no cumplía completamente con los requisitos del EGSI en términos de seguridad de la infraestructura tecnológica y protección de datos personales. La conformidad del GAD con las regulaciones internas de la Contraloría General del Estado fue uno de los elementos evaluados. La Norma 410, relacionada con la tecnología de la

información, planteó un desafío para el GAD al actualizar sus políticas de seguridad informática.

Tabla 1
Evaluación de criterios para el sistema de riesgo.

Criterio	Descripción	Indicador	Método de Evaluación	Resultado Esperado
Designación de un Oficial de Seguridad de la Información	Nombrar a un responsable de la seguridad de la información conforme al Acuerdo Ministerial No. 003-2024	Existencia de un oficial designado	Revisión documental y entrevistas a personal del GAD	Oficial designado y liderando la implementación del EGSI
Implementación de una Plataforma de Participación Ciudadana Digital	Desarrollo de una plataforma que permita a los ciudadanos acceder a la información y participar en la toma de decisiones, según Acuerdo	Disponibilidad y funcionalidad de la plataforma digital	Evaluación técnica de la plataforma y encuestas a la ciudadanía	Plataforma implementada y accesible para los ciudadanos

	Ministerial No. 004-2024			
Fortalecimiento de la Auditoría y Monitoreo Continuo	Implementación de auditorías internas y externas para asegurar el cumplimiento de políticas de seguridad	Número de auditorías realizadas y reporte de cumplimiento	Revisión de informes de auditoría	Auditorías regulares con resultados que evidencian cumplimiento
Capacitación en Normativas de Protección de Datos	Programas de formación para funcionarios sobre el EGSI, LOTAIP y normativas relacionadas	Número de funcionarios capacitados	Revisión de registros de capacitación y encuestas de retroalimentación	Alto porcentaje de funcionarios capacitados y aplicando buenas prácticas

Fuente: Elaboración propia

Brechas identificadas en la implementación del EGSI

El análisis de este estudio identificó brechas significativas en la implementación del Esquema Gubernamental de Seguridad de la Información (EGSI) en el GAD Municipal de Biblián. Según el Acuerdo Ministerial No. 003-2024, la designación de un oficial de seguridad de la información es un requisito esencial. La ausencia de esta figura afectó la capacidad del GAD para responder a incidentes de seguridad y gestionar de forma proactiva los riesgos asociados con la custodia de datos sensibles.

Aunque se tomaron medidas iniciales para proteger la información, los procedimientos actuales no cubrían todas las etapas del ciclo de vida de los datos, lo que aumentó la posibilidad de acceso no autorizado, pérdida o alteraciones de la información. Además, la evaluación reveló la inexistencia de un sistema efectivo para auditar y monitorear continuamente los riesgos, lo cual es esencial para cumplir con las obligaciones legales y normativas de protección de datos.

Participación ciudadana y transparencia en la gestión de la información

La relación entre la seguridad de la información y la participación de los ciudadanos en los procesos de toma de decisiones también fue evaluada. El Acuerdo Ministerial No. 004-2024 desarrolló pautas claras sobre cómo las entidades públicas deben brindar al público acceso a la información. La evaluación indicó que el GAD Municipal de Biblián no había aprovechado al máximo estas oportunidades debido a la falta de una plataforma digital sólida que permitiera la transparencia y el control social en la gestión de la información.

Otro hallazgo importante fue el incumplimiento de la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP). Aunque se hicieron esfuerzos para publicar información pública en portales web, los mecanismos actuales de difusión de información eran limitados y no cumplían con los estándares establecidos por la LOTAIP. Este incumplimiento impactó negativamente en la confianza de los ciudadanos y su percepción de la transparencia de la gestión pública.

Discusión

La investigación sobre la gestión de riesgos de la información en el GAD Municipal del Cantón Biblián revela una base legal sólida sustentada en la Constitución de la República, la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) y la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Estas leyes establecen principios y obligaciones claras para la protección y seguridad de los datos, lo cual es fundamental para garantizar una gestión de riesgos adecuada en las organizaciones públicas, como destacan Lozano y Andrade (2020). Sin embargo, a pesar de contar con este marco normativo robusto, se identifican brechas significativas en la implementación de las políticas de gestión de riesgos.

Al comparar los hallazgos de este estudio con investigaciones previas, como la de Chimborazo (2021), se observa que ambos coinciden en señalar problemas relacionados con la falta de recursos y la capacitación continua del personal. Estos factores limitan la capacidad del GAD Municipal de Biblián para establecer un sistema de gestión de riesgos efectivo. Chimborazo también destaca la falta de coordinación de las políticas de riesgos en diferentes áreas operativas, y nuestro análisis confirma la ausencia de una estrategia coherente, lo que ha generado silos que obstaculizan una respuesta coordinada a los eventos de seguridad. Para abordar este problema, se propone la creación de un comité de gestión de riesgos interdepartamental que mejore la colaboración entre las diferentes áreas.

La falta de identificación y clasificación de los activos de información es otro hallazgo clave de este estudio, lo que limita la capacidad de evaluar completamente los riesgos. Según Rodríguez et al. (2008), una clasificación incorrecta de los activos de información impide una priorización efectiva de los riesgos y limita la capacidad de respuesta ante incidentes. Esta conclusión corrobora nuestros hallazgos. Además, las restricciones presupuestarias y tecnológicas se mencionan como obstáculos para la implementación de estrategias de mitigación apropiadas. Investigaciones anteriores han demostrado que la falta de recursos adecuados es un obstáculo común para la implementación de sistemas de gestión de riesgos en entidades públicas de países en vías de desarrollo.

Otra coincidencia con estudios similares es la necesidad de auditorías regulares, revisiones de seguridad y pruebas de penetración como parte de un proceso de mejora continua. Estas prácticas son esenciales para mantener la integridad y seguridad de los sistemas de información y deben estar integradas en la gestión de riesgos del GAD.

Para garantizar una respuesta coordinada y efectiva a incidentes, la gestión de riesgos de la información debe integrarse con otros sistemas de gestión de riesgos institucionales. Este estudio corrobora los hallazgos de Sánchez et al. (2022), quienes sostienen que dividir las funciones de gestión de riesgos puede causar ineficiencias y retrasos en la atención de incidentes de seguridad. La creación de un comité de riesgos interdepartamental facilitará la coordinación y el uso eficiente de los recursos, permitiendo al GAD de Biblián ser más resistente a las amenazas de seguridad.

Aunque el GAD Municipal del Cantón Biblián cuenta con un marco legal adecuado, la implementación efectiva de políticas de gestión de riesgos requiere mejoras significativas en

la coordinación, recursos y capacitación. La adopción de un enfoque integrado y colaborativo es esencial para fortalecer la seguridad de la información y aumentar la confianza de los ciudadanos en la gestión pública.

Tabla 2.

Modelo de gestión de riesgos de información para el GAD Municipal del Cantón Biblián.

Componente	**Descripción**
Identificación y clasificación de activos de información	- Crear un inventario detallado de todos los activos de información, incluyendo datos, sistemas, infraestructura y personal. - Establecer criterios claros para clasificar los activos según su importancia y sensibilidad, lo que permitirá priorizar los riesgos.
Evaluación de riesgos	- Identificar las amenazas potenciales y las vulnerabilidades existentes en los sistemas de información. - Determinar el impacto potencial de cada riesgo identificado en las operaciones del GAD.
Desarrollo de estrategias de mitigación	- Implementar controles técnicos y administrativos para mitigar los riesgos identificados, como cifrado de datos, autenticación de usuarios y políticas de acceso. - Desarrollar un plan detallado para responder a incidentes de seguridad, incluyendo procedimientos de notificación y recuperación.
Capacitación y concienciación del personal	- Establecer programas de capacitación regulares para el personal, enfocándose en

	prácticas de seguridad de la información y manejo de incidentes. - Fomentar una cultura organizacional que valore la seguridad de la información y la gestión de riesgos.
Monitoreo y auditoría continua	- Implementar sistemas para el monitoreo continuo de la seguridad de la información, permitiendo la detección temprana de incidentes. - Realizar auditorías periódicas para evaluar el cumplimiento de las políticas de seguridad y la efectividad de los controles implementados.
Designación de un Oficial de Seguridad de la Información	- Designar un oficial de seguridad de la información responsable de supervisar la implementación del modelo de gestión de riesgos y coordinar la respuesta a incidentes.
Integración con otros sistemas de gestión	- Crear un comité de gestión de riesgos interdepartamental para asegurar la coordinación y el uso eficiente de los recursos. - Asegurar que el modelo esté alineado con estándares internacionales de gestión de riesgos, como ISO 27001.
Evaluación y mejora continua	- Evaluar regularmente el modelo de gestión de riesgos para identificar áreas de mejora y adaptarse a cambios en el entorno de amenazas. - Incorporar retroalimentación de las auditorías y revisar para ajustar y mejorar continuamente el modelo.

Conclusiones

La investigación reveló que la identificación y clasificación detallada de los activos de información en el GAD Municipal del Cantón Biblián era limitada, lo que dificultó la evaluación completa de los riesgos. La falta de una clasificación adecuada impidió que el GAD priorizara los riesgos a los que estaba expuesta su información. Este hallazgo subraya la importancia de crear un sistema de identificación claro y completo que cubra todos los activos importantes, incluyendo personal, sistemas y datos.

Se evidencia que el personal encargado de la gestión de la información carecía de recursos adecuados y de capacitación continua. Esta situación impactó negativamente en la implementación de métodos para mitigar y proteger los activos de información. La falta de preparación adecuada del personal para manejar los riesgos de seguridad de la información de manera efectiva resalta la necesidad de programas de capacitación regulares y específicos.

La ausencia de un oficial de seguridad de la información, un requisito esencial según el Acuerdo Ministerial No. 003-2024, demostró que la implementación del EGSI en el GAD fue incompleta. La falta de esta carga afectó la capacidad del GAD para responder a incidentes de seguridad y gestionar los riesgos de manera proactiva, lo que es crucial para una gestión de riesgos efectiva.

Además, se encontró que no existía un sistema sólido de auditoría y monitoreo continuo para evaluar el cumplimiento de las políticas de seguridad de la información. La realización de auditorías y pruebas de seguridad regulares es esencial para mejorar la capacidad del GAD de detectar y corregir fallas antes de que se materialicen como incidentes de seguridad.

A pesar de que el GAD Municipal del Cantón Biblián cuenta con un marco legal sólido para la gestión de la información, se identifican problemas en la implementación de las políticas de seguridad, falta de recursos y capacitación, y escasez de monitoreo. Estos hallazgos demuestran la necesidad de un modelo de gestión de riesgos de información más completo. Implementar un sistema de gestión que se adapte a las necesidades específicas del GAD y se base en estándares internacionales fortalecerá la confianza pública y la seguridad de la información.

Referencias bibliográficas

Acuerdo de la Contraloría General del Estado. (2014). NORMAS DE CONTROL INTERNO DE LA CONTRALORIA.

Álvarez, C., & Torres, J. (2023). Propuesta del modelo de implementación de la gestión de riesgos de desastres en el Gobierno Autónomo Descentralizado municipal del cantón Déleg. Retrieved 2024, from https://dspace.ups.edu.ec/handle/123456789/24625

Bedoya, J., & Patiño, J. (2023). Plan estratégico para la identificación de riesgos y vulnerabilidades en la seguridad de la información de los datos personales en una empresa. Retrieved 2024, from https://dspace.tdea.edu.co/handle/tdea/3576

Chimborazo, C. (2021). Manual de políticas de seguridad de la información basado en la norma ISO 27001 en el GAD intercultural de el Tambo. Retrieved 2024, from http://dspace.ucacue.edu.ec:4000/items/77b7c55e-90de-4bfe-8ad5-13871c35aa1e

Constitución de la República del Ecuador. (2008). Decreto Legislativo. 87-92. 88-93. Retrieved 2024, from https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Cortes, Y. (2018). Apoyo al área de seguridad de la información de la corporación de alta tecnología para la defensa de Codaltec para concluir la implementación y operación del sistema de gestión de seguridad de la información SGSI según la norma técnica colombiana ISO-IEC. Retrieved 2024, from http://www.securitybydefault.com/2011/08/deficiencias-mas-comunes-en-los-sgsi.html

Isaza, H. (2023). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO/IEC 27001: 2022, para la Esal Asociación Esperanza Viva. Retrieved 2024, from https://repository.ucc.edu.co/entities/publication/8dda9d11-6a06-466c-86d1-548c8926185d

ISO. (2018). *ISO 31000:2018(es).*

LOTAIP. (18 de mayo de 2024). *Ley Orgánica de Transparencia y Acceso a Información Pública.* Registro Oficial Suplemento 337 de 18-may.-2004: https://www.educacionsuperior.gob.ec/wp-content/uploads/downloads/2014/09/LOTAIP.pdf

Lozano, L., & Andrade, M. (2020). Políticas de Seguridad de la Información bajo la Norma ISO 27002: 2013 para el Gobierno Autónomo Descentralizado del Cantón Biblián.

Polo del Conocimiento: Revista científico-profesional, 5(11), 591-621. Retrieved 2024, from https://dialnet.unirioja.es/servlet/articulo?codigo=9435836

Mena, Z. G. (2021). *EL PRINCIPIO CONSTITUCIONAL DE TRANSPARENCIA EN LA CONTRATACIÓN PÚBLICA DEL ECUADOR. UN ENFOQUE DESDE LA PARTICIPACIÓN CIUDADANA.*

MINTEL 0003. (2024). *Oficio Nro. MINTEL-SGERC-2024-0146-O.* Retrieved 2024, from https://www.gob.ec/sites/default/files/2024-02/Lineamientos%20reporte%20avances%20planes%202024.pdf

MINTEL 0004. (2024). *Ministerio de Telecomunicaciones y de la Sociedad de la Información.* ACUERDO Nro. MINTEL-MINTEL-2024-0004: https://www.gobiernoabierto.ec/wp-content/uploads/2019/10/MINTEL-MINTEL-2024-0004.pdf

Mitnick, K. (2022). *El arte del engaño: Controlar el elemento humano de la seguridad.*

Porras, M. (2020). Sistema de Gestión de Seguridad de la Información para la Gestión de Riesgos en Activos de Información. Retrieved 2024, from https://repositorio.upla.edu.pe/handle/20.500.12848/2604

Rodriguez, L., Cruzado, C., & Diaz, M. (2008). Aplicación de ISO 27001 y su influencia en la seguridad de la información. *Propósitos y representaciones, 8*(3). Retrieved 2024, from http://www.scielo.org.pe/scielo.php?pid=S2307-79992020000400011&script=sci_abstract&tlng=en

Sánchez, M., Carrillo, J., & Fernando, M. (2022). Análisis y evaluación de riesgos aplicados a la seguridad de la información bajo la norma ISO. Informática y Sistemas. *Revista de Tecnologías de la Informática y las Comunicaciones, 6*(1), 63-78. Retrieved 2024, from https://pdfs.semanticscholar.org/20f8/f8d55ffc31de79cab0101fc1f974580022af.pdf

Sanchez, P., Reyes, A., & Saura, J. (2019). Modelos de Adopción de Tecnologías de la Información y Cloud Computing en las Organizaciones. *Información tecnológica, 30*(3), 3-12. Retrieved 2024, from https://www.scielo.cl/scielo.php?pid=S0718-07642019000300003&script=sci_arttext

Subía Guerra, J. (2021). Auditoría basada en riesgos: una alternativa de mayor eficacia en las acciones de control en el Ecuador.

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.