Revista Científica Multidisciplinar G-ner@ndo
ISSN: 2806-5905

Desarrollo de un plan de gestión de seguridad para sistemas de información geográfica en empresas públicas de Ecuador

Development of a security management plan for geographic information systems in public companies in Ecuador.

Jimy Vinicio Cuesta Garzón, Andrés Sebastián Quevedo Sacoto

CIENCIA E INNOVACIÓN EN DIVERSAS DISCIPLINAS CIENTÍFICAS.
Julio - Diciembre, V°5-N°2; 2024

✓ **Recibido:** 01/07/2024
✓ **Aceptado**: 09/07/2024
✓ **Publicado:** 31/12/2024

PAIS

- Cuenca – Ecuador
- Cuenca – Ecuador

INSTITUCIÓN:

- Universidad Católica de Cuenca
- Universidad Católica de Cuenca

CORREO:

jimy.cuesta.52@est.ucacue.edu.ec
asquevedos@ucacue.edu.ec

ORCID:

https://orcid.org/0009-0002-3318-8030
https://orcid.org/0000-0001-5585-0270

FORMATO DE CITA APA.

Cuesta, J. Quevedo, A. *(2024). Desarrollo de un plan de gestión de seguridad para sistemas de información geográfica en empresas públicas de Ecuador. Revista G-ner@ndo, V°5 (N°2,).1-14.*

Resumen

La seguridad en los Sistemas de Información Geográfica (SIG) es crucial para las empresas públicas de Ecuador. Estos sistemas, que integran datos espaciales con información descriptiva, son esenciales para la planificación y gestión eficiente de los servicios públicos. No obstante, los Sistemas de Información Geográfica (SIG) enfrentan riesgos significativos como accesos no autorizados, pérdida de datos sensibles y ciberataques, destacando la necesidad urgente de implementar medidas efectivas de ciberseguridad. Este artículo presenta el desarrollo de un plan de gestión de seguridad específico para los Sistemas de Información Geográfica (SIG) en Ecuador. Utilizando un enfoque descriptivo y evaluativo, se identificaron las necesidades de seguridad, se evaluó la infraestructura existente y se propusieron políticas y procedimientos adecuados. La metodología incluyó entrevistas con administradores de la plataforma y una revisión exhaustiva de la documentación técnica y literatura académica. Entre los resultados obtenidos se destacan la identificación y valoración de los activos de información geográfica, la evaluación de riesgos, la implementación de controles de seguridad, el establecimiento de políticas y procedimientos claros, y la capacitación del personal. Estas medidas han demostrado ser efectivas para mejorar la seguridad de la información geográfica, reduciendo significativamente los incidentes de seguridad y asegurando la continuidad de los servicios públicos. Este artículo no solo amplía el conocimiento existente, sino que también ofrece un plan práctico que puede ser adaptado y replicado en otras empresas públicas.

Palabras clave: Seguridad de la Información Geográfica, Sistemas de Información Geográfica (SIG), Gestión de seguridad, Empresas públicas de Ecuador, Ciberseguridad.

Abstract

Security in Geographic Information Systems (GIS) is crucial for Ecuador's public companies. These systems, which integrate spatial data with descriptive information, are essential for the efficient planning and management of public services. However, Geographic Information Systems (GIS) face significant risks such as unauthorized access, loss of sensitive data, and cyber-attacks, highlighting the urgent need to implement effective cybersecurity measures. This paper presents the development of a specific security management plan for Geographic Information Systems (GIS) in Ecuador. Using a descriptive and evaluative approach, security needs where identified, existing infrastructure was assessed, and appropriate policies and procedures were proposed. The methodology included interviews with platform administrators and an exhaustive review of technical documentation and academic literature. Among the results obtained were the identification and valuation of geographic information assets, risk assessment, implementation of security controls, establishment of clear policies and procedures, and staff training. These measures have proven to be effective in improving the security of geographic information, significantly reducing security incidents and ensuring the continuity of public services. This article not only expands on existing knowledge, but also offers a practical model that can be adapted and replicated in other public companies.

Keywords: Geographic Information Security, Geographic Information Systems (GIS), Security Management, Public Companies in Ecuador, Cybersecurity.

Introducción

Actualmente, los Sistemas de Información Geográfica (SIG) en las empresas públicas del Ecuador están expuestos a riesgos como accesos no autorizados, pérdida de datos sensibles y ciberataques. En Ecuador, por ejemplo, tras la revocación del asilo a Julian Assange, las instituciones ecuatorianas sufrieron más de 40 millones de ciberataques, lo que destaca la importancia de implementar medidas de ciberseguridad efectivas para proteger la información sensible (Fingas, 2019). Según Wang et al. (2024), la detección de peligros de seguridad en los sistemas de información geográfica es crítica, especialmente en el contexto del Internet de las cosas (IoT). Su estudio destaca que los riesgos de accesos no autorizados y la pérdida de datos sensibles son prevalentes en los Sistemas de Información Geográfica (SIG), lo que subraya la necesidad de una mayor concienciación y medidas de seguridad robustas para mitigar estos problemas. Asegurar la integridad, confidencialidad y disponibilidad de la información geográfica es vital para la continuidad y eficiencia de los servicios públicos. Sin estas medidas, las consecuencias pueden ser severas, incluyendo interrupciones en los servicios esenciales y pérdida de confianza por parte del público.

El presente artículo busca desarrollar un plan de gestión de seguridad adaptado a las necesidades específicas del contexto ecuatoriano. Cárdenas Solano et al. (2016) señaló que la adopción de ISO 27001 puede fortalecer la protección de los datos. Asimismo, Bork et al. (2024) destacó que la implementación de ISO 27001 en la gestión de seguridad de la información mejora la calidad de los servicios proporcionados en la infraestructura de datos de investigación. Wysokińska et al. (2023) argumentó que la adopción de ISO 27001 en organizaciones privadas, públicas y sin fines de lucro mejora la gestión de la seguridad de la información. Además, Mera-Amores y Roa (2024) enfatizaron que la conformidad con ISO 27001 mejora la gestión de seguridad de la información en pequeñas y medianas empresas (Mera-Amores y Roa, 2024). No obstante, existe una carencia de planes específicos para la gestión de seguridad de los Sistemas de Información Geográfica (SIG) en el sector público de Ecuador, lo que este artículo pretende

abordar. Por ejemplo, en el documento "Lineamientos para la Gobernanza de la Gestión del Riesgo de Desastres" se subraya la necesidad de mejorar los sistemas de información geográfica y la gestión de riesgos, indicando una falta de políticas claras y específicas en esta área (Gobernanza de la Gestión del Riesgo de Desastres, 2022).

La investigación previa de Azaz (2011) y Longley et al. (2001) sobre la adopción y gestión de los Sistemas de Información Geográfica (SIG) en el sector público ha subrayado la importancia de medidas de seguridad adecuadas. Además, Peggion et al. (2008) y Alzahrani y Sheikh Abdullah (2021) han demostrado que una gestión efectiva de la seguridad puede mitigar los riesgos asociados con los Sistemas de Información Geográfica (SIG). Los objetivos del artículo son identificar las necesidades de seguridad, evaluar la infraestructura actual, desarrollar políticas y procedimientos de seguridad, capacitar al personal y establecer un plan de respuesta ante incidentes. Las preguntas de investigación incluyen: ¿Cuáles son los mecanismos de control de acceso más efectivos para proteger la información geográfica?, ¿Qué medidas se pueden implementar para garantizar la seguridad de los servidores y los datos geográficos?, ¿Cómo se pueden detectar y abordar oportunamente las violaciones de seguridad? Resolver estos problemas es crucial para mejorar la protección de los datos geográficos y garantizar la continuidad de los servicios públicos. Este artículo no solo contribuirá al conocimiento existente, sino que también proporcionará un plan práctico que puede ser adaptado y replicado en otras empresas públicas.

Materiales Y Métodos

Para desarrollar un plan de gestión de seguridad enfocado en los Sistemas de Información Geográfica (SIG) en las empresas públicas de Ecuador, se implementó un enfoque analítico y evaluativo, centrado en el análisis de causas y evaluación de impactos, identificando las necesidades de seguridad y se evaluación de la infraestructura actual. Con esta información, se propusieron políticas y procedimientos adecuados basados en un análisis detallado de las

vulnerabilidades y sus posibles consecuencias. La investigación se basó en la experiencia combinada del equipo del departamento de Sistemas de Información Geográfica (SIG), responsable de administrar la plataforma, y del departamento de Seguridad de la Información, encargado de crear y aplicar normas, políticas y procedimientos. Esta colaboración permitió una comprensión profunda de los problemas y la formulación de soluciones específicas.

Para la recolección de datos, se diseñó una estructura clara y rigurosa que incluyó tanto fuentes primarias como secundarias. Las fuentes primarias consistieron en entrevistas detalladas y sesiones de trabajo con miembros de ambos departamentos en al menos dos empresas públicas seleccionadas por tener estructuras organizativas de los Sistemas de Información Geográfica (SIG) similares. Esto facilitó una comparación efectiva y la generalización de los hallazgos. Se utilizaron cuestionarios estructurados y guías de entrevista para asegurar la consistencia y profundidad de la información recopilada. Los participantes fueron seleccionados según su rol y experiencia, garantizando la inclusión de diversos puntos de vista y conocimientos especializados. Las fuentes secundarias incluyeron una revisión exhaustiva de políticas y procedimientos de seguridad existentes, documentos técnicos sobre la gestión de los Sistemas de Información Geográfica (SIG) y literatura académica relevante. Se emplearon criterios específicos para seleccionar estos documentos, tales como relevancia temática, actualidad y procedencia de fuentes confiables.

El análisis de datos se llevó a cabo mediante un enfoque mixto que combinó técnicas cualitativas y cuantitativas. Los datos cualitativos obtenidos de las entrevistas y sesiones de trabajo fueron codificados y analizados temáticamente para identificar patrones y áreas que requieren mejoras. Los datos cuantitativos provenientes de las revisiones documentales fueron analizados estadísticamente para corroborar los hallazgos cualitativos y proporcionar una base sólida para la mejorar las políticas y procedimientos.

Las consideraciones éticas fueron estrictamente respetadas, asegurando el consentimiento informado de todos los participantes y garantizando la confidencialidad y anonimato de la información proporcionada. Se implementaron procedimientos específicos, como la revisión cruzada de datos por varios investigadores y la validación de los hallazgos con los participantes. Además, el comité de ética de la Universidad Católica de Cuenca aprobó el estudio, asegurando el cumplimiento de todas las normativas aplicables. Esta metodología ética y bien estructurada permitió recopilar y analizar información crucial, identificando causas de vulnerabilidades y evaluando los impactos potenciales de las mismas. En última instancia, la experiencia y conocimientos combinados del equipo del departamento de Sistemas de Información Geográfica (SIG) y del departamento de Seguridad de la Información fueron esenciales para proponer soluciones prácticas y aplicables, enfocadas en la mejora continua del plan de gestión de seguridad.

Gráfico 1:

Metodología del plan de gestión de seguridad para los Sistemas de Información Geográfica (SIG)

Identificación de Activos	- Identificar bases de datos - Valorar aplicaciones - Evaluar servicios - Determinar roles de usuarios
Evaluación de Riesgos	- Identificar amenazas - Evaluar vulnerabilidades - Determinar impacto - Establecer probabilidad
Definición de Medidas de Seguridad	- Autenticación - Autorización - Cifrado - Monitoreo
Implementación de Controles de Seguridad	- Aplicar controles - Monitorear acceso - Detectar actividades sospechosas
Establecimiento de Políticas	- Crear directrices de acceso - Desarrollar procedimientos de gestión de incidentes - Actualizar protocolos de seguridad
Capacitación del Personal	- Realizar talleres - Organizar seminarios - Implementar nuevas políticas
Mejora Continua	- Revisar controles - Actualizar políticas - Adaptarse a nuevas amenazas

Nota: El gráfico 1 muestra según el enfoque planteado, cada etapa del proceso, representada junto con sus pasos correspondientes, lo que permite una visualización clara y estructurada del plan.

Análisis de Resultados

El desarrollo de un plan de gestión de seguridad para los sistemas de información geográfica (SIG) en las empresas públicas del Ecuador ha producido resultados notables. Estos resultados están orientados a proteger la información geográfica, prevenir amenazas y minimizar los riesgos relacionados con la seguridad de la información. Los principales logros del plan incluyen: la identificación y valoración de activos de información geográfica, la evaluación de riesgos, la implementación de controles de seguridad, el establecimiento de políticas y procedimientos claros, la capacitación del personal y la mejora continua del plan de gestión de seguridad.

Identificación de Activos de Información Geográfica

Se identificaron y valoraron los activos de información geográfica, incluyendo bases de datos, aplicaciones, servicios y roles de usuarios. Este paso permitió a la organización comprender mejor el valor de su información geográfica y priorizar las medidas de protección necesarias.

Tabla 1

Identificación y Valoración de Activos de Información Geográfica

Activo	Descripción	Valor para la Organización
Bases de datos geográficas	Datos espaciales críticos	Alto
Aplicaciones geográficas	Software utilizado para análisis geográfico	Medio
Servicios geográficos	Servicios web de mapas y geoprocesamiento	Alto
Roles de usuarios	Permisos y accesos de diferentes usuarios	Medio

Nota: La Tabla 1 muestra la identificación y valoración de los activos de información geográfica, proporcionando una base sólida para la implementación de medidas de seguridad.

Evaluación de Riesgos y Definición de Medidas de Seguridad

Se evaluaron los riesgos asociados a la seguridad de la información geográfica y se definieron medidas de seguridad adecuadas. Este proceso incluyó la identificación de posibles amenazas y vulnerabilidades, así como la determinación del impacto potencial y la probabilidad de ocurrencia.

Tabla 2

Evaluación de Riesgos y Medidas de Seguridad

Riesgo	Impacto Potencial	Probabilidad
Acceso no autorizado	Alto	Medio
Pérdida de datos	Alto	Bajo
Ataques de malwar	Medio	Alto
Errores humanos	Medio	Alto

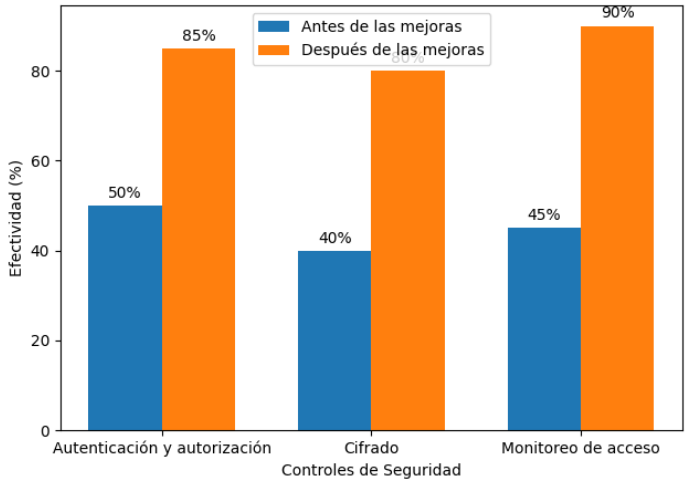
Nota: La Tabla 2 presenta una evaluación de riesgos junto con las medidas de seguridad implementadas para mitigar dichos riesgos.

Implementación de Controles de Seguridad

Se implementaron diversos controles de seguridad para proteger la información geográfica, incluyendo autenticación, autorización, cifrado y monitoreo de acceso. Estos controles fueron diseñados para garantizar que solo los usuarios autorizados puedan acceder a la información geográfica y que cualquier actividad sospechosa sea detectada y respondida de manera oportuna.

Gráfico 2

Efectividad de los Controles de Seguridad Implementados



***Nota*:** El Gráfico 2 ilustra la efectividad de los controles de seguridad implementados, destacando una mejora significativa en la protección de la información geográfica.

Establecimiento de Políticas y Procedimientos de Seguridad

Se establecieron políticas y procedimientos claros para la gestión de la información geográfica. Estas políticas incluyeron directrices sobre el acceso y uso de la información, la gestión de incidentes de seguridad y la actualización de los sistemas de seguridad.

Tabla 3

Políticas y Procedimientos de Seguridad Establecidos

Política/Procedimiento	Descripción
Política de acceso y uso	Directrices sobre quién puede acceder y cómo utilizar la información geográfica
Procedimientos de gestión de incidentes	Pasos a seguir en caso de un incidente de seguridad
Protocolo de actualización de seguridad	Mantenimiento y actualización regular de los sistemas de seguridad

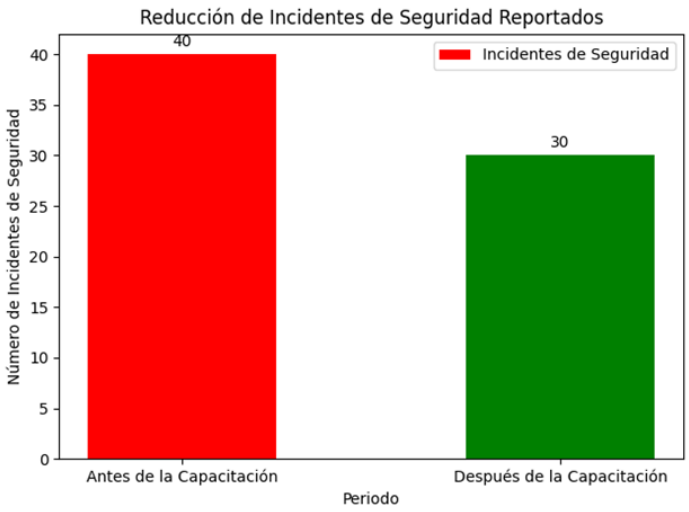
***Nota*:** La Tabla 3 detalla las políticas y procedimientos de seguridad establecidos, que garantizan una gestión adecuada y segura de la información geográfica.

Educación y Capacitación del Personal

Se llevaron a cabo programas de educación y capacitación para el personal sobre materias de seguridad de la información geográfica. Estas sesiones incluyeron talleres prácticos y seminarios sobre ciberseguridad, así como la implementación de nuevas políticas de seguridad.

Gráfico 3

Incremento en el Conocimiento de Seguridad del Personal



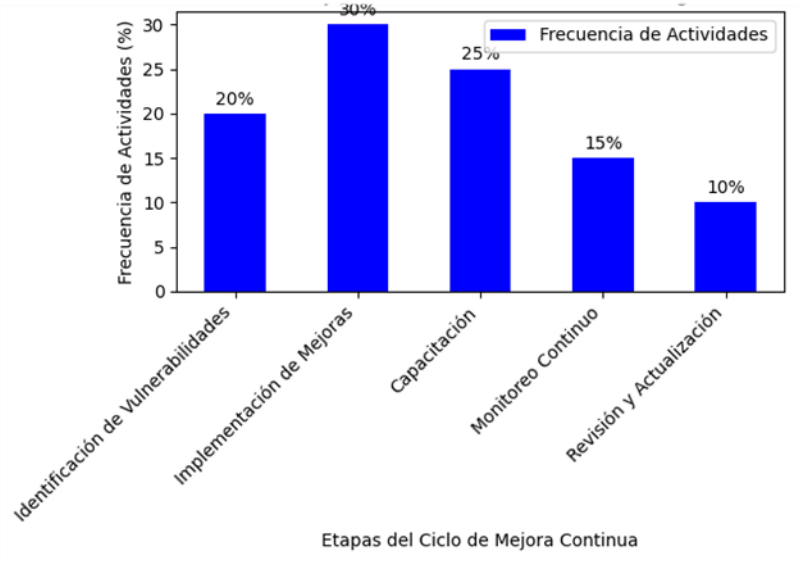
***Nota*:** El Gráfico 3 muestra un aumento significativo en el conocimiento de seguridad del personal, lo cual es fundamental para prevenir incidentes y gestionar adecuadamente la información geográfica.

Mejora Continua del Plan de Gestión de Seguridad

Se estableció un proceso de revisión y actualización periódica de los controles y políticas de seguridad. Este enfoque de mejora continua asegura que el plan de gestión de seguridad se adapte a nuevas amenazas y desafíos, manteniendo la protección de la información geográfica.

Gráfico 4

Ciclo de Mejora Continua en la Gestión de Seguridad



***Nota*:** El Gráfico 4 destaca el ciclo de mejora continua implementado, asegurando que las políticas y controles de seguridad sean revisados y actualizados regularmente.Los resultados de este estudio demuestran que la implementación de un plan de gestión de seguridad en los Sistemas de Información Geográfica (SIG) de las empresas públicas del Ecuador ha tenido un impacto positivo en la protección de la información geográfica. La identificación y valoración de activos, evaluación de riesgos, implementación de controles de seguridad, establecimiento de políticas y procedimientos, y la capacitación del personal han contribuido significativamente a la mejora de la seguridad.

Conclusiones

El artículo demuestra la vulnerabilidad de los Sistemas de Información Geográfica (SIG) en las empresas públicas de Ecuador, subrayando la importancia de implementar un plan de gestión de seguridad adaptado a este contexto específico. Se identificaron y evaluaron activos críticos de información geográfica y se analizaron riesgos importantes como accesos no autorizados, pérdida de datos y ataques de malware.

La implementación de controles de seguridad, el desarrollo de políticas y procedimientos específicos, y la capacitación del personal demostraron ser estrategias efectivas para mejorar la seguridad de la información geográfica. La creación de directrices claras para el acceso y uso de la información geográfica, así como la gestión de incidentes, ha fortalecido la seguridad en las empresas públicas. Además, la formación continua del personal en temas de ciberseguridad es esencial para prevenir y manejar incidentes de seguridad. Establecer un proceso de revisión periódica de las políticas y controles de seguridad asegura que se adapten a nuevas amenazas y desafíos tecnológicos, que destacan la importancia de implementar medidas de seguridad adecuadas para los Sistemas de Información Geográfico (SIG). Sin embargo, este artículo se enfoca específicamente en el contexto ecuatoriano, abordando las brechas existentes en la implementación de estas prácticas en el sector público.

Los aspectos sobresalientes del artículo incluyen la identificación y valoración de activos, que es un proceso esencial para priorizar las medidas de protección necesarias. La evaluación de riesgos permite identificar y mitigar amenazas significativas, asegurando la continuidad de los servicios públicos. La implementación de controles de seguridad mejora la protección de la información geográfica, reduciendo la incidencia de problemas de seguridad. El establecimiento de políticas y procedimientos fortalece la estructura de seguridad organizacional, mientras que la educación y capacitación aumentan la capacidad del personal para manejar y proteger la información geográfica.

Agradecimientos

Quiero expresar mi más profundo agradecimiento a todas las personas que han sido fundamentales en la realización de este trabajo. En primer lugar, a mi querida esposa Daniela, cuyo amor, apoyo incondicional y paciencia han sido mi mayor fortaleza. Su constante aliento y comprensión durante los momentos difíciles y su fe en mis capacidades me han dado la energía para seguir adelante. Daniela, gracias por estar siempre a mi lado y por creer en mí.

A mis hijos, por ser mi fuente de inspiración y motivación constante. Noelia, tu alegría, curiosidad y creatividad son un faro de luz en mi vida, y tu capacidad de hacerme sonreír en los momentos más difíciles me ha brindado una perspectiva invaluable. Juan Fernando, tu presencia, aunque reciente, ha llenado nuestro hogar de amor y esperanza. Tus sonrisas y la inocencia de tus primeros meses de vida me recuerdan la importancia de luchar por un futuro mejor para ustedes.

A mis padres, por su amor, sacrificio y enseñanzas, que han formado la base de mi carácter y determinación. A mis hermanos, Christian, Gabriela y Lenin, por su respaldo y comprensión en todo momento. A mis sobrinos y cuñados, por su apoyo incondicional.

Finalmente, quiero agradecer a mis tutores de la maestría y al personal de la Universidad Católica de Cuenca, por su guía y asesoría a lo largo de este proceso. Su experiencia y conocimientos han sido invaluables para la culminación de este trabajo.

Referencias Bibliográfica

Fingas, J. (2019). Ecuador says it faced 40 million cyberattacks after giving up Assange. Engadget. Obtenido de: https://www.engadget.com/2019/04/16/ecuador-cyberattacks-after-assange-arrest/.

Wang, B., Zhao, Q., & Wei, G. (2024). Detection of Geographic Information System Security Hazards in the IoT Based on Network Security Situation Awareness. Journal of Testing and Evaluation. Obtenido de: https://asmedigitalcollection.asme.org/testingevaluation/article/doi/10.1520/JTE20230065/1199558.

Azaz, L. (2011). The use of geographic information systems (GIS) in business. International Conference on Humanities. Obtenido de http://mlsvc01-prod.s3.amazonaws.com/f27e9ca7001/7290b7e9-0fb4-4394-9817-b2234970b27b.pdf.

Longley, P. A., Goodchild, M. F., Maguire, D. J., & Rhind, D. W. (2001). New Developments in Geographical Information Systems; Principles, Techniques, Management and Applications. Obtenido de https://www.geos.ed.ac.uk/~gisteac/gis_book_abridged/files/pref.pdf.

Peggion, M., Bernardini, A., & Bernardini, C. (2008). Geographic information systems and risk assessment. Office for Official Publications of the European Communities. Obtenido de https://publications.jrc.ec.europa.eu/repository/bitstream/JRC42503/gis_risk_assessment_jan%2007%202008.pdf.

Alzahrani, N. A., & Sheikh Abdullah, S. N. H. (2021). The adoption of geographic information systems in the public sector of Saudi Arabia: a conceptual model. Mathematical Problems in Engineering. Obtenido de https://www.hindawi.com/journals/mpe/2021/1099256/.

Cárdenas Solano, A. J., Martínez Ardila, A. M., & Becerra Ardila, G. A. (2016). Normas y estándares de seguridad de la información. Bogotá: Universidad Nacional de Colombia.

Bork et al., 2024: Implementación de ISO 27001 en la gestión de seguridad de la información mejora la calidad de los servicios proporcionados. Obtenido de: https://juser.fz-juelich.de/record/1020011/files/110_387_Hoffmann_et_al.-2.pdf.

Wysokińska et al., 2023: Adopción de ISO 27001 en organizaciones mejora la gestión de la seguridad de la información. Obtenido de: https://managementpapers.polsl.pl/wp-content/uploads/2024/01/184-Wysoki%C5%84ska-Zawierucha-Koz%C5%82owska-1.pdf.

Mera-Amores y Roa, 2024: Conformidad con ISO 27001 mejora la gestión de seguridad de la información en pequeñas y medianas empresas. Obtenido de: https://link.springer.com/chapter/10.1007/978-3-031-53963-3_14.

Gobernanza de la Gestión del Riesgo de Desastres, 2022: Lineamientos que subrayan la necesidad de mejorar los sistemas de información geográfica y la gestión de riesgos en Ecuador. Obtenido de: https://www.gestionderiesgos.gob.ec/wp-content/uploads/2022/02/LineamientosGobernanzaGAD_24012022.pdf.

Remache Coyago, J. P., Puente Moromenacho, C. A., Noroña Merchán, M. E., & Jerez Mayorga, F. (2018). La seguridad de la información según ISO 27001. Quito.