RPNS: 2090 | ISSN: 2074-0735
Volumen 22 (2026)
n°1 (enero - marzo)

Recibido: *25/abril/2025* ***Aceptado:*** *16/julio/2025*

La seguridad y privacidad de la información en los sistemas de información gerencial (Revisión)

Information security and privacy in Management Information Systems (Review)

Marilyn Jamibeth Alay Ponce. *Estudiante de la Universidad Estatal del Sur de Manabí. Manabí, UNESUM, Ecuador.* [alay-marilyn3160@unesum.edu.ec]
[https://orcid.org/0009-0006-3405-2695]

Scarlen Mallely Sánchez Baque. *Estudiante de la Universidad Estatal del Sur de Manabí, Manabí, UNESUM, Ecuador.* [sanchez-scarlen9652@unesum.edu.ec]
[https://orcid.org/0009-0009-7025-4501]

Lorena Maricela Vera Vera. *Estudiante de la Universidad Estatal del Sur de Manabí. Manabí, UNESUM, Ecuador.* [vera-lorena6293@unesum.edu.ec]
[https://orcid.org/0009-0006-1163-529X]

Carlos Zea Barahona. *Economista. Docente de la Carrera Administración de Empresas de la Universidad Estatal del Sur de Manabí, UNESUM, Manabí, Ecuador.*
[carlos.zea@unesum.edu.ec] [https://orcid.org/0000-0001-7546-7148]

Resumen

La seguridad de la información en los sistemas de información gerencial implica proteger los datos importantes y privados de una empresa, implementar medidas, técnicas organizativas y legales que garanticen la confidencialidad, integridad y disponibilidad de la información, así como el cumplimiento de las leyes y regulaciones de privacidad. Esto se hace para evitar que sean mal utilizados, accedidos sin permiso, interrumpidos o destruidos, es decir, se enfoca en asegurar que la información sea confidencial. Este estudio tiene como objetivo principal **a**nalizar la seguridad y privacidad de la información en los sistemas de información gerencial. La metodología tiene un enfoque cualitativo mediante la revisión bibliográfica de artículos científicos, revistas, tesis y sitios web. Los resultados de esta investigación muestran que, la seguridad y privacidad de la información en los sistemas de información gerencial son una parte fundamental para proteger la información y evitar el uso inadecuado de los datos. Se evidenció la existencia de algunas normativas como las ISO/IEC y la Ley Orgánica de Protección de Datos Personales que pueden guiar la protección, así como medidas basadas en el análisis de riesgos. Este estudio también demuestra que existe una estrecha relación entre los riesgos, la privacidad y

las normativas, ya que estos elementos trabajan en conjunto para asegurar una gestión responsable, segura y eficiente de la información dentro de las organizaciones.

Palabras claves: Normativas; herramientas; software; protección; confidencialidad

Abstract

Information security in management information systems involves protecting a company's important and private data, implementing organizational and legal measures and techniques to guarantee the confidentiality, integrity, and availability of information, as well as compliance with privacy laws and regulations. This is done to prevent misuse, unauthorized access, interruption, or destruction of information; in other words, it focuses on ensuring that information remains confidential. This study aims to analyze information security and privacy in Management Information Systems. The methodology employs a qualitative approach through a bibliographic review of scientific articles, journals, theses, and websites. The results of this research show that information security and privacy in management information systems are fundamental to protecting information and preventing its misuse. The study identified the existence of standards such as ISO/IEC and the Organic Law on the Protection of Personal Data, which can guide protection efforts, as well as measures based on risk analysis. This study also demonstrates a close relationship between risk, privacy, and regulations, as these elements work together to ensure responsible, secure, and efficient information management within organizations.

Keywords: Regulations; tools; software; protection; confidentiality

Introducción

La información es el activo más importante de cualquier organización, ya que es la materia prima para proveer servicios y/o productos, y cumplir con las exigencias y expectativas de los clientes. Con los avances tecnológicos que se desarrollan a diario, las personas tienen diversas herramientas y dispositivos a su disposición, como celulares, portátiles, dispositivos inteligentes, entre otros, y requieren mayor velocidad y acceso a cualquier tipo de información, con el fin de aplicarlas y aprovecharlas en los diferentes aspectos de su diario vivir (Pinto et al., 2024).

La seguridad de la información se refiere a medidas de protección de la privacidad digital que se aplican para evitar el acceso no autorizado a los datos, los cuales pueden encontrarse en ordenadores, bases de datos y sitios web, protegiendo los datos de una posible

corrupción. Actualmente organizaciones de todo el mundo invierten fuertemente en la tecnología de información relacionada con la ciberdefensa con el fin de proteger sus activos críticos: su marca, capital intelectual y la información de sus clientes (López, 2025).

En las organizaciones la seguridad de la información era considerada solamente como gasto general, ahora se ha transformado en inversión para las empresas; y se enfrenta, constantemente, a retos de justificación económicas de inversiones importantes que deben ser argumentados por los equipos responsables, respondiendo preguntas de cómo, por qué, para qué, con quién (Montoya, 2024). Ante lo explicado, nuestra investigación está orientada por las siguientes preguntas de investigación, ¿cuáles son las normativas existentes para la seguridad y privacidad de la información?, ¿de qué manera se determinan las medidas de seguridad y privacidad que implementan los sistemas de información para protección de la información?, ¿qué relación existe entre los riesgos de seguridad, privacidad y normativas existentes para regularla? Mediante la resolución de estas preguntas se desarrolla la investigación, cuyo objetivo principal es analizar la seguridad y privacidad de la información en los sistemas de información gerencial

La presente investigación tiene un enfoque cualitativo analizando las diferentes perspectivas teóricas ya existentes sobre la seguridad y privacidad de la información en los sistemas de información gerencial, permitiendo un estudio sobre interpretaciones que ya existen de los riesgos, desafíos y soluciones que enfrentan el entorno gerencial en el tema de la seguridad. La metodología utilizada es de revisión bibliográfica, recopilando información de artículos científicos, revistas, sitios web y normativos, publicadas de los últimos cinco años. La información recopilada y analizada fue obtenida de artículos nacionales e internacionales, de alto impacto, así mismo de tesis con informaciones claras del tema y de revistas, asegurando que los hallazgos encontrados sean de utilidad para futuras investigaciones. El análisis de la información recopilada permitió identificar enfoques teóricos, buenas prácticas y problemas frecuentes que se presentan en la protección de datos y la gestión de seguridad en los sistemas de información dentro de la toma de decisiones gerenciales.

Desarrollo

Según Barcia (2023), la seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no

autorizada. Esta definición básicamente significa que se debe proteger datos y recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos. Para González (2025), la privacidad de los datos se centra en los derechos individuales de interesados, es decir, en los usuarios que poseen los datos. Para las organizaciones, la práctica de la privacidad de los datos es una forma de implementar políticas y procesos que permitan a los usuarios controlar sus datos de acuerdo con las regulaciones de privacidad de los datos pertinentes.

Montecino (2023) argumenta que los sistemas de información son sistemas de recogida, almacenamiento y transmisión de información; son un conjunto ordenado de procesos y herramientas cuyo fin es administrar datos e información, de manera que puedan ser recuperados y procesados fácil y rápidamente. Ante lo observado por estos autores, se puede decir que la seguridad y privacidad de la información en la parte gerencial cumple un rol importante al momento de querer confidencialidad de datos que solo le pertenezcan a la organización o persona dueña de la información guardada, y que solo aquella decide con quién compartir dicha información.

Normas para la seguridad de la información

En una época en la que los datos y la información se comercializan como si fueran mercancías, es esencial protegerlos. Una forma de hacerlo es aplicar una gestión de la seguridad de la información basada en la serie de normas de seguridad de la información ISO/IEC 2700x. Se trata de una familia internacional de normas para la seguridad informática y de la información en organizaciones privadas, públicas o sin ánimo de lucro.

Norma ISO/IEC 2700x

ISO/IEC 27001: Un Sistema de Gestión de Seguridad de la Información (SGSI) ISO 27001 define los requisitos, reglas y métodos para garantizar la seguridad de la información que requiere protección en las organizaciones. La norma ISO proporciona un modelo para establecer, implementar, supervisar y mejorar el nivel de protección. El objetivo es identificar los riesgos potenciales para la empresa, analizarlos y hacerlos controlables mediante las medidas adecuadas. La norma ISO 27001 formula los requisitos de dicho sistema de gestión, que se auditan en el marco de un proceso de certificación externa, es decir, sirve de base para implementar controles y proteger la información en organizaciones públicas y privadas.

ISO/IEC 27002: Esta norma brinda orientación sobre los controles de seguridad de la información, es una guía con recomendaciones para la implementación de las medidas de la ISO 27001.

ISO/IEC 27005: La norma ISO 27005 ofrece orientación sobre la gestión de riesgos de la seguridad de la información y apoya los conceptos generales al respecto establecidos en la norma ISO 27001.

ISO/IEC 27006: Esta norma describe los requisitos que deben seguir los organismos de certificación al evaluar los sistemas de gestión de sus clientes según la norma ISO 27001 para su certificación.

ISO/IEC 27007: La norma es una guía para la realización de auditorías y está dirigida a los auditores internos y externos que evalúan un SGSI según la norma ISO 27001.

ISO/IEC 27701: Esta norma es una extensión de la ISO 27001, ISO 27002 se enfoca en la gestión de la protección de datos personales, aplicable a controladores y procesadores de datos, alineando controles de seguridad y privacidad.

ISO/IEC 27017: La norma proporciona orientación sobre las medidas de seguridad de la información en la computación en nube dentro de las normas de seguridad de la información.

ISO/IEC 27018: La norma ISO 27018 proporciona orientación para garantizar que los proveedores de servicios en la nube ofrezcan controles de seguridad de la información adecuados para proteger la privacidad de los clientes de sus clientes, asegurando los datos personales que se les confían (Pinargote, 2021).

La Ley Orgánica de Protección de Datos Personales (LOPDP, 2021) garantiza el derecho a la protección de datos personales, estableciendo principios como el consentimiento informado, finalidad específica, proporcionalidad, seguridad y confidencialidad en el tratamiento de datos personales. Además, regula la recolección, archivo, procesamiento y difusión de datos, asegurando la calidad y exactitud de los mismos. Esta normativa se basa en la Constitución ecuatoriana y busca proteger los derechos digitales y la privacidad de los ciudadanos en el entorno digital.

Para garantizar que los datos personales no se conserven más tiempo del necesario, el responsable del tratamiento establecerá plazos para su supresión o revisión periódica. La conservación ampliada de tratamiento de datos personales únicamente se realizará con fines de archivo en interés público, fines de investigación científica, histórica o estadística, siempre y

cuando se establezcan las garantías de seguridad y protección de datos personales, oportuna y necesaria, para salvaguardar los derechos previstos en esta norma.

Los responsables y encargados de tratamiento de los datos personales deberán implementar todas las medidas de seguridad adecuadas y necesarias, entendiéndose por tales las aceptadas por el estado de la técnica, sean estas organizativas, técnicas o de cualquier otra índole, para proteger los datos personales frente a cualquier riesgo, amenaza o vulnerabilidad, atendiendo a la naturaleza de los datos de carácter personal, al ámbito y el contexto (González, 2023).

Para garantizar la protección de la información, los sistemas de información implementan diversas medidas de seguridad y privacidad que abarcan tanto aspectos técnicos como administrativos. Entre estas medidas se incluyen el uso de cifrado de datos, autenticación multifactorial, control de accesos, monitoreo continuo, copias de seguridad periódicas y políticas de gestión de incidentes. Asimismo, se aplican normas y marcos regulatorios como ISO/IEC 27001 o la LOPDP (2021), que aseguran el cumplimiento de estándares internacionales en la gestión segura de la información. Estas prácticas buscan prevenir accesos no autorizados, pérdida de datos y vulnerabilidades, garantizando la confidencialidad, integridad y disponibilidad de los datos.

Medidas básicas para proteger la información

Cuando se habla de información en la empresa se refiere a uno de los activos más importantes que estas poseen. El trabajo de las organizaciones está basado en el uso y gestión que se hace de esta, siendo crucial en el día a día de una empresa. La información debe estar rigurosamente catalogada y ser accesible para así poder consultarla y clasificarla fácilmente según las necesidades. Así pues, debe estar salvaguardada y controlada para evitar que algún agente externo pueda acceder a ella, modificándola o destruyéndola (Farfán & Catalán, 2024). Entre las medidas más significativas están:

1. Controles de acceso a los datos más estrictos. Es una de las principales medidas de seguridad, su objetivo es limitar el acceso a la información. Cuantas menos personas accedan a una información, menor será el riesgo de comprometerla. Por lo tanto, es necesario implantar en nuestra empresa un sistema que impida dar acceso a datos innecesarios, a un usuario o cliente.

2. Realizar copias de seguridad. Poseer un sistema de copias de seguridad periódico permite que la empresa garantice que pueda recuperar los datos ante una incidencia de carácter

catastrófico, impidiendo la pérdida de los mismos y permitiendo la recuperación de la normalidad en el trabajo en apenas unos minutos.

3. Utilizar contraseñas seguras. El acceso a las distintas plataformas que utiliza la empresa (correo electrónico, servidor de copias de seguridad, entre otros) debe realizarse utilizando claves de seguridad (contraseñas) seguras, que impidan que puedan ser fácilmente descubiertas por piratas informáticos. El uso de contraseñas seguras es una de las medidas de seguridad informática más importantes en una empresa.

4. Proteger el correo electrónico. Una medida de seguridad es utilizar filtros antispam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de toda esa información.

5. Contratar un software integral de seguridad. Poseer un paquete de seguridad integral que contenga antivirus, anti espías, antimalware, firewall, y que permita proteger la información ante posibles ataques externos a través de internet.

6. Utilizar software DLP. Existen programas de prevención de pérdidas de datos que pueden ser implementados como medida de seguridad en nuestra empresa para supervisar que ningún usuario esté copiando o compartiendo información o datos que no deberían.

7. Trabajar en la nube. Permite, entre otras ventajas, contar con los sistemas de seguridad de la información que posee el proveedor de servicios. Además, este proveedor será responsable de esa seguridad.

8. Involucrar a toda la empresa en la seguridad. Para que las medidas de seguridad informática de una empresa funcionen, debemos involucrar en su participación a todos los estamentos que participan en la misma, incluyendo a los agentes externos como puedan ser clientes o proveedores. Muchas veces, las empresas tienen implantados los sistemas correctos de seguridad, y la brecha en la misma, se produce al relacionarnos con un tercero que carece de estas medidas de seguridad.

9. Monitorización continua y respuesta inmediata. Implementar en la empresa un sistema que permita monitorizar la gestión de los datos y detectar aquellos posibles fallos o actuaciones incorrectas. Este sistema de control permitirá actuar rápidamente para solventar cualquier incidencia y minimizar su repercusión (Bósquez & Torres, 2024).

Tipos de seguridad informática

Seguridad de hardware: Este tipo de seguridad se relaciona con la protección de dispositivos que se usan para proteger sistemas y redes apps y programas de amenazas exteriores, frente a diversos riesgos. Esta seguridad también se refiere a la protección de equipos físicos frente a cualquier daño físico.

Seguridad de software: Este tipo de seguridad se emplea para salvaguardar los sistemas frente ataques malintencionados de hackers y otros riesgos relacionados con las vulnerabilidades que pueden presentar los softwares. A través de estos defectos los intrusos pueden entrar en los sistemas, por lo que se requiere de soluciones que aporten, entre otros, modelos de autenticación.

Seguridad de red: La seguridad de la red está relacionada con el diseño de actividades para proteger los datos que sean accesibles por medio de la red y que existe la posibilidad de que sean modificados, robados o mal utilizados. Las principales amenazas en esta área son: virus, troyanos, phishing, programas espía, robo de datos y suplantación de identidad.

Un sistema de información es el conjunto de técnicas, herramientas y agentes involucrados en la administración y uso de datos para la obtención de objetivos empresariales. Estos sistemas ayudan en la gestión de la información que produce y utiliza una organización para el mejoramiento de procesos y operaciones, se basa en el uso de software para la gestión de datos, en él se agregan todos los procesos y operaciones. Algunas de las funciones más importantes que utilizan las empresas son las siguientes:

- Gestionar y administrar datos e información que componen a una empresa.
- Automatizar procesos internos sin necesidad de contar con intermediarios para ejecutar ciertas operaciones.
- Unificar la información de la empresa a través de almacenes estandarizados para facilitar el uso y la comprensión de los datos generados.
- Brindar información actualizada en tiempo real y disponible para todos los colaboradores o para aquellos encargados de la toma de decisión, lo permite agilizar y mejorar procesos y actividades de forma rápida.
- Favorecer un mejor aprovechamiento del tiempo que tus empleados disponen para ciertas actividades.

Los elementos de un sistema de información son el software, el hardware, las personas, las técnicas y los datos.

Tipos de sistemas de información

Los sistemas de información cuentan con la ventaja de que no solo tienen una única función y pueden ser útiles para todo tipo de sectores e industrias, dependiendo de sus necesidades y solicitudes. Para ello existen diferentes tipos de sistemas que cumplen con funcionalidades especiales. Entre ellos se encuentran los Sistemas de procesamiento de transacciones, los Sistemas de información gerencial, los Sistemas de control de procesos de negocio, los Sistemas de información de marketing, los Sistemas de colaboración empresarial, los Sistema de apoyo a la toma de decisiones y los Sistemas de información ejecutiva (Vitale & Chaves, 2024).

Los resultados de la investigación sobre qué tan importante es la seguridad y privacidad de la información en los sistemas de información gerencial se muestran a continuación, estos resultados se basaron en las tres preguntas de investigación que fue un factor clave para el direccionamiento de la misma.

Como respuesta a la primera pregunta ¿cuáles son las normativas existentes para la seguridad y privacidad de la información? Los estudios analizados mostraron una serie de normativas dentro del grupo de lasNormas ISO/IEC 2700x que se utilizan en la parte gerencial para asegurar que no se difunda información confidencial. Se detallan a continuación las normativas existentes encontradas en la investigación: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27005, ISO/IEC 27006, ISO/IEC 27007, ISO/IEC 27701, ISO/IEC 27017, ISO/IEC 27018. Otra normativa que garantiza la privacidad y protección de datos es la LOPDP (2021), esta normativa es ecuatoriana y está basada en la constitución.

Como respuesta a la segunda pregunta de investigación ¿de qué manera se determinan las medidas de seguridad y privacidad que implementan los sistemas de información para protección de la información? Las medidas de seguridad y privacidad en los sistemas de información se establecen a través de un análisis de riesgos, el cumplimiento de normativas, y la implementación de controles que sean adecuados y relacionados a la sensibilidad de la información y a los objetivos de una organización.

En base a la tercera pregunta de investigación, ¿qué relación existe entre los riesgos de seguridad, privacidad y normativas existentes para regularla? En los sistemas de información los

riesgos de seguridad, la privacidad y las normativas que regulan el uso de los datos están completamente conectados. Los riesgos de seguridad se refieren a amenazas que pueden comprometer la confidencialidad, integridad y disponibilidad de la información, como accesos no autorizados, pérdidas de datos o ciberataques. Estos riesgos afectan directamente la privacidad de los usuarios, para reducir estos riesgos y garantizar la privacidad, existen normativas legales para que las organizaciones puedan implementar medidas de seguridad que aseguren una gestión adecuada de los datos. Una vinculación unida de aquello está en que la seguridad previene incidentes, la privacidad protege los derechos individuales, y las normativas garantizan que ambos aspectos sean cumplidos de forma obligatoria y estandarizada.

La investigación contribuye con perspectivas complementarias que permiten comprender la seguridad y privacidad de la información desde varias dimensiones. Al respecto, Barahona et al. (2024) destacan la importancia de la información como activo fundamental y la necesidad de acceso rápido en la era tecnológica, estableciendo un marco para la relevancia de la seguridad y privacidad. Por otro lado, Cardozo y Tulio (2025) aportan una visión sobre el aumento del riesgo de manipulación y exposición de la información debido a la evolución tecnológica y la insuficiencia de los sistemas para protegerla, subrayando la problemática que justifica la necesidad de seguridad de la información.

La seguridad de la información ya no es solo un gasto, sino una inversión, que requiere justificación económica y argumentación por parte de los responsables. Esto aporta una dimensión gerencial y estratégica (Montoya, 2024). González (2025) comparte sobre la noción específica de privacidad de datos, destacando el enfoque en los derechos individuales y el control que los usuarios deben tener sobre su información, ampliando la discusión hacia la dimensión legal y ética.

La LOPDP (2021) de Ecuador, regula la protección de datos personales, enfatizando principios como consentimiento, seguridad, confidencialidad y derechos digitales (González, 2023). Esto amplía la discusión hacia el cumplimiento normativo y la responsabilidad legal. Las recomendaciones prácticas basadas en fuentes como Farfán y Catalán (2024) y Bósquez y Torres (2024), establecen las medidas concretas para proteger la información en la empresa, desde controles de acceso hasta monitorización continua, mostrando la aplicación práctica y diaria de los conceptos y normas mencionados.

Conclusiones

Luego de analizar toda la información recopilada se puede concluir que la seguridad y la privacidad de los datos se han convertido en aspectos fundamentales dentro de cualquier organización. Hoy en día, la información no solo representa un recurso valioso, sino que es la base para ofrecer servicios, tomar decisiones y mantenerse competitivos.

Los avances tecnológicos han abierto nuevas oportunidades, pero también han incrementado las amenazas cibernéticas, haciendo indispensable que las empresas adopten sistemas de información seguros con políticas claras y herramientas de protección eficaces. En este ámbito, la seguridad de la información ya no es vista como un gasto innecesario, sino como una inversión estratégica que permite a las organizaciones garantizar la confidencialidad, integridad y disponibilidad de sus datos.

Las normas internacionales, como la familia ISO/IEC 27000, junto con leyes nacionales como la LOPDP en Ecuador, establecen un marco fundamental para gestionar los riesgos y proteger los derechos de los usuarios. Por ello, proteger la información en las organizaciones debe ser una responsabilidad y compromiso de los involucrados, aplicando medidas claras y prácticas que garanticen el uso seguro y correcto de los datos.

Referencias bibliográficas

Barahona, G. E., Barzola, Y. G., & Peñafiel, L. V. (2024). El derecho a la protección de datos y el avance de las nuevas tecnologías en Ecuador: Implicaciones legales y éticas. *Journal of Economic and Social Science Research*, 4(3), 46-64, 2024. https://economicsocialresearch.com/index.php/home/article/view/113

Barcia, G. A. (2023). *Implementación del estándar ISO/IEC 27001 para la seguridad de la información en la unidad educativa fiscal cultura Machalilla* [Tesis de grado, Jipijapa-UNESUM]. http://repositorio.unesum.edu.ec/handle/53000/5917

Bósquez, E. I., & Torres, M. M. (2024). Auditoría continua y monitorización en tiempo real: detección, mitigación de riesgos empresariales en industrias hoteleras. *Revista Metropolitana De Ciencias Aplicadas*, 7(S2), 76-86. https://doi.org/10.62452/q62zma54

Cardozo, J. P., & Tulio, V. J. (2025). *Diseño de políticas y controles de seguridad de la información* [Tesis de grado, Universidad El Bosque]. https://hdl.handle.net/20.500.12495/14876

Constitución de la República de Ecuador. (2021, 26 de mayo). Ley Orgánica de Protección de Datos Personales. Quinto Suplemento del Registro Oficial No.459. https://deltechaudit.ec/wp-content/uploads/2025/04/LEY-DE-DATOS-PERSONALES.pdf

Farfán, P. M., & Catalán, I. D. (2024). *La importancia de la gestión de activos físicos dentro de una organización para la toma de decisiones de inversión*. Universidad de Antioquia. https://hdl.handle.net/10495/44611

González, A. (2025). *La política de privacidad en la investigación de mercados* [Tesis de grado, Universidad de Valladolid]. UVA Repositorio documental. https://uvadoc.uva.es/handle/10324/77459

González, I. (2023). Protección de datos y seguridad de la información. *Revista Canaria De Administración Pública*, *1*, 285-311. https://doi.org/10.36151/RCAP.2023.9

López, W. L. (2025). *Plan de seguridad de la información para la prevención de accesos no autorizados a la información en el Gobierno Autónomo Descentralizado del Cantón Montalvo*. Babahoyo: UTB-FAFI. https://dspace.utb.edu.ec/handle/49000/17920

Montecino, L. A. (2023). *Diseño de un aplicativo para el mejoramiento del sistema de información del programa ampliado de inmunizaciones en instituciones prestadoras de salud, Montería 2.022* [Tesis de grado, Universidad de Córdoba]. https://repositorio.unicordoba.edu.co/server/api/core/bitstreams/31a3ab86-0c57-4c95-b23c-f5d6b7113563/content

Montoya, S. A. (2024). *Gastos por servicios de seguridad de la Empresa Inteligencia Security RMM Cía. Ltda. De la ciudad de Cuenca durante el periodo 2023*. UTB-FAFI. https://dspace.utb.edu.ec/handle/49000/17221

Pinargote, B. J. (2021). *Incidencias de las Normas ISO en la Seguridad Informática para la protección de datos usada por proveedores que ofrecen servicio de Cloud Computing en la ciudad de Guayaquil* [Tesis de maestría, Universidad Tecnológica Empresarial de Guayaquil].

Pinto, L. J., Osorio, M. A., & Fabra, C. I. (2024). *Estrategia para la adopción de tecnologías que automaticen el soporte en línea de primer nivel en el área de atención al cliente de Tecnoinformatica S.A.S. Informe técnico resultado de investigación*. Universidad Ean http://hdl.handle.net/10882/14689

Vitale, K. D., & Chaves, E. A. (2024). *Análisis y Evaluación del Sistema de Información de la Municipalidad de Neuquén para la Gestión de las Compensaciones y sus Principales Dificultades de Interoperabilidad con otros Sistemas de Administración en el Período 2016-2020* [Tesis de grado, Universidad Nacional del Comahue]. https://rdi.uncoma.edu.ar/bitstream/handle/uncomaid/17959/Tesis%20de%20grado%20Vitale -%20Chaves.pdf?sequence=1&isAllowed=y