Ciencias y Saberes

ISSN 2960-8430

RIESGOS DE LA SEGURIDAD INFORMÁTICA EN EL SISTEMA CONTABLE

Ana Mélida Anrango Tayan
ana.anrango1961@utc.edu.ec
Universidad Técnica de Cotopaxi - Ecuador
https://orcid.org/0009-0006-4077-9460

Alison Berenice Toaquiza Toaquiza
alison.toaquiza7173@utc.edu.ec
Universidad Técnica de Cotopaxi - Ecuador
https://orcid.org/0009-0004-2214-4010

Recibido: 02/07/24
Aceptado: 20/08/24
Publicado: 01/09/24

RESUMEN

La evolución tecnológica ha contribuido de manera significativa a las organizaciones en el ámbito contable, reduciendo tiempos en los procesos, mediante la implementación de sistemas informáticos. Por ejemplo, en el área contable, todos los procesos que se realizaban de manera manual fueron reemplazados por procesos electrónicos. Sin embargo, estos avances tecnológicos han traído consigo varios desafíos en temas de seguridad, exponiendo a las organizaciones a riesgos, como los ataques cibernéticos y phishing. La presente investigación tiene como objetivo realizar una revisión documental referente a los riesgos asociados en los sistemas contables. Se aplicó una metodología cualitativa, basada en la recopilación de información de varios artículos científicos de los últimos 5 años publicados. Los resultados muestran que los sistemas contables son vulnerables ante los ataques cibernéticos. Como conclusión, se resalta la importancia de implementar políticas de seguridad informática, capacitar al personal de trabajo y adoptar tecnologías de protección de datos, para garantizar la seguridad en los sistemas informáticos con la finalidad de minimizar los riesgos; además, es esencial realizar copias de seguridad periódicas y almacenarlas en la nube, para garantizar la protección de la información.

Palabras clave: riesgos informáticos, seguridad informática, ciberdelincuencia, sistemas contables.

COMPUTER SECURITY RISKS IN THE ACCOUNTING SYSTEM

ABSTRACT

Technological evolution has contributed significantly to organizations in the accounting area, reducing process times through the implementation of computer systems. For example, in the accounting area, all processes that were performed manually were replaced by electronic processes. However, these technological advances have brought with them several security challenges, exposing organizations to risks such as cyber-attacks and phishing. The purpose of this research is to conduct a documentary review of the risks associated with accounting systems. A qualitative methodology was applied, based on the collection of information from several scientific articles published in the last 5 years. The results show that accounting systems are vulnerable to cyber-attacks. In conclusion, the importance of implementing computer security policies, training staff and adopting data protection technologies to ensure security in computer systems in order to minimize risks is highlighted; in addition, it is essential to perform regular backups and store them in the cloud to ensure the protection of information.

Key words: computer risks, computer security, cybercrime, accounting systems.

Correo principal para contacto: ana.anrango1961@utc.edu.ec

1. INTRODUCCIÓN

La evolución tecnológica ha generado innumerables beneficios, pero también ha dado lugar a varios riesgos que afectan a los sistemas contables de las organizaciones y al ser humano que está expuesto en la red. El primer caso de vulnerabilidad ocurrió en el año de 1978, cuando el colapso de varios sistemas presento fallas en su funcionamiento; a partir de ese instante, comenzaron a surgir amenazas como virus, ataques cibernéticos, códigos maliciosos, entre otros. Los riesgos informáticos se definen como amenazas y vulnerabilidades que afectan los procesos operativos de toda organización y que al final tienen consecuencias negativas.

Con el auge de la revolución tecnológica en el ámbito empresarial, nacen nuevas tecnologías informáticas que impactan significativamente en la economía, desarrollando sistemas informáticos para el procesamiento electrónico de la información. Esto implica grandes transformaciones cualitativas en la contabilidad y el control sobre el concepto tradicional del Control Interno y la estructura de los registros contables (Martínez, 2020).

La creación de los sistemas informáticos ha facilitado las actividades laborables y educativas. El siguiente autor menciona la importancia de mantener una educación en el ámbito digital: "la importancia de la seguridad informática en la educación digital es un tema relevante y actual que requiere una atención especial debido a los constantes avances tecnológicos y la creciente dependencia de las herramientas digitales en los entornos educativos" (Guaña-Moya, 2023, p. 3). En este sentido, la seguridad informática es una de las bases principales para reducir los riesgos cibernéticos y la ciberdelincuencia, a través del planteamiento de políticas de seguridad y controles.

El desarrollo tecnológico se ha convertido en un recurso importante para el funcionamiento y crecimiento económico de las organizaciones. La implementación de sistemas informáticos ha permitido optimizar tiempos, para así lograr una eficiencia laboral. En el ámbito contable, la creación e implementación de sistemas contables ha agilizado significativamente los procesos contables que anteriormente se llevaban a cabo de forma manual. Por ejemplo, las facturas impresas han sido sustituidas por la facturación electrónica, al igual que los pedidos, órdenes de compra, entre otros. Toda la información contable se realiza y se almacena ahora en un software contable especializado, lo que ha llevado a la sustitución de la mayoría de procesos contables en papel por aparatos tecnológicos más eficientes y seguros.

No obstante, el principal problema de los sistemas contables en relación a la seguridad informática, es que están expuestos a varios riesgos como amenazas y vulnerabilidades. Los riesgos significativos son ciberataque, ciberdelincuencia y el phishing. Estos son los principales y más usados para filtrar y extraer información financiera, con la finalidad de realizar un fraude económico o chantajes, comprometiendo así a las organizaciones y a la vez generando grandes pérdidas económicas. En este tema, Colombia es uno de los países que presenta una mayor actividad de ciberdelincuencia, donde usan la tecnología para ingresar a los sistemas de seguridad. Cabe recalcar que la seguridad informática para la protección de datos en los sistemas contables es un tema de suma importancia en la era digital, permitiendo

protegiendo a toda la organización ante cualquier amenaza que afecte información confidencial.

En este contexto, esta investigación es fundamental para las personas y empresas que utilizan varios sistemas informáticos para optimizar sus actividades. Se resalta la importancia de implementar políticas de seguridad, para enfrentar los principales riesgos cibernéticos y de esta manera proteger la confidencialidad de la información. Por lo tanto, el principal objetivo de esta investigación es realizar una revisión documental sobre los riesgos asociados a los sistemas contables, a través de un análisis de varios antecedentes investigativos, donde se exponen los principales riesgos presentes en los sistemas informáticos, destacando especialmente la importancia de la seguridad informática.

Riesgos en el sistema informático

Los riesgos informáticos presentan una amenaza que afecta a todos, con consecuencias significativas a nivel empresarial, que puede tener consecuencias graves que afectan de manera física y económica. Sin embargo, existen varias definiciones, que con el tiempo han cambiado.

Para Muñoz et al. (2019), el riesgo informático se define como "la combinación de una amenaza y vulnerabilidad, representada a través de la fórmula riesgo = amenaza + vulnerabilidad. Las empresas poseen un conjunto de elementos, denominados activos que están expuestos a riesgos que van ligados a amenazas y vulnerabilidades" (p. 4). Esto indica que, si una computadora no tiene, los respectivos sistemas de protección de seguridad, estaría expuesta a situaciones vulnerables como ciberdelincuencia.

Los casos de ciberdelincuencia son los más comunes en América Latina. "Colombia es uno de los países donde existen grupos armados que usan la tecnología. Estos crean programas para intervenir en los sistemas de seguridad social de empleados con la finalidad de robar contraseñas e identificaciones asociadas a información financiera" (Muñoz et al., 2019, p. 6). Muchas de las empresas colombianas, como el personal administrativo, se han visto afectados debido a que han perdido información importante sobre el manejo de dinero de las organizaciones. De igual manera, los cajeros automáticos son los más vulnerables.

En definitiva, la ciberdelincuencia es un factor representativo que enfrentan las organizaciones, es un riesgo común al que están expuestas. Los delincuentes son astutos para el robo y manejo de datos importantes de una organización. Afortunadamente, también existen programas que protegen este riesgo.

Seguridad informática

> La seguridad informática se trata sobre la protección de información de índole personal, empresarial o gubernamental, contenida no solo en la red, sino también en los dispositivos de uso diario como teléfonos celulares, tabletas, computadoras de escritorio, laptop o cualquier dispositivo digital, de amenazas que puedan poner en riesgo la información almacenada o transportada en alguno de los dispositivos (Gamboa, 2020, p.7).

La seguridad informática no solo es prevención, sino detectar y corregir a tiempo estos ataques, para así reducir los riesgos de ciberataques. “La seguridad informática ha hecho tránsito de un esquema caracterizado por la implantación de herramientas de software que neutralizan el acceso ilegal y los ataques a los sistemas de información” (Ramos, et al., 2023, p. 6).

Actualmente, la seguridad informática es más digitalizada y corre el riesgo que personas no autorizadas ingresen a bases de datos y hagan mal uso de la información. Cabe mencionar que la mayoría de entidades financieras tienen programas, que emiten notificaciones en tiempo real, cuando ingresa una persona extraña a la base de datos. Es así que programas de seguridad de la información buscan mitigar riesgos asociados al manejo de información y a los recursos tecnológicos que dan soporte. Estos programas se fundamentan en tres principios básicos:

Integridad: garantizan que la información sea exacta, completa y sin modificaciones no autorizadas. Este principio asegura que ni usuarios ni procesos no autorizados alteren el contenido de los datos. Los cambios pueden darse tanto en el contenido como en el entorno que los soporta.

Confidencialidad: previene el uso no autorizado de la información por parte de personas no autorizadas. Los datos deben ser accesibles únicamente para individuos o grupos específicos definidos por el responsable de la información. Este principio está estrechamente vinculado con la privacidad, que ha adquirido mayor relevancia y claridad en su aplicación en los últimos años.

Disponibilidad: asegura que los usuarios puedan acceder a recursos de información de manera oportuna y fiable, lo que permite continuidad operativa del negocio.

Estos principios son esenciales para desarrollar e implementar políticas de seguridad de la información. Juntos, apoyan la idea de proteger la información como un recurso estratégico para el negocio, otorgándole el valor que merece (Rocha, 2020).

Sistema contable

El sistema contable agrupa personas, recursos y conocimientos para recolectar, organizar, resumir y analizar la información que generan las transacciones, los hechos económicos y las actividades realizadas por una entidad. “También, permite asegurar la integridad de los datos, el adecuado registro y procesamiento de las operaciones, la presentación de la información financiera de forma confiable y, además, debe garantizar la oportunidad en la presentación de las informaciones”. (Cristo, 2021, p. 6)

Estos sistemas de información contable tienen la finalidad de realizar transacciones y generar información confiable, libre de error, para de esta manera aumentar el rendimiento operacional. Estos se conforman por elementos como: hardware, software, recursos humanos, políticas y normas contables, etc., que permite el funcionamiento de los sistemas.

Políticas de seguridad informática

Las políticas son requisitos generalizados que deben ser escritos en papel y comunicados a ciertos grupos de personas, dentro y en algunos casos fuera de la organización. Aunque las políticas de seguridad informática varían de una organización a otra, un típico documento de este tipo incluye: una exposición de motivos, la descripción de las personas a quienes van dirigidas las políticas, el historial de las modificaciones efectuadas, unas cuantas definiciones de términos especiales y las instrucciones gerenciales específicas sobre el tratamiento de estas. Estas son obligatorias y pueden considerarse como una ley propia dentro de la organización.

> Una política de seguridad son un conjunto de directrices, normas, procedimientos e instrucciones que guía las instrucciones de trabajo y definen los criterios de seguridad para que sean adoptados a nivel local o institucional, con el objetivo de establecer, estandarizar y normalizar la seguridad tanto en el ámbito humano como tecnológico. (Dussan, 2022)

De igual manera, la información implementada por la organización para proteger su información puede ser uno de los temas que pueden generar controversia. La razón es que, a pesar de la existencia de esta información, la seguridad de la información es violada por factores humanos. Los diferentes roles que desempeñan las personas, como usuarios finales, administradores de equipos de seguridad, administradores de información, administradores de políticas de seguridad, atacantes de sistemas de información, tendrán diferentes efectos y consecuencias para cada situación. Como consecuencia, la seguridad de la información no es sólo cuestión de tener nombres de usuario y contraseñas, sino que requiere normativas y diversas estrategias de privacidad y protección de datos que impongan obligaciones a la organización (Díaz & Guerra, 2021).

La seguridad de los datos, en la contabilidad se refiere a un conjunto de medidas hacia la protección física de los documentos y archivos contables hasta el resguardo de la información, a través de software de seguridad. El objetivo de la seguridad informática es minimizar el riesgo de pérdida, fraude o mal uso de la documentación contable. La “seguridad de datos en la contabilidad es esencial para proteger la confidenciales almacenados en un sistema contable. Esto incluye la protección contra el acceso no autorizado, la defensa de la integridad de los datos y la conservación de la confidencialidad” (Ríos, 2024, p. 10).

Actualmente, existen varios sistemas que permiten realizar actividades contables de una manera efectiva. Esto facilita el trabajo a todos los profesionales dedicados a la contabilidad. Los softwares contables más utilizados en Ecuador son: Siigo Contífico, Dora, Perseo, Iconta. Estos permiten realizar operaciones como facturación, comprobantes, compras, ventas, pagos, inventarios, depreciaciones, amortizaciones de activos fijos, registros económicos, aperturas y cierres contables, asientos de ajustes. También, estos permiten obtener informes financieros. Las ventajas que estos sistemas brindan son la elaboración de información financiera de manera rápida, oportuna y eficiente, actualizaciones constantes en los procesos de acuerdo a las reformas tributarias y protección ante cualquier error. Las empresas cuentan con diversas fuentes de información que permite conocer su desempeño para

tomar decisiones y determinar medidas específicas para alcanzar sus objetivos (Soto, 2021).

Riesgos informáticos en los sistemas contables

De acuerdo con el avance tecnológico, los fraudes informáticos han aumentado. Una persona experta extrae información importante de la organización, sin dejar rastro alguno de ello. Por tal razón, existen organizaciones que se exponen a varios riesgos informáticos y a la ciberdelincuencia. Ante ello, deben plantear políticas que les permitan salvaguardar su información, como respaldos en caso de sufrir "hackeo" en sus sistemas.

En este sentido, algunos de los riesgos que se puede presentar en el sistema contable pueden ser: riesgos de integridad, riesgos de relación, riesgos de acceso, riesgos de infraestructura, riesgos de seguridad local y riesgos cibernéticos.

Actualmente, los riesgos cibernéticos son los más comunes que una organización puede tener. Esta actividad consiste en robar la información confidencial del cliente por hackers o grupos criminales para ejecutar estafas electrónicas y desfalcos. "El delito de phishing también representa una amenaza, ya que los perpetradores se infiltran mediante correos electrónicos, con el objetivo de obtener información confidencial de las empresas" (Ojeda et al., 2020, p. 8).

Por esta razón, es importante realizar la gestión de riesgos dentro de una organización, es decir, un sistema de control interno que permite tomar acciones pertinentes ante cualquier ciberdelincuencia detectada que afecte las actividades de una organización. Este sistema permite respaldar, actuar y resguardar la información y así evitar exponerla ante personas ajenas o que no estén autorizadas por los jefes.

Seguridad informática en el sistema contable

Es importante el mantenimiento de copias de seguridad de los sistemas contables para la seguridad de la información y de los procesos para así garantizar un buen servicio. Toda organización debe tener políticas de almacenamiento de las copias de seguridad que sean oportunas. Estas copias de seguridad se deben realizar diariamente y almacenarlas en un disco duro. También, se almacena la misma copia en la nube para que una organización tenga mayor confianza.

La ciberseguridad dentro de los sistemas contables es una manera de proteger los procesos contables de la organización, ya que están puede estar expuestos a delitos cibernéticos. La implementación de controles internos y políticas es importante para salvaguardar la confidencialidad de la información contable, y disminuir los riesgos cibernéticos. "Para mitigar estos riesgos, es fundamental implementar medidas de seguridad robustas, como el cifrado de datos, capacitación en ciberseguridad para el personal y copias de seguridad regulares" (Ojeda et al., 2020, p. 10).

Los controles de seguridad constituyen medidas o acciones destinadas a salvaguardar los activos de información de una organización ante posibles amenazas y riesgos. Estos controles se rigen por estándares y marcos de referencia, como la norma ISO 27001, que ofrece un enfoque sistemático para establecer, implementar, mantener y mejorar un sistema de gestión de la seguridad de la información. Asimismo, la norma

ISO 27002 proporciona un conjunto de controles y buenas prácticas específicas para la seguridad de la información en una organización (Muñoz et al., 2019, p. 10).

La implementación de un sistema de gestión de seguridad de la información (SGSI) basado en la norma 27001 es un proceso complejo que comprende tareas como la identificación de activos y de amenazas, el análisis de riesgos y el razonamiento de seguridad; además, la norma exige considerar leyes y reglamentos, así como la preocupación de privacidad. Todos estos requerimientos se convierten en desafíos multidisciplinarios para los ingenieros de seguridad (Manosalve, 2024).

Desde el momento en que una aplicación web, de tipo organizacional, es desplegada en un ambiente de producción bajo una determinada infraestructura es susceptible de recibir ataques malintencionados. La prevención de esos ataques es uno de los principales intereses del área de seguridad de cualquier entidad gubernamental o privada (Moreno & Coronado, 2021).

2. ESTRATEGIAS METODOLÓGICAS / MATERIALES Y MÉTODOS

La investigación fue de tipo descriptivo. Se revisó la bibliografía documental sobre riesgos de la seguridad informática en el sistema contable en libros, revistas y artículos científicos disponibles y validados por varios autores. La información fue obtenida, a través del buscador Google Académico, en las bases de datos Redalyc, Scielo y Dialnet.

Además, se recopiló el enfoque cualitativo que permitió recabar información relacionada a los riesgos en los sistema contables y la seguridad informática. Para ello, se utilizaron palabras claves en el buscador como: riesgos informáticos, seguridad, informática, análisis, vulnerabilidad informática, ciberseguridad, tecnología, nivel de seguridad, riesgos informáticos, alternativas de seguridad, sistemas contables, el rol de la seguridad informática, política informática, seguridad de la gestión informática, ataques informáticos, plan de seguridad, diseños de seguridad, herramientas informáticas.

Una vez realizada la verificación se obtuvo una muestra de 57 documentos recopilados. Posteriormente, se filtraron los documentos según la fecha de publicación, seleccionando documentos publicados en los últimos cinco años, relacionados a los riesgos informáticos, se seleccionaron 30 documentos bibliográficos para realizar un analisis descriptivo. Las Tablas 1, 2 y 3 detallan los artículos seleccionados.

Tabla 1

Artículos seleccionados de Redalyc.

Redalyc		
Títulos	**Autores**	**Año**
Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas**.**	Gil, V. y Gil, J.	2024
Auditoría con informática a sistemas contables.	Martínez, A. Yeiniel, A. y Loy, L.	2023

Diseño de un sistema contable de costos para la finca Yanapanakuna	Pirovano, G.	2022
Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia.	Muñoz, H., Zapata, L. y Requena Vidal.	2020
Políticas de seguridad informática.	Dussan, C.	2020
La interiorización del cambio de un sistema contable de gestión en la pequeña empresa.	Facin,C; Ripoll,V; Palanca,M	2020
La seguridad informática.	Rocha, C.	2020
Seguridad de la información en el intercambio de datos entre dispositivos móviles con sistema android utilizando el método de encriptación RSA.	Solís, F., Pinto, D. y Solís, S.	2021
Metodología para la implementación de la gestión automatizada de controles de seguridad informática.	Cairo, M., Valdés, O. y Perés, I.	2019
Aproximaciones meta-teóricas sobre el constructor de los sistemas contables.	Betancur, H. y Cano, A.	2019

Fuente: autoría propia.

Tabla 2

Artículos seleccionados de Scielo.

Scielo		
Títulos	**Autores**	**Año**
Efectividad de las políticas implementadas para garantizar la seguridad cibernética en Ecuador.	Suárez, J.	2024
Impacto del uso de diversos marcos de seguridad en las auditorías informáticas dentro de las organizaciones: revisión sistemática.	Burgos, M., Haro, C. y Mendoza, A.	2024
Ciberseguridad en servicios de apoyo al médico ocupacional de la ciudad de Lima. Estudio piloto.	Cuadra, R. y Calle, D.	2024
Propuesta de sistema de costos e incidencia en la utilidad de la lavandería Industrial Wash S.A.C.	Soto, J.	2021
Modelo base de conocimiento para auditorías de seguridad en servicios web con inyección SQL.	Moreno, J.	2020
Metodología para la Implementación de la gestión automatizada de controles de seguridad informática.	Cairo, M., Puga, O. y Mallea, I.	2020

Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias.	Guerra, E., Neira, H., Díaz, J. y Patiño, J.	2020
Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia.	Ospina, M. y Sanabria, P.	2020
Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia).	Coronel, I.	2019
El sistema de información en la propiedad horizontal y su relación con los procesos contables.	Rodríguez, O. y Sánchez, X.	2019

Fuente: autoría propia.

Tabla 3

Artículos seleccionados de Dialnet.

Dialnet		
La influencia de los sistemas de información en el desempeño organizacional de la PYME.	Solano, O.	2024
Riesgos y seguridad informática.	Pons, P.	2023
Las ventajas de una aplicación informática para evaluaciones de riesgos, estudios y planes de seguridad.	Sierra, F.	2023
Seguridad en informática.	Quiroz, S. Macías, D.	2022
Inseguridad informática.	Cano, J.	2020
La seguridad informática como motor del desarrollo del e-business.	Núñez, F.	2020
Seguridad informática.	Antón, E.	2019
Seguridad, análisis de riesgos y auditorías en el RGPD.	Pérez, J.	2019
Aplicación informática para la evaluación de riesgos industriales a fin de determinar un indicador de riesgos en empresas venezolanas.	Manduca, L.	2019
Análisis de riesgos informáticos en el sistema contable Syscofin de la empresa Goldenshrimp S.A de la ciudad de Machala.	Pineda, K.	2019

Fuente: autoría propia.

3. RESULTADOS

El análisis de la información recopilada en distintas fuentes académicas revela que los sistemas contables han sido víctimas de constantes ataques cibernéticos. Estos buscan obtener beneficios económicos mediates chantajes, fraudes y robos de información financiera. Entre los principales riesgos identificados se encuentran los

ciberataques, el phishing y la ciberdelincuencia. Todos estos con la finalidad de comprometer los datos contables de las entidades.

A pesar de los avances tecnológicos y la evolución de los sistemas contables, los problemas de seguridad persisten. Sin embargo, las nuevas plataformas cuentan con medidas de protección más avanzadas para mitigar los posibles ataques cibernéticos. Por ello, en los resultados obtenidos es importante la implementación de políticas de seguridad informática y las capacitaciones al personal, ya que estas estrategias permitirán minimizar las amenazas y fortalecer la protección de la información financiera de las organizaciones.

4. CONCLUSIONES / CONSIDERACIONES FINALES

La tecnología es una herramienta excelente que reduce, los tiempos en los entornos laborales y educativos. Los dispositivos electrónicos y los sistemas inteligentes permiten al ser humano desarrollarse de una manera rápida en sus conocimientos. En el ámbito empresarial, optimiza el tiempo en las actividades laborales, lo que se traduce a obtener mejores resultados, cumpliendo con sus metas propuestas a corto y largo plazo. Sin embargo, al analizar esta información presentada, se evidencian los riesgos que presentan los sistemas informáticos ocasionados por la ciberdelincuencia.

En varios países desarrollados, estos ataques no han podido ser controlados. Sin embargo, estos riesgos se pueden reducir a través de la implementación de políticas de seguridad y controles sistemáticos. Las organizaciones enfrentan diariamente el desafío de proteger sus bases de datos. Entre las estrategias que benefician a las entidades se destaca la realización de copias de seguridad semanalmente, las que deben ser almacenadas en la nube, con la finalidad de mitigar estas acciones

5. REFERENCIAS

Arévalo-Cordovilla, F. (2020). Importancia de la seguridad de los sistemas de información frente el abuso, error y hurto de información. *Revista científica.* https://dominiodelasciencias.com/ojs/index.php/es/article/view/1197/1898

Bao, C. (2020). *Modelo de Gestión de Seguridad Informática para 4PX Iberia.* España: Universidad de Alcalá. http://hdl.handle.net/10017/44659

Bogantes, A. (2020). *El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados. Revista de Sistemas*. https://www.iiisci.org/journal/PDV/risci/pdfs/CB294NT20.pdf

Caamaño Fernández, E. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano organizacional. *Revista de Ciencias Sociales Aplicadas*. file:///D:/pdf%20articulo%20laboratorio%20de%20auditria/571361695004.pdf

Calle-Tenesaca, M. E. (2024). *Ciberseguridaden contabilidad: protegiendo la integridad de los datos financieros en empresas comerciales.* Universidad Católica de Cuenca. https://remca.umet.edu.ec/index.php/REMCA/article/view/734/723

Caminos Manjarrez, W. (2023). Los sistemas contables y su incidencia en la dirección empresarial en el Ecuador. *Revista Latinoamericana de Ciencias Sociales y Humanidades.*Dialnet-LosSistemasContablesYSuIncidenciaEnLaDireccionEmpr-9586232.pdf

Coronel Suárez, I. (2022). Seguridad informática, metodologías, estándares y marco de gestión en un enfoque hacia las aplicaciones web. *Revista Científica y Tecnológica UPSE.* http://scielo.senescyt.gob.ec/pdf/rctu/v9n2/1390-7697-rctu-9-02-00097.pdf

Cristo, L. R. (2021). Los sistemas contables automatizados y su utilización en las entidades. *Scielo Cuba.* http://scielo.sld.cu/scielo.php?pid=S2073-60612021000100008&script=sci_arttext

Dussan, C. (2022). Políticas de seguridad informática. https://www.redalyc.org/articulo.oa?id=265420388008

Díaz, J., & Guerra, E. (2021). Desarrollo de un sistema de gestión para la seguridad de la información basado en metodología de identificación y análisis de riesgo en bibliotecas universitarias. *Scielo Chile.* https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-07642021000500145&lang=es

Encarnación, M. K. (2019). *Análisis de riesgos informáticos en el sistema contable syscofin de la empresa goldenshrimp s.a de la ciudad de machala.* UTMACH. https://repositorio.utmachala.edu.ec/bitstream/48000/13671/1/ECUACE-2019-CA-DE01053.pdf

Escobar, D. S. (2021). *Seguridad informática en los sistemas contables.* Universidad de Buenos Aires. http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0817_EscobarDS.pdf

Gallardo, A. T. (2019). Elementos de un sistema de información contable efectivo. *Revista Quipukamayoc.* https://core.ac.uk/download/pdf/304895619.pdf

Guachún-Orellana P. (2024). Medidas de ciberseguridad aplicadas a los softwares contablesen las PYMES de Cuenca, Ecuador. *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología.* https://cienciamatriarevista.org.ve/index.php/cm/article/view/1324/2214

Guaña-Moya, J. (2023). *La importancia de la seguridad informática en la educación digital: retos y soluciones.* Saberes del Conocimiento. Dialnet-LaImportanciaDeLaSeguridadInformaticaEnLaEducacion-8977055.pdf

Mackay-Castro, C. (2023). Desafíos tecnológicos para el contador en los procesos contables. ¿Ventaja para evitar riesgos de fraude? *Revista Científica Arbitrada de Investigación en Comunicación, Marketing y Empresa.* https://reicomunicar.org/index.php/reicomunicar/article/view/109/192

Manosalve, J. (2024). Estudio y gestión de vulnerabilidades informáticas para una empresa privada en el departamento de Boyacá (Colombia). *Scielo Colombia.* http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-11292014000200007&lang=es

Martínez, A. (2020). *Auditoría con Informática a Sistemas Contables.* https://www.redalyc.org/articulo.oa?id=193924743004

Moreno, J., y Coronado, P. (2021). Modelo base de conocimiento para auditorías de seguridad en servicios web con inyección SQL. *Scielo Colombia.* http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0121-750X2020000300264&lang=es

Muñoz Hernández, H., Zapata Cantero, L. y Requena Vidal, D. (2019). *Riesgos informáticos y alternativas para la seguridad informática en sistemas contables en Colombia.* Revista Venezolana de Gerencia. https://www.redalyc.org/journal/290/29063446029/29063446029.pdf

Navas, N. A. (2021). *Modelo de seguridad informática para riesgos de robo de información por el uso de las redes sociales.* Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/20949/1/UPS-GT003391.pdf

Ojeda-Contreras, F. (2020). Gestión del riesgo y la ciberseguridad en el sector financiero popular y solidario del Ecuador. *Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología.*

Quezada Riofrío, G. (2020). *Análisis histórico de la contabilidad en el Ecuador.* Universidad Nacional de Loja. https://dspace.unl.edu.ec/jspui/bitstream/123456789/23174/1/Gladys%20Adriana%20Quezada%20Riofr%c3%ado.pdf

Ramos, R., Llanqui, R., & Cahuaya, R. (2023). *Política informática y la gestión de la seguridad de la información en base a la norma ISO 27001.* https://www.redalyc.org/journal/6738/673874721007/html/

Ríos, L. (2024). *Seguridad de datos en la contabilidad.* https://gesdatta.com/seguridad-de-datos-en-la-contabilidad/#:~:text=La%20seguridad%20de%20datos%20en,uso%20de%20la%20documentaci%C3%B3n%20contable.

Rocha, C. (2020). https://www.redalyc.org/articulo.oa?id=582663867004

Sánchez-Párraga, Á. (2023). Implementación de la gestión contable en el crecimiento empresarial. *Revista Científica Multidisciplinaria Arbitrada YACHASUN*. https://editorialibkn.com/index.php/Yachasun/article/view/330/556

Sisti, M. A. (2019). Seguridad informática: la protección de la información en una empresa vitivinícola de Mendoza, Universidad Nacional De Cuyo. https://siip2019-2021.bdigital.uncu.edu.ar/objetos_digitales/15749/sistimariaagustina.pdf

Soto, J. (2021). Propuesta de sistema de costos e incidencia en la utilidad de la lavandería Industrial Wash S.A.C. *Scielo Perú*. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S1609-81962021000300085&lang=es

Suárez, J. L. (2020). *Importancia de la seguridad informática y ciberseguridad en el mundo actual*. Universidad Piloto de Colombia. https://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/8668/IMPORTANCIA%20DE%20LA%20SEGURIDAD%20INFORM%c3%81TICA%20Y%20CIBERSEGURIDAD%20EN%20EL%20MUNDO%20ACTUAL.pdf?sequence=1&isAllowed=y