Revista de Investigación Multidisciplinaria

CTSCAFE PARA CIUDADANOS.....

http://www.ctscafe.pe

ISSN 2521-8093

Volumen VII- Nº 20 Julio 2023

http://www.ctscafe.pe

Lima - Perú

REVISTA DE INVESTIGACIÓN MULTIDISCIPLINARIA

CTS CAFE Para ciudadanos…

http://www.ctscafe.pe

Volumen VII- N° 20 Julio 2023

ISSN 2521-8093

Metodologías de gestión de riesgos de TI en empresas u organizaciones

Sr. Marvin Alberto Chavez Ferrel
Universidad Nacional de Trujillo
Correo electrónico: t513300420@unitru.edu.pe

Sr. Raphael Andre Prieto Pastor
Universidad Nacional de Trujillo
Correo electrónico: t0233300720@unitru.edu.pe

Recibido:29 mayo 2023
Aceptado: 20 Julio 2023

Resumen: La gestión de riesgos comprende una serie de procesos esenciales para identificar, evaluar y mitigar los riesgos relacionados a los operaciones y actividades de las empresas. Su objetivo principal es reducir los posibles efectos de los riesgos en la organización, proteger sus activos y recursos y maximizar las oportunidades de negocio. El objetivo de esta investigación fue examinar una variedad de metodologías utilizadas por diversas organizaciones en distintos sectores, tanto públicas como privadas, pequeñas y medianas empresas, durante el periodo comprendido entre 2013 y 2023. Para ello se usó la metodología Prisma para la revisión sistemática, además se emplearon 5 bases de datos que contenían artículos de prestigio tanto a nivel nacional como del extranjero. En la investigación pudimos encontrar el uso de metodologías como ISO 31000, ISO/IEC 27000, NIST, OCTAVE, MAGERIt, ECU@Risk, NTC/ISO 9001:2015 y COBIT; así como su aplicación en diversos sectores empresariales como educación, agropecuario, telecomunicaciones, financiero, transporte, publicidad, salud, agroindustrial, TIC y saneamiento. Estas permitieron identificar, clasificar y establecer estrategias, planes de solución o prevención de riesgos de TI para minimizar sus efectos y de este modo poder garantizar la realización de los objetivos planteados de acuerdo a la empresa donde fueron aplicadas.

Palabras claves: Gestión de riesgos/ Tecnologías de la información/ Mitigación de riesgos.

Abstract: Risk management comprises a series of essential processes to identify, evaluate and mitigate the risks related to the operations and activities of companies. Its main objective is to reduce the possible effects of risks on the organization, protect its assets and resources and maximize business opportunities. The objective of this research was to examine a variety of methodologies used by various organizations in different sectors, both public and private, small and medium-sized companies, during the period between 2013 and 2023. For this, the Prisma methodology was used for the systematic review, In addition, 5 databases containing prestigious articles both nationally and abroad were used. In the research we were able to find the use of methodologies such as ISO 31000, ISO/IEC 27000, NIST, OCTAVE, MAGERIT, ECU@Risk, NTC/ISO 9001:2015 and COBIT; as well as its application in various business sectors such as Education, Agriculture, Telecommunications, Finance, Transportation, Advertising, Health, Agroindustrial, ICT and Sanitation. These made it possible to identify, classify and establish strategies,

solution plans or prevention of IT risks to minimize their effects and thus be able to guarantee the achievement of the objectives set according to the company where they were applied.

Keywords: Risk management/ Information technology/ Risk mitigation.

Résumé : La gestion des risques comprend une série de processus essentiels pour identifier, évaluer et atténuer les risques liés aux opérations et aux activités des entreprises. Son principal objectif est de réduire les effets possibles des risques sur l'organisation, de protéger ses actifs et ses ressources et de maximiser les opportunités commerciales. L'objectif de cette recherche était d'examiner une variété de méthodologies utilisées par diverses organisations de différents secteurs, tant publics que privés, petites et moyennes entreprises, au cours de la période comprise entre 2013 et 2023. Pour cela, la méthodologie Prisma a été utilisée pour la revue systématique, en plus de 5 bases de données contenant des articles prestigieux tant au niveau national qu'à l'étranger. Dans la recherche, nous avons pu trouver l'utilisation de méthodologies telles que ISO 31000, ISO/IEC 27000, NIST, OCTAVE, MAGERIt, ECU@Risk, NTC/ISO 9001:2015 et COBIT ; ainsi que son application dans divers secteurs d'activité tels que l'éducation, l'agriculture, les télécommunications, la finance, les transports, la publicité, la santé, l'agro-industrie, les TIC et l'assainissement. Celles-ci ont permis d'identifier, de classer et d'établir des stratégies, des plans de solutions ou de prévention des risques informatiques pour minimiser leurs effets et ainsi pouvoir garantir l'atteinte des objectifs fixés selon l'entreprise où ils s'appliquaient.

Mots-clés: Gestion des risques/ Technologies de l'information/ Atténuation des risques.

1. Introducción

Actualmente, las tecnologías de la información (TI) son la base fundamental en la optimización de los procesos de una organización. Las TI engloban recursos tecnológicos para el eficiente funcionamiento de los sistemas de información que posee una empresa u organización. Esta infraestructura abarca hardware, software y otros elementos, lo que permite ofrecer servicios a los clientes y gestionar los procesos internos de manera eficiente (Pérez, D.,2005).

Las organizaciones emplean la tecnología de la información (TI) con el propósito de optimizar la eficacia de sus operaciones, incrementar la productividad de los trabajadores, mejorar la satisfacción del cliente y utilizarla como fundamento para la toma de decisiones. No obstante, la integración de la TI también ha generado nuevos riesgos, lo cual implica que las entidades deben garantizar la salvaguardia de sus sistemas ante posibles ataques cibernéticos y violaciones de seguridad y datos. Esta protección se logra mediante la identificación y gestión de riesgos de manera adecuada.

Se puede describir un riesgo como la posible ocurrencia de una amenaza se haga realidad debido a una vulnerabilidad, lo cual pone en peligro los activos fundamentales de una organización. Si este evento llega a suceder, tendrá un impacto negativo en el logro de un objetivo específico, y potencialmente impactar en el valor de la organización (Arteaga, M., 2017).

En este contexto, el tratamiento de los riesgos de TI es un aspecto crucial para las entidades que buscan salvaguardar sus activos y preservar la confianza de sus clientes y socios comerciales. Este procedimiento abarca el hallazgo, análisis, evaluación y clasificación de los riesgos, para poder implementar estrategias para mitigarlos y reducir su impacto (Valverde, D.,2022).

Existen diversas metodologías de gestión de riesgos, que se han desarrollado para adaptarse a las necesidades específicas de diferentes tipos de empresas y sectores. Esta puede ser definida como un conjunto de métodos para optimizar el tratamiento de riesgos de TI, principalmente en los procesos que manejan mucha información importante, en base a los objetivos organizacionales (Molina, M.,2015),

Entre estas se encuentran MAGERIT, desarrollada por el Gobierno español para la gestión de riesgos en las TI; OCTAVE, creada para evaluar amenazas, activos y vulnerabilidades críticas operativas, centrándose en la confidencialidad e integridad; CORAS, proyecto europeo de investigación tecnológica que propone siete pasos para gestionar los riesgos de seguridad; AS/NZS 4360, desarrollada por los estándares australianos y neozelandeses, que consta de cinco fases: limitar el contexto, enumerar, analizar, clasificar y tratar los riesgos; e ISO 31000, una norma internacional que establece los principios generales para el tratamiento de riesgos (Acevedo, N. et al., 2016).

Dado el amplio abanico de metodologías de gestión de riesgos disponibles, es posible adaptar distintas opciones a los diversos sectores empresariales, lo que resultaría en una serie de beneficios para las empresas que las implementen.

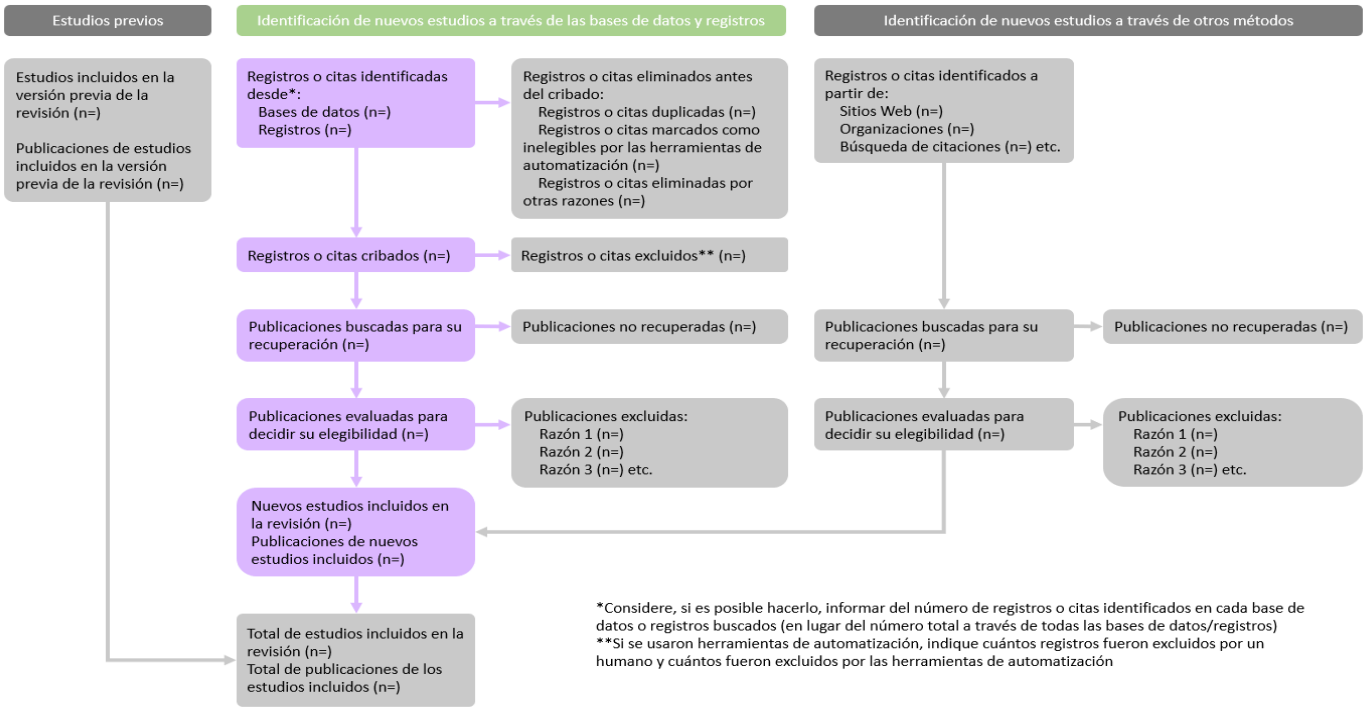
2. Material y métodos

Se llevó a cabo una investigación documental utilizando el enfoque del procedimiento PRISMA como guía. Se planteó una serie de preguntas clave para orientar la implementación de la metodología, tales como: ¿Cuáles son las metodologías utilizadas para la gestión de riesgos en distintos sectores empresariales? ¿Cuál es el impacto y los beneficios que experimentan las empresas al aplicar estas metodologías de gestión de riesgos de TI?

2.1. Fundamentación de la metodología

Según Yepes et al. (2021), se reconoce que la metodología PRISMA posee la capacidad de brindar beneficios a múltiples grupos de interés. La publicación completa de revisiones bibliográficas permite a los lectores evaluar la calidad de los procedimientos utilizados y la confiabilidad de los resultados obtenidos. La identificación y síntesis de características clave en las investigaciones ayuda a simplificar el proceso y proporcionar recomendaciones pertinentes para la práctica o las políticas. Además, la presentación exhaustiva de todas las secciones del formato PRISMA 2020 (Figura 1) facilita la discusión y la adaptación de las revisiones bibliográficas, así como su inclusión en revistas generales o especializadas en investigación metodológica y en compendios de buenas prácticas, lo cual permite que los investigadores puedan aprovechar el trabajo realizado y evitar esfuerzos innecesarios en sus propias investigaciones.

Figura N°1: Diagrama de flujo PRISMA 2020



6

2.2. Criterios de inclusión y de exclusión

Se utilizó como criterio de inclusión a los escritos divulgados entre los años 2013 y 2023 (Tabla 1). Además, se consideró los encabezados que tengan la especificación de "Metodología de gestión de riesgos", "Aplicación de una metodología de gestión de riesgo en una empresa o rubros de empresas", "Metodología de gestión de riesgos de tecnologías de la información", "Application risk management methodology in company". Asimismo, los escritos deberán estar tanto en español como en inglés para una mayor profundización de nuestra revisión bibliográfica.

No obstante, se descartaron las presentaciones en formato de diapositivas y ejemplares debido a que no proporcionan la misma fiabilidad que la información obtenida a través de fuentes de mayor calidad. También se eliminaron las lecturas grises, que son documentos no publicados, y aquellos escritos que se encontraron en varios archivos digitales para evitar la duplicación de información.

Finalmente, se consideró los criterios de exclusión como cuando a aplicación no ha sido hacia una empresa o rubro empresarial, o cuando la empresa no maneja tecnologías de la información-

Tabla N°1: Criterios de inclusión y exclusión

CRITERIOS DE INCLUSIÓN	Artículos o tesis que hayan sido publicados en los últimos 10 años (2013 - 2023)
	Idioma en español o inglés
	Tiene que haberse aplicado una metodología de gestión de riesgos
CRITERIOS DE EXCLUSIÓN	La aplicación no ha sido hacia una empresa o rubro empresarial
	La empresa no maneja tecnologías de la información

Fuente: Elaboracion propia

2.3.Proceso de recolección de la información

El proceso de búsqueda y recolección de datos se llevó a cabo utilizando una combinación de palabras clave relacionadas con la metodología de gestión de riesgos y su aplicación en empresas o rubros específicos. Las palabras clave incluyeron "metodología de gestión de riesgos", "aplicación de una metodología de gestión de riesgo en una empresa o rubros de empresas", "metodología de gestión de riesgos de tecnologías de la información" y "application risk management methodology in company". Se utilizó un enfoque transparente para buscar lecturas científicas, y se emplearon diferentes fuentes de datos como SciELO, Google Académico, Scopus, Dialnet y CORE.

En el caso del buscador académico SciELO se utilizó el siguiente motor de búsqueda: Metodología de gestión de riesgos. Los resultados fueron un total de 128 revistas encontradas, de las cuales aplicando los criterios de inclusión y exclusión se seleccionaron 2.

Luego para Google cadémico, se buscó con el siguiente motor de búsqueda: “Aplicación de una metodología de gestión de riesgo en una empresa o rubros de empresas”; donde los resultados fueron un total de 90,200 escritos generalizados, ya que es una cantidad muy elevada se le aplicó el filtrado por “artículos”, resultando un total final de 544 artículos académicos de los cuales fueron seleccionados 7.

Para el caso de Scopus se hizo la búsqueda en base a “TITLE-ABS-KEY (application AND of AND risk AND management AND methodology AND in AND a AND company)” la cual arrojo un resultado de 743, pero incluimos un filtrado para los artículos que tienen libre acceso de los cuales quedaron 134 y fueron seleccionados 2 en base a los criterios de exclusión/inclusión.

Para Dialnet se realizó la búsqueda a partir de "Metodología de gestión de riesgos de tecnologías de la información" donde se encontraron 194 documentos, luego se realizó un filtrado por "artículos de revista" y "tesis", obteniéndose 180 documentos, donde luego de aplicar los criterios de inclusión y exclusión se seleccionaron 5.

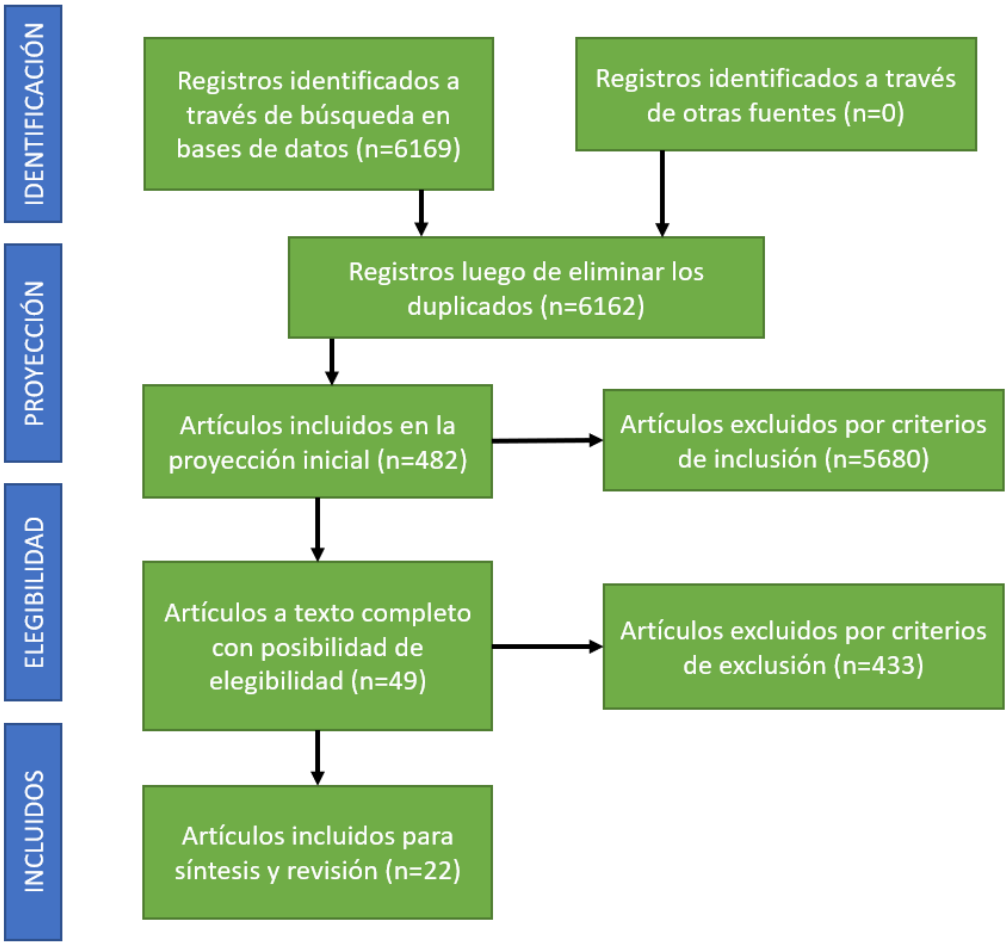
Finalmente, con respecto a CORE se realizó la búsqueda a partir de "Metodología de gestión de riesgos de TI en las organizaciones" donde se encontraron 36519 documentos, estos fueron filtrados por "tesis", donde se obtuvo 4560 documentos, donde luego de aplicar los criterios de inclusión y exclusión se seleccionaron 6.

Tabla N°2: Bases de datos y artículos seleccionados

Bases de datos	Motor de Búsqueda	Resultados	Seleccionados
SciELO	Metodología de gestión de riesgos	128	2
Google Académico	Aplicación de una metodología de gestión de riesgo en una empresa o rubros de empresas	544	7
Scopus	TITLE-ABS-KEY (application AND of AND risk AND management AND methodology AND in AND a AND company) AND (LIMIT-TO (OA, "all"))	132	2
Dialnet	Metodología de gestión de riesgos de tecnologías de la información	180	5
CORE	Metodología de gestión de riesgos de TI en las organizaciones	4560	6

Fuente: Elaboracion propia

Figura 2: Proceso de selección de artículos / Flujograma PRISMA



Fuente: Elaboracion propia

3. Resultados

Teniendo ya los artículos seleccionados se procedió a su debida revisión y se obtuvieron resultados de cada uno de ellos y estos fueron plasmados en la siguiente tabla, donde se muestra el(los) autor(es), rubro de la empresa, país y resultados.

Tabla N°3: Resultados de artículos seleccionados

º	Autor(es)	Rubro de empresa	País	Resultados
1	Pérez Suárez et al. (2020)	Educación	Cuba	La investigación sugiere que es viable combinar la metodología basada en ISO 31000, el enfoque de trabajo en equipo y el análisis modal de fallas y efectos para abordar los riesgos relacionados con los procesos de autoevaluación de las maestrías en el contexto cubano. Además, se propone actualizar el estándar de calidad existente para la evaluación externa y la acreditación en la educación superior.
2	Cruz & Morejón (2019)	Agropecuario	Cuba	Se implementó una metodología basada en la norma ISO 31000/2018, donde se pudo notar la necesidad de establecer y poner en marcha un sistema de medición y monitoreo de las actividades propensas a riesgos en cada uno de los procesos identificados, clasificándolos de acuerdo con su nivel de gravedad o consecuencias. Asimismo, plantea formar un sistema de comunicación de riesgos para tener mejor conocimiento, monitoreo, control y tratamiento de los riesgos como fundamento de un eficaz proceso de gestión integral de riesgos.
3	López (2021)	Telecomunicaciones	Perú	La aplicación de la metodología NIST SP 800-30 tuvo un impacto positivo en la seguridad de las redes inalámbricas, se logró una mejora en la seguridad de la información de los clientes al utilizar equipos más actuales, se pudo mejorar notablemente la seguridad de la información y las redes de la empresa.
4	Muñoz (2022)	Servicio Tecnológico (TIC)	Ecuador	Se realizó la adaptación de la metodología Octave para su implementación en una infraestructura en la nube utilizando el ciclo PHVA para una infraestructura en la nube de tipo IAAS, con el objetivo de lograr un enfoque de gestión de riesgos y seguridad de la información efectivo.
5	Pacheco Fernández et al. (2021)	Financiero	Colombia	La realización de un análisis multidimensional permite identificar de manera más sencilla las áreas que requieren mayores esfuerzos en términos de tiempo, costos y asignación de personal. La metodología OCTAVE permite una identificación clara y detallada de los riesgos en los que se deben asignar recursos para su solución o reducción de la probabilidad de ocurrencia o impacto.
6	Fuentes Yancha (2019)	Transporte	Ecuador	Se aplicó la metodología MAGERIT para la definición de los pasos necesarios para realizar la identificación y evaluación de activos, amenazas, riesgos y medidas de protección en la gestión de riesgos tecnológicos. Al

				examinar los activos tecnológicos en cada uno de estos pasos, se pueden determinar los factores y criterios pertinentes para identificar y evaluar los riesgos y medidas de protección en el proceso de gestión de riesgos.
7	RAMIREZ PORTOCARRERO (2021)	Educación	Perú	Se realizó un análisis de riesgos utilizando la metodología MAGERIT y PILAR Basic con el fin de identificar los riesgos relacionados con los activos de Tecnologías de la Información TI. La implementación de esta metodología y herramienta respaldó la suposición de que su adopción como estrategia de control en la seguridad de las TI conlleva una mejora significativa en la gestión del riesgo.
8	Valverde Flores (2022)	Publicidad	Perú	Inicialmente, la agencia publicitaria no contaba con un registro de sus activos. Sin embargo, al aplicar la metodología MAGERIT, se logró identificar y evaluar los riesgos a los que activos de la organización estaban expuestos y valorarlos de manera apropiada. Además, se implementaron planes de acción y controles frente a estos.
9	Ávila Ávila (2018)	Salud	Ecuador	La metodología ECU@Risk pudo establecer los principios y pasos necesarios para establecer la gestión de riesgos dentro de una organización. Con la utilización de esta metodología, se realizó un exhaustivo registro de los activos de información, y se identificaron las potenciales amenazas, lo cual posibilitó la determinación de estrategias de mitigación y la identificación de controles factibles para su implementación.
10	Guagalango et al. (2017)	Agroindustrial	Ecuador	En este informe se describe la implementación de la metodología MAGERIT para realizar un análisis de riesgos en el Departamento de Tecnología e Información de una empresa específica. Los resultados obtenidos del análisis de riesgos proporcionaron información valiosa a los inversores y ejecutivos para tomar decisiones informadas sobre las inversiones necesarias para mejorar la seguridad de la información de la empresa y obtener el máximo retorno de inversión en seguridad.
11	Bravo Ramos & Guun Yoo (2020)	Educación	Ecuador	Describe una nueva metodología de análisis de riesgos para bibliotecas basada en pasos filtrados de metodologías existentes que son compatibles con el estándar ISO/IEC 27000: 2013. La implementación del ISMS en el sistema bibliotecario de la EPN le dotó de mecanismos de optimización de recursos y de un proceso de mejora continua que facilita el logro de los objetivos de la universidad.
12	Castillo et al. (2018)	Educación	Ecuador	Se implementó de un sistema para el tratamiento de riesgos de seguridad informática, basado en las metodologías MAGERIT y OCTAVE, condujo a una disminución del 80,59% en las vulnerabilidades de alto nivel identificadas

				durante el análisis, y se logró eliminar el 19,41% de dichas vulnerabilidades. Se plantea y se lleva a cabo la implementación de un modelo destinado a reducir los riesgos de seguridad informática, centrándose en la evaluación del impacto generado por las vulnerabilidades. Se priorizan las acciones a tomar para mitigar los riesgos más significativos.
13	Enríquez & Hidalgo (2015).	TIC	Ecuador	Basándose en la norma ISO/IEC 27005, se concluyó que tanto el valor del impacto como el riesgo asociado deben considerarse en el proceso de Tratamiento de Riesgos, dándole prioridad a la implementación de controles en las amenazas que puedan generar impactos y riesgos elevados. Estos controles pueden prevenir o disminuir notablemente los riesgos de seguridad. Para evaluar la efectividad de dichos controles, resulta necesario realizar un análisis de retroalimentación utilizando la metodología propuesta.
14	Holguín & Lema (2015).	Transporte marítimo	Ecuador	Como resultado de la integración de las metodologías MAGERIT, OCTAVE y MEHARI, se propone un modelo basado en la creación de un Mapa de Control. Este modelo tiene como objetivo evaluar a la organización en relación al grado de análisis de riesgo actuales. En base a este, se focalizarán en las vulnerabilidades identificadas en cada aspecto, se trazarán actividades de mejora y se llevará a cabo una autoevaluación de su cumplimiento. El propósito final es lograr mejoras sustanciales en el futuro.
15	Palacios et al. (2019)	Educación	Ecuador	Al utilizar la metodología COBIT 5.0, se observó que el proceso de Soporte Técnico Distrital presenta un nivel de riesgo moderado, con una ponderación del 61.75% en la gestión de riesgos informáticos. De igual manera, el proceso de Creación de Cuentas de Usuarios y Perfiles para sistemas de información se encuentra en un nivel de riesgo moderado, con una ponderación del 50.75%. Adicionalmente, se identificó que el proceso de Instalación de Enlaces de Internet y Telefonía presenta un riesgo alto, debido a que la infraestructura tecnológica no cumple con las normas y estándares establecidos para el cableado estructurado y los conductores de energía eléctrica.
16	López et al. (2014)	Entidades financieras	Argentina	Se llevó a cabo la creación de una estructura RBS que sirve como base para la elaboración de planes eficientes con el fin de mitigar los impactos de sucesos negativos. Esta propuesta proporcionará a los directivos un cimiento para el análisis de riesgos, la implementación de estrategias que reduzcan el impacto de los riesgos, enfocándose en el los objetivos de la organización.
17	Herrera & Quiroga (2019)	TIC (Desarrollo de sistemas informáticos)	Colombia	La propuesta basada en la norma NTC/ISO 9001, permitió proporcionar las herramientas necesarias para abordar diversos desafíos, tales como: - La definición de los riesgos relacionados a las distintas actividades organizacionales. - El establecimiento de canales de comunicación interna y externa para el hallazgo y control de los riesgos. - La descripción de los riesgos en las diversas tareas que comprenden los procesos, así como la implementación de criterios y métodos para su seguimiento y medición.

18	Joya & Sácristan (2017)	Salud	Colombia	Después de aplicar la metodología MAGERIT, se pudo elaborar una lista de los riesgos relacionados a los activos lógicos de la organización, así como evaluar el impacto que podrían tener en caso de ocurrir. También se plantearon marcos a implementar para reducir el riesgo de vulneraciones a la información.
19	Guamán (2019)	Educación	Ecuador	Se utilizó la metodología MAGERIT para un análisis exhaustivo de los riesgos, abarcando aspectos como disponibilidad, confidencialidad, integridad y autenticidad. La evaluación del sistema docente muestra un grado elevado de acatamiento de las estrategias de seguridad de la información, alcanzando un 53%. No obstante, se requiere un compromiso por parte de las partes interesadas para elevar este porcentaje.
20	Moscoso et al. (2018)	Sector de Saneamiento	Perú	La implementación del modelo propuesto, que se basa en las metodologías MAGERIT, OCTAVE, NIST y COBIT 5, llevó a la identificación de un total de 165 riesgos, de los cuales se determinó que 52 tenían una alta prioridad. Además, se elaboraron 16 proyectos específicos para gestionar los riesgos de alta prioridad. Estos apoyan en la toma de decisiones y evitan los gastos relacionados con la solución de los efectos de un riesgo. Asimismo, se identificaron los recursos necesarios y se definieron las actividades de mejora continua para abordar estos riesgos.
21	Castillo (2022)	TIC (Consultoría de sistemas)	Perú	La metodología MAGERIT se empleó para establecer políticas y actividades de evaluación de riesgos, con el propósito de implementar un sistema para resguardar la información. Para evaluar la eficacia del sistema INFORISK, se llevaron a cabo encuestas a los usuarios, obteniendo valoraciones satisfactorias que respaldan su validez.
22	Vásquez. & Alva (2018)	Entidades Financieras	Perú	En el método propuesto, se ha empleado como base las normas ISO/IEC 31000:2009, ISO/IEC 27005:2008, ISO/IEC 22301:2012, así como las metodologías OCTAVE, MAGERIT y COBIT 5. Se ha incluido una etapa de análisis de impacto empresarial para identificar los procesos críticos y, a partir de ellos, obtener los riesgos de TI. Esto ha permitido desarrollar una plantilla estandarizada de planes de acción que abarca todos los parámetros necesarios para la gestión de riesgos de TI en el contexto de las microfinanzas.

Fuente: Elaboracion propia

Figura N°3: Mapa coroplético de los artículos seleccionados

Fuente: Elaboracion propia

De los países que se han tomado en cuenta para obtener los artículos, se centraron en países latinoamericanos principalmente, se han identificado en mayor cantidad a menor cantidad en el siguiente orden: 10 artículos en Ecuador, 6 artículos en Perú, 3 artículos en Colombia, 2 artículos en Cuba y 1 artículo en Argentina.

Tabla N°4: Artículos clasificados y contabilizados en base a su metodología y sus rubros empresariales

Metodología / Rubro empresarial	ISO 31000	ISO/IEC 27000	NIST SP 800-30	OCTAVE	MAGERIT	ECU@Risk	Cobit 5.0	NTC/ISO 9001:2015	Total
Educación	1	1	-	1	3	-	1	-	**7**
Agropecuario	1	-	-	-	-	-	-	-	**1**
Telecomunicaciones	-	-	1	-	-	-	-	-	**1**
Financiero	1	1	-	2	1	-	1	-	**6**
Transporte	-	-	-	1	2	-	-	-	**3**
Publicidad	-	-	-	-	1	-	-	-	**1**
Salud	-	-	-	-	1	1	-	-	**2**
Agroindustrial	-	-	-	-	1	-	-	-	**1**
TIC	-	1	-	1	1	-	-	1	**4**
Saneamiento	-	-	1	1	1	-	1	-	**4**
Total	**3**	**3**	**2**	**6**	**11**	**1**	**3**	**1**	

Fuente: Elaboracion propia

4. Discusión

En base a lo presentado, se pudo notar que debido a la adaptabilidad y complementariedad se encontraron investigaciones que referencian el uso simultáneo de metodologías, principalmente entre MAGERIT y OCTAVE, las cuales aparece conjuntamente en 4 publicaciones. Asimismo, se notaron casos en los que algunos artículos usaron más de 2 metodologías en conjunto como fue el caso de Holguín & Lema (2015), utilizando las metodologías MAGERIT, OCTAVE y MEHARI, en el artículo publicado por Moscoso et al. (2018) se tomaron en cuenta las metodologías MAGERIT, OCTAVE, NIST y COBIT 5 y en el caso de Vásquez. & Alva (2018) teniendo como base a las normas ISO/IEC 31000:2009, ISO/IEC 27005:2008, ISO/IEC 22301:2012 y a las metodologías OCTAVE, MAGERIT y COBIT 5.

Después de ordenar los resultados de cada uno de los artículos se procedió a clasificarlos y contabilizarlos en base a su metodología como a sus rubros. Y se obtuvo que, la metodología más usada en los diferentes rubros fue MAGERIT seguida de OCTAVE, los rubros empresariales en los cuales se han aplicado más metodologías han sido educación y financiero. Por otro lado, entre las metodologías menos usadas se encuentran ECU@Risk y NTC/ISO 9001:2015, y los rubros empresariales donde no se tiene

numerosos usos de metodologías de gestión de riesgo son agropecuario, telecomunicaciones, publicidad y agroindustrial.

5. Conclusiones

En los últimos años, se ha notado como las tecnologías de la información crecen a gran escala, esto ocasiona que las organizaciones tengan la necesidad de hacer frente a los riesgos que puedan aparecer con respecto a los servicios de TI.

La presente investigación identificó las metodologías utilizadas para la gestión de riesgos de TI en diferentes organizaciones a partir de la revisión de artículos científicos y tesis publicadas a partir de 2013 tomando como referencia las bases de datos SCOPUS, SCIELO, GOOGLE ACADEMICO, DIALNET Y CORE; donde se pudo determinar que MAGERIT es la metodología más utilizada, teniendo presencia en 11 publicaciones, principalmente en el sector de educación, seguido de OCTAVE, que tuvo presencia en 6 artículos, siendo el sector financiero el que presenta la mayor cantidad de aplicación de dicha metodología. Asimismo, las metodologías de gestión de riesgos de TI permitieron a las organizaciones identificar los riesgos, establecer niveles de prioridad y planes de acción para su tratamiento, así como la optimización de recursos y de un proceso de mejora continua que permita cumplir los objetivos organizacionales.

En cuanto a las limitaciones, podemos decir que los resultados obtenidos corresponden a cinco bases de datos, cantidad que puede ser ampliado en una investigación más profunda que complemente la realizada en esta revisión. A futuro, se espera el incremento de la utilización y evolución de los aspectos que abarca cada metodología en función a la gestión de riesgos de TI con el fin de permitir el crecimiento y desarrollo de las organizaciones, haciendo posibles investigaciones futuras sobre cuáles serían las más óptimas metodologías orientadas a rubros empresariales específicos.

6. Literatura citada

Acevedo, N. & Satizábal, C. (2016). Risk management and prevention methodologies: a comparison https://www.redalyc.org/articulo.oa?id=411545767003

Andocilla, I. & Fuentes, M. (2019) Propuesta de un plan de gestión de riesgo tecnológicos para la empresa pública metropolitana de transporte de pasajeros de Quito. http://repositorio.uisrael.edu.ec/handle/47000/2182

Arteaga Martínez, M.M. (2017). Gestión de riesgos de TI. https://repository.ucc.edu.co/server/api/core/bitstreams/33666758-6d02-46e7-8f62-f78e13067663/content

Ávila, N. (2018). Aplicación de la metodología ECU@Risk para la gestión de riesgos de la información en el sector hospitalario. https://dspace.uazuay.edu.ec/bitstream/datos/7978/2/13715.pdf

Bravo, M. & Yoo, S. (2020). Developing an Information Security Management System for Libraries Based on an Improved Risk Analysis Methodology Compatible with ISO/IEC 27001. https://www.scopus.com/record/display.uri?eid=2-s2.0-85075816739&origin=resultslist&sort=plf-f&src=s&st1=Developing+an+Information+Security+Management+System+for+Libraries+Based+on+an+Improved+Risk+Analysis+Methodology+Compatible+with+ISO%2fIEC+27001&sid=5bdc27caf8282689ced5ffd9ee0fec75&sot=b&sdt=b&sl=158&s=TITLE-ABS-KEY%28Developing+an+Information+Security+Management+System+for+Libraries+Based+on+an+Improved+Risk+Analysis+Methodology+Compatible+with+ISO%2fIEC+27001%29&relpos=0&citeCnt=0&searchTerm=

Castillo Fiallos, J. N., Cisneros Barahona, A. S., Méndez Naranjo, P. M., & Jácome Segovia, D. F. (2019). Modelo para la reducción de riesgos de seguridad informática en servicios web. Cumbres, 4(2), 19–30. https://doi.org/10.48190/cumbres.v4n2a2

Castillo, R. (2022). Desarrollo de una aplicación web y móvil para la gestión de riesgos de seguridad de la información aplicado a una empresa de consultoría de sistemas. https://core.ac.uk/reader/534030682

Cruz, M. & Morejón, M. (2019). Metodología para la gestión integral de riesgos y seguros con enfoque de gestión social cooperativa. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2310-340X2019000100074

Enríquez, V., & Hidalgo, P. (2015). Metodología de Valuación de Riesgos Como Parte del Sistema de Gestión de Seguridad de la Información (SGSI) Aplicado a un Data Center de Alta Gama. Revista Politécnica, 36(1), 45. Recuperado a partir de https://revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/view/494

Guamán, V. (2019). Evaluación de seguridad de la información aplicado al sistema de evaluación de docentes de la Universidad Técnica del Norte basado en la ISO 27002:2017 con la metodología MAGERIT V3. https://core.ac.uk/reader/270101232

Herrera, C. & Quiroga, D. (2019). Planificación del sistema de gestión de calidad bajo norma NTC/ISO 9001: 2015 en la Empresa Cívico Digital S.A.S. https://core.ac.uk/reader/223029733

Holguin, F. & Lema, L. (2019). Modelo para medir la madurez del análisis de riesgo de los activos de información en el contexto de las Empresas Navieras. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 31, 1–17. https://doi.org/10.17013/risti.31.1-17

Joya, J. & Sacristán, C. (2017). Desarrollo de una propuesta de mitigación de riesgos y vulnerabilidades en activos lógicos para la Empresa Javesalud I.P.S. https://core.ac.uk/reader/151749220

Lopez, J. (2021). Gestión de riesgos con metodología NIST SP 800-30 a la seguridad en redes inalámbricas en la empresa Servintecomp Ucayali-Pucallpa:2018. http://repositorio.unu.edu.pe/handle/UNU/4982

López, M., Albanese, E., & Sánchez, A. (2014). Gestión de riesgos para la adopción de la computación en nube en entidades financieras de la República Argentina. Contaduría y administración, 59(3), 61–88. https://doi.org/10.1016/s0186-1042(14)71266-5

Molina, M. (2015). LITORAL http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014 propuesta de un plan de gestión de riesgos de tecnología aplicado en la escuela superior politécnica del - 2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Moscoso, L., Peña, E. & Soto, M. (2018). Modelo de gestión de riesgos de TI que contribuye a la operación de los procesos de gestión comercial de las empresas del sector de saneamiento del norte del Perú. https://core.ac.uk/reader/225142829

Pacheco, A. et al. (2021). Aplicar la metodología OCTAVE de identificación de amenazas y vulnerabilidades en una entidad bancaria. https://proyectosmaestrias.virtual.uniandes.edu.co/images/mlC4bCJ5XSVNmWQUD6uN4V2gJFMiZDbyVCkn22QE.pdf

Palacios, A., Bosquez, V., Palacios, J. & Camacho, L. (2019). Auditoría de seguridad informática a la dirección distrital 02d03 chimbo-san miguel-educación, aplicando COBIT 5. Revista de Investigación Talentos, 6(2), 1–11. https://dialnet.unirioja.es/servlet/articulo?codigo=8551279

Pérez González, D. (2005). Contribución de las tecnologías de la información a la generación de valor en las organizaciones: Un modelo de análisis y valoración desde la gestión del conocimiento, la productividad y la excelencia en la gestión. https://repositorio.unican.es/xmlui/bitstream/handle/10902/1173/1de8.DPG_capt1.pdf?sequence=2&isAllowed=y

Pérez, Y. S. (2020). Metodología para gestionar riesgos en la autoevaluación de las maestrías del Instituto de Farmacia y Alimentos de la Universidad de La Habana. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0257-43142020000300019

Ramirez, P. (2021). Gestión del riesgo de las tecnologías de la información y la comunicación con la metodología MAGERIT en el Instituto Tecnológico del Oriente de Tingo María http://181.176.159.234/bitstream/handle/20.500.14292/2071/TS_PKRP_2021.pdf?sequence=1&isAllowed=y

Vaca, C. & Muñoz, C. (2022). Propuesta de un esquema de gestión de riesgos tecnológicos para modelos de servicio de tipo Infraestructura como servicio "IAAS" utilizando la metodología OCTAVE dentro del ciclo de mejora continua PHVA. http://repositorio.uisrael.edu.ec/handle/47000/3363

Valverde Flores, D.A. (2022). Implementación de una gestión de riesgos de TI para mejorar la seguridad de la información de una empresa de agencia publicitaria - 2021. https://repositorio.utp.edu.pe/bitstream/handle/20.500.12867/5529/D.Valverde_Tesis_Titulo_Profesional_2022.pdf?sequence=1&isAllowed=y

Vásquez, F. & Alva, J. (2018). Modelo de gestión de riesgos de TI para contribuir en la continuidad del negocio de las microfinancieras de la región Lambayeque. https://core.ac.uk/reader/225142827

Vega, R. et al. (2017). Experience in Applying the Analysis and Risk Management Methodology called MAGERIT to Identify Threats and Vulnerabilities in an Agroindustrial Company https://www.scopus.com/record/display.uri?eid=2-s2.0-85036569219&origin=resultslist&sort=plf-f&src=s&st1=Experience+in+Applying+the+Analysis+and+Risk+Management+Methodology+called+MAGERIT+to+Identify+Threats+and+Vulnerabilities+in+an+Agro-industrial+Company&sid=9f13ae3adfb8e2942ea6f1d4d26d7d7f&sot=b&sdt=b&sl=167&s=TITLE-ABS-KEY%28Experience+in+Applying+the+Analysis+and+Risk+Management+Methodology+called+MAGERIT+to+Identify+Threats+and+Vulnerabilities+in+an+Agro-industrial+Company%29&relpos=0&citeCnt=3&searchTerm=

Villaverde, H. (2022). Implementación de una gestión de riesgos de TI para mejorar la seguridad de la información de una empresa de agencia publicitaria – 2021. https://repositorio.utp.edu.pe/handle/20.500.12867/5529

Yepes-Nuñez, J. J., Urrútia, G., Romero-García, M., & Alonso-Fernández, S. (2021). Declaración PRISMA 2020: una guía actualizada para la publicación de revisiones sistemáticas. Revista Española De Cardiología, 74(9), 790-799. https://doi.org/10.1016/j.recesp.2021.06.016

REVISTA DE INVESTIGACIÓN MULTIDISCIPLINARIA

CTSCAFE Para ciudadanos…

http://www.ctscafe.pe

Volumen VII- N° 20 Julio 2023

Contáctenos en nuestro correo electrónico
revistactscafe@ctscafe.pe

Página Web:
http://ctscafe.pe

Blog:
https://ctscafeparaciudadanos.blogspot.com/

Facebook
https://www.facebook.com/Revista-CTSCafe-1822923591364746/

latindex