View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Repositorio Institucional UPeU (Universidad Peruana Unión)

UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

Métodos difusos y factores para la identificación del nivel de riesgos de TI en entidades gubernamentales: Una revisión sistemática de la literatura

Trabajo de Investigación para obtener el Grado Académico de Bachiller en Ingeniería de Sistemas

Autor:

Norma Lucía Riquelme Challco

Asesor:

Mg. Fernando Manuel Asin Gomez

Lima, diciembre del 2020

DECLARACIÓN JURADA DE AUTORÍA DEL TRABAJO DE INVESTIGACIÓN

Mg. Fernando Manuel Asin Gomez, de la Facultad de Ingeniería y Arquitectura, Escuela Profesional de Ingeniería de Sistemas, de la Universidad Peruana Unión.

DECLARO:
Que el presente informe de investigación titulado: **"Métodos difusos y factores para la identificación del nivel de riesgos de TI en entidades gubernamentales: Una revisión sistemática de la literatura"** constituye la memoria que presenta la estudiante Norma Lucía Riquelme Challco para aspirar al grado de bachiller en Ingeniería de Sistemas, cuyo trabajo de investigación ha sido realizado en la Universidad Peruana Unión bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente constancia en Lima, al 22 de diciembre del año 2020.

Mg. Fernando Manuel Asin Gomez

ACTA DE SUSTENTACIÓN DE TRABAJO DE INVESTIGACIÓN

En Lima, Ñaña, Villa Unión, a……..los.....21.....día(s) del mes de…..diciembre.....del año 2020..siendo las.....11:20 horas, se reunieron los miembros del jurado en la Universidad Peruana Unión campus Lima, bajo la dirección del(dela) presidente(a): ..... Dra. ErikaInés Acuña Salinas....., el (la) secretario(a) Ing. Jenson Daniel Chambi Aguilar..... y los demás miembros:.… Mg. Geraldine Verónica Alvizuri Llerena …..y el (la) asesor(a) Mg. Fernando Manuel Asin Gomez.… con el propósito de administrar el acto académico de sustentación del trabajo de investigación titulado: "Métodos difusos y factores para la identificación del nivel de riesgos de TI en entidades gubernamentales: Una revisión sistemática de la literatura".....de los (las) egresados (as): a)……..... Norma Lucía Riquelme Challco ……

……..……b)……..……..……

…… conducente alaobtención delgradoacadémico deBachiller en……

……..……Ingeniería de Sistemas……..
(Denominación del Grado Académico de Bachiller)

El Presidente inició el acto académico de sustentación invitando …a la… candidato(a)/s hacer uso del tiempo determinado para su exposición. Concluida la exposición, el Presidente invitó a los demás miembros del jurado a efectuar las preguntas, y aclaraciones pertinentes, las cuales fueron absueltas por …la… candidato(a)/s. Luego, se produjo un receso para las deliberaciones y la emisión del dictamen del jurado.

Posteriormente, el jurado procedió a dejar constancia escrita sobre la evaluación en la presente acta, con el dictamen siguiente:

Candidato/a (a): ..... Norma Lucía Riquelme Challco ……..……..……

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	
Aprobado	**19**	**A**	Con nominación de **Excelente**	Excelencia

Candidato/a (b): ……..

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	

(*) Ver parte posterior

Finalmente, el Presidente del jurado invitó …a la… candidato(a)/s a ponerse de pie, para recibir la evaluación final y concluir el acto académico de sustentación procediéndose a registrar las firmas respecti

Presidente Dra. Erika Inés Acuña Salinas		Secretario Ing. Jenson Daniel Chambi Aguilar
Asesor Mg. Fernando Manuel Asin Gomez	Miembro	Miembro Mg. Geraldine Verónica Alvizuri Llerena
Candidato/a (a) Norma Lucía Riquelme Challco		Candidato/a (b)

ÍNDICE

Métodos difusos y factores para la identificación del nivel de riesgos de TI en entidades gubernamentales: Una revisión sistemática de la literatura

Fuzzy methods and factors for identifying the level of IT risk in government entities: A systematic review of the literature

Norma Lucía Riquelme Challco[1]

[1] Universidad Peruana Unión, Lima- Carretera Central Km 19.5 Ñaña, Perú
normariquelme@upeu.edu.pe

Resumen. En la actualidad la tecnología está tomando un rol muy importante en la automatización de procesos en las organizaciones, éstos son abastecidos por activos como: servidores y aplicaciones, donde se involucra todo tipo de información que pueda ser manejada y manipulada. Todo ello trae consigo riesgos de TI a los que se encuentran expuestos por falta de una gestión y análisis organizacional adecuado; los ciberataques cada día evolucionan conjuntamente con los avances tecnológicos, según reportes de dos grandes compañías de seguridad informática como ESET y Kaspersky muestra que la preocupación de las empresas en general se centra en el robo de la información y la infección con códigos maliciosos. Para poder realizar un análisis de riesgos es necesario clasificarlos por niveles a través de factores evaluados de manera cualitativa, así como también hacer uso de una metodología que permita obtener resultados en cuanto a las variables establecidas, para ello es necesario el uso de un modelo difuso adecuado que permita la graduación de los valores introducidos para el análisis. En este estudio se busca identificar métodos de lógica difusa, como también el reconocimiento de factores para la identificación de riesgos de las tecnologías de la información, para su determinación se realizó una revisión sistemática de la literatura utilizando bases de datos reconocidas, de un total de 352 artículos identificados se revisaron 31 artículos donde se puede concluir que existen distintos métodos difusos para la evaluación de riesgos de TI en base a factores como: probabilidad e impacto.

Palabras claves: Métodos difusos, lógica difusa, riesgos de Tecnologías de la Información, tecnologías de la información, seguridad de la información, ciberseguridad, factores de riesgos de TI

Abstract. At present, technology is taking a very important role in the automation of processes in organizations, they are supplied by assets such as: servers and applications, where all kinds of information that can be managed and manipulated is involved. All of this brings with it IT risks to which they are exposed due to the lack of adequate management and organizational analysis; Cyberattacks evolve every day along with technological advances, according to reports from two large computer security companies such as ESET and Kaspersky show that the concern of companies in general is centered on the theft of information and infection with malicious code. In order to perform a risk analysis, it is necessary to classify them by levels through qualitatively evaluated factors, as well as to make use of a methodology that allows obtaining results in terms of the established variables, for this it is necessary to use a fuzzy model suitable that allows the graduation of the values entered for the analysis. This study seeks to identify fuzzy logic methods, as well as the recognition of factors for the identification of risks of information technologies, for its determination a systematic review of the literature was carried out using recognized databases, of a total of 352 articles identified, 31 articles were reviewed where it can be concluded that there are different fuzzy methods for IT risk assessment based on factors such as: probability and impact.

Keywords: Fuzzy methods, fuzzy logic, Information Technology risks, information technology, information security, cybersecurity, IT risk factors

1 Introducción

Las tecnologías de la información (TI) son aquellas que permiten acceder, almacenar, transmitir y manipular todo tipo de información; diferentes organizaciones reconocidas internacionalmente han creado modelos donde definen una serie de pasos que permiten a las empresas implementar sistemas de seguridad de la información basados en el análisis de riesgos para evitar el impacto que podría ocurrir en el cumplimiento de sus objetivos [1]. La evaluación de riesgos se basa en cálculos de valores cualitativos, todo es medido bajo una incertidumbre donde se dan valores aproximados en un rango numérico, aplicable a un modelo de lógica difusa [2].

El sistema de inferencia difusa fue introducido en 1965 por Lotfy Zadeh para ayudar a lidiar con los problemas que tienen información vaga o difusa; por ello, los valores exactos son usados ampliamente para aproximar el razonamiento en los eventos [3]. La teoría de la lógica difusa proporciona un marco matemático para modelar la incertidumbre de los procesos cognitivos humanos que puede manejar una computadora, proporcionando herramientas formales para su tratamiento; recientemente, se han utilizado métodos de lógica difusa en el proceso de evaluación de riesgos en diferentes situaciones [3].

A través de una revisión preliminar, se descubrió que existen descripciones parciales relacionadas al objeto de estudio, las cuales proporcionan un marco metodológico para la definición de la aplicación de lógica difusa a la evaluación de riesgos identificados sobre tecnologías de la información. Los análisis previos se han llevado a cabo en base a evidencia empírica y hay orientación de elementos diseminados guía para el respectivo análisis.

El objetivo principal de esta revisión sistemática es identificar los diversos métodos o técnicas de lógica difusa que ayuden a la identificación de riesgos de tecnologías de la información mediante factores para su evaluación. Asimismo, a través de dicha revisión se pretende encontrar complementariamente experiencias y propuestas bajo las cuales se debe evaluar los riesgos que involucran las tecnologías de información que serán sometidas a la aplicación de un modelo de lógica difusa.

Este artículo está distribuido de la siguiente manera: la sección 2 presenta la revisión sistemática de la literatura donde se definirán los conceptos clave: riesgos en Tecnologías de Información y lógica difusa; para comprender el contexto de investigación; la sección 3 describe el método de la revisión sistemática de la literatura; en el que se analizarán diferentes artículos relacionados al objetivo de estudio ya mencionado, con la finalidad de obtener información para ser utilizada en el estudio; la sección 4 presenta los resultados de la revisión que fueron analizados previamente teniendo como referentes los artículos seleccionados que abrirán una vista más amplia; para finalmente, en la sección 5 describir las conclusiones finales a la que nos llevó el proceso de investigación.

2 Revisión de la literatura

En esta sección se exponen algunas definiciones del entorno sobre el cual se realiza el estudio y el objeto de análisis.

2.1 Riesgos en Tecnologías de Información

La seguridad informática garantiza que la información privada de la empresa solo esté disponible para personas con privilegios suficientes para realizar las operaciones que se les otorgan a través de las políticas dadas por la empresa [2]. En las redes de TI, los activos clave que están protegidos son: información como datos de cuentas bancarias, registros de tarjetas de crédito y registros de clientes. La seguridad de cualquier sistema de TI se centra principalmente en la confidencialidad de los datos a toda costa, lo que incluso puede requerir el cierre de la red durante varias horas [4].

Realizar evaluaciones de vulnerabilidad también puede ser útil, lo que ayuda a identificar situaciones en las que no realizar ciertas actividades puede exponer a la organización a mayores riesgos. Por ejemplo, si no utiliza el último software antivirus, aumenta el riesgo de ataques de virus. Finalmente, los resultados del análisis de riesgos se resumen en un informe de gestión, que incluye las medidas de mitigación recomendadas [2]. Los riesgos y las preocupaciones sobre la seguridad a menudo conducen a mejoras generales en la seguridad de TI en una organización [5].

Actualmente, se utilizan muchos métodos para identificar y priorizar un riesgo. Entre estos métodos, el modelado de amenazas parece ser el más eficiente. Es un proceso que identifica, cuantifica y analiza los posibles riesgos de un sistema informático. El modelo identifica los activos más importantes de una aplicación informática y la descompone. También reconoce las amenazas a cada componente o activo y, respectivamente, las clasifica según sus probabilidades de riesgo. Después de calificar los riesgos, se desarrollan e implementan estrategias que pueden usarse para reducir las posibilidades de ocurrencia de riesgos [3].

Debido a ciertos problemas, es difícil obtener valores de riesgo cuantitativos confiables en la práctica. Primero, la mayoría de los factores de riesgo son de naturaleza cualitativa; es difícil estimarlos cuantitativamente. En segundo lugar, a menudo no es posible obtener información estadística sobre ciertos incidentes de seguridad de la información. En tercer lugar, los expertos generalmente no tienen información precisa sobre el valor de los activos [1].

Las entidades gubernamentales como cualquier otro tipo de organización cuenta con activos referentes a la tecnología los cuales se han visto vulnerables a riesgos de ciberataque tales como: SSH.Connection.Brute.Force, SMB.Login.Brute.Force, W32/Bancos.CFR!tr, W32/Tibs.PACKED!tr, W32/Generic_PUA_MC.FXK; en la situación de pandemia global [6] eso implica que existen fallas en el sistema de ciberseguridad del Estado que se deben analizar debido a la información sensible que se maneja. Si bien es cierto que los riesgos de ciberataque han aumentado por la coyuntura actual, éstos siempre han estado presentes [7]

2.2 Lógica Difusa

La lógica difusa es esencialmente una lógica multivalor que permite representar la incertidumbre matemática y la vaguedad [3]. Para lidiar con la vaguedad en el pensamiento humano, el padre de la lógica difusa Lotfi A. Zadeh fue el primero en introducir la teoría de conjuntos difusos, los cuales tiene la capacidad de representar - manipular los datos y la información que poseen en base a incertidumbres no estadísticas [8].

Un conjunto difuso también se puede ver como un conjunto de pares ordenados de la forma {x, C (x)} donde x es un elemento de X y C (x) denota su grado de pertenencia correspondiente. Las funciones de membresía se pueden representar en diferentes formas. Las funciones de membresía más comunes son: triangular; trapezoidal, membresía T, membresía S, gaussiana y exponencial. El tipo de función de membresía debe reflejar el problema que se enfrenta, la percepción del concepto representado y el nivel de detalle requerido [9]. Las técnicas de lógica difusa tipo 2 de intervalo son efectivas cuando existe un grado de incertidumbre en el proceso de razonamiento. Las funciones de membresía difusas indican el grado de verdad de entrada y salida [10]. La teoría de conjuntos difusos se ha diseñado para expresar matemáticamente la incertidumbre y la ambigüedad, y para proporcionar herramientas formales para lidiar con la falta de precisión inherente a los problemas de toma de decisiones [8].

La lógica difusa es una técnica apropiada de inteligencia artificial para aplicarse en el dominio de defensa cibernética; la gran cantidad de información generada por los sensores de monitoreo de la red abruma a los humanos y ésta puede automatizarse; codificar el conocimiento de los expertos en seguridad cibernética compensa la incapacidad de las computadoras de "razonar" sobre la operación prevista y los estados cambiantes de una red compleja [11].

Un sistema de inferencia difuso proporciona un marco matemático para simular la incertidumbre de los procesos cognitivos humanos que pueden ser manejados por una computadora [12]. Existen tres tipos básicos de sistemas de inferencia difusos: modelos Mamdani, Sugeno y Tsukamoto, cuyas formas de resultado se diferencian por las reglas difusas establecidas por cada modelo [13].

3 Método de la revisión sistemática de la literatura

La metodología de investigación acreditado como la Revisión Sistemática de la Literatura (RSL), es un estudio de mapeo sistemático, realizado con base en pautas de métodos de análisis y evaluación que lo justifiquen, del mismo modo se desarrolla un protocolo de revisión basado en procedimientos [14].

Las revisiones sistemáticas de la literatura y los estudios de mapeo se han centrado en la evaluación de riesgos en proyectos de desarrollo de software. Sin embargo, existen pocos tipos de revisión donde se han analizado específicamente los métodos de estudio de riesgos para los sistemas de TI usando lógica difusa para mejorar la toma de decisiones [14].

3.1 Necesidad de la revisión sistemática

La revisión sistemática de la literatura presentada en este estudio surge de la necesidad de identificar métodos o técnicas de lógica difusa y factores para la identificación de niveles de riesgos de Tecnologías de Información en entidades gubernamentales, para la revisión e identificación de experiencias y propuestas para un trabajo futuro por la necesidad de buscar alternativas eficientes que ayude a la toma rápida de decisiones soportado por una metodología, en este caso la lógica difusa; para minimizar los riesgos que se puedan presentar en entidades gubernamentales.

Basándonos en la plantilla Goal, Question, Metric (GQM por sus siglas en inglés) la cual busca establecer el objetivo de la investigación, se puede observar los componentes en la tabla I.

TABLA I. OBJETIVO DE LA INVESTIGACIÓN

CAMPO/CRITERIOS	VALOR
Objeto de estudio	Identificar y describir riesgos en Tecnologías de Información y métodos de lógica difusa
Propósito	Identificar, Describir
Foco	Factores, Métodos
Involucrados	Entidades Gubernamentales, TP-ISO/IEC 17799, Gestión de Riesgos, Lógica Difusa, Método Mamdani, Método Takagi-Sugeno-Kang (TSK)

3.2 Preguntas para la revisión sistemática

Para la definición y estructuración de las preguntas de investigación se utilizó como referencia la intención de investigación explicada en la sección anterior. La tabla II enumera las preguntas planteadas y la motivación para cada pregunta.

TABLA II. PREGUNTAS DE INVESTIGACIÓN

ID	PREGUNTAS	MOTIVACIÓN
PI-01	¿Cuáles son los métodos que se utilizan en la construcción de un modelo difuso?	Identificar métodos que son utilizados en la construcción de un modelo difuso.
PI-02	¿Cuáles son los factores que intervienen para la identificación de riesgos en Tecnologías de Información?	Identificar los factores para la identificación de riesgos de Tecnologías de información

Además, la tabla III presenta los problemas bibliométricos propuestos para obtener visibilidad del progreso de la investigación y las tendencias a lo largo del tiempo.

TABLA III. PREGUNTAS BIBLIOMÉTRICAS

ID	PREGUNTAS	MOTIVACIÓN
PB-01	¿Cuál es el número de publicaciones por tipo de artículo?	Determinar el número de publicaciones por tipo de artículo para identificar la convergencia de los mismos.
PB-02	¿Cuál es la frecuencia en la que se realizan publicaciones sobre este tema?	Identificar la frecuencia de las publicaciones para poder determinar la relevancia del tema en el tiempo.
PB-03	¿Cuáles son las publicaciones en las que se encontraron estudios relacionados al tema?	Identificar el campo de aplicación en las que se centralizan mayormente las publicaciones sobre este tema

3.3 Definición de las cadenas de búsqueda

La estrategia de cadena de búsqueda diseñada elegida fue la estrategia PICO en todo el proceso de iteración. En este proceso, la selección de los resultados se ha ajustado adecuadamente.

TABLA IV. POBLACIÓN - PICO

POBLACIÓN		
TÉRMINO PRINCIPAL	**TÉRMINOS ALTERNOS**	**JUSTIFICACIÓN**
Factores	Causas, Elementos	Realizar búsquedas que involucren la palabra FACTORES y sus derivados
Métodos	Procedimientos, técnicas	Realizar búsquedas que involucren la palabra MÉTODOS y sus derivados.

TABLA V. INTERVENCIÓN - PICO

INTERVENCIÓN		
IDENTIDAD	**TÉRMINO PRINCIPAL - TÉRMINOS ALTERNOS**	**JUSTIFICACIÓN**
Evaluación de riesgos en tecnologías de información	Riesgos en Tecnologías de Información, Seguridad de la información, Ciberseguridad	Se selecciona el término por ser el elemento en el cual se realizarán la evaluación de riesgos y se obtienen términos alternos por relacionarse al término principal.
Aplicación de Lógica Difusa	Lógica Difusa	Se selecciona el término por ser el elemento en el cual se realizarán la aplicación de acuerdo a métodos difusos y se obtienen términos alternos por relacionarse al término principal.

TABLA VI. COMPARACIÓN - PICO

COMPARACIÓN		
TÉRMINO PRINCIPAL	**TÉRMINOS ALTERNOS**	**JUSTIFICACIÓN**
No aplicable porque en la RSL no se compara con ningún estándar de referencia		

TABLA VII. RESULTADOS - PICO

RESULTADOS		
ENTIDAD	**TÉRMINOS ALTERNOS**	**JUSTIFICACIÓN**
Propuestas y experiencias de riesgos en Tecnologías de Información	Experiencias Propuestas	Identificar las experiencias / propuestas de riesgos en Tecnologías de Información para obtener como resultado de la investigación
Propuestas y experiencias de métodos de lógica difusa	Experiencias Propuestas	Revisar e identificar experiencias / propuestas de aplicaciones de métodos de lógica difusa para obtener como resultado de la investigación

Siguiendo las recomendaciones de la estrategia PICO, la cadena de búsqueda se obtuvo utilizando operadores booleanos en los elementos previamente definidos: población, intervención, comparación y resultados, descrito en la Tabla VIII.

Cabe indicar que los términos que generan la cadena de búsqueda mostrada en el siguiente cuadro, deben ser aplicadas al idioma español e inglés, donde se tomó como referencia el contexto de búsqueda en librerías digitales previamente seleccionadas de acuerdo a la relevancia del ámbito científico.

TABLA VIII. CADENA DE BÚSQUEDA

TÉRMINOS Y CONECTORES LÓGICOS A SER USADOS EN LA BÚSQUEDA	
CONCEPTO	TÉRMINOS
Población	(Factores OR Causas), (Métodos OR Técnicas)
Intervención	(Riesgos en Tecnologías de Información OR Seguridad de la Información OR Ciberseguridad), ("Lógica Difusa")
Comparación	No Aplica
Resultado	(Propuestas OR Experiencias)
Contexto	No Aplica

3.4 Criterios de inclusión y exclusión

Se desarrolló un protocolo de revisión en la fase inicial de búsqueda de la revisión. Contiene antecedentes de investigación, preguntas de investigación, estrategia de búsqueda, evaluación de validez, instrucciones de extracción de datos y estrategias de síntesis de datos. En base a lo expuesto se tomó en consideración los criterios inclusión y exclusión para la selección de los estudios [14].

TABLA IX. CRITERIOS DE INCLUSIÓN

CRITERIOS DE INCLUSIÓN	
C.I.1	Se consideran todos aquellos artículos provenientes de librerías digitales indexadas. Se consideran tesis provenientes de repositorios universitarios
C.I.2	Los artículos deben provenir del área de Inteligencia Artificial
C.I.3	Se aceptarán artículos que contengan Métodos de lógica difusa o Técnicas de Lógica Difusa o Procedimientos de lógica difusa o Aplicación de Lógica Difusa Se aceptarán artículos que contengan factores de riesgo de TI, Causas de riesgo de TI, Circunstancias de riesgo de TI, Ciberseguridad
C.I.4	Se considerarán todos los artículos que se encuentren dentro del rango de temporalidad definido (2010-2020)
C.I.5	Se aceptarán artículos provenientes de revistas científicas y conferencias. Tesis publicadas en cualquier base de datos

TABLA X. CRITERIOS DE EXCLUSIÓN

CRITERIOS DE EXCLUSIÓN	
C.E.1	Se excluirán artículos duplicados.
C.E.2	Se rechazarán artículos que no se encuentren en idioma inglés y/o español
C.E.3	Se rechazarán artículos de contenido similar, quedándose solo los que tengan el contenido más completo.
C.E.4	Se excluirán estudios secundarios, estudios terciarios y resúmenes.
C.E.5	Se excluirán artículos cuyo título no tenga relación con el objeto de estudio

Temporalidad. Según el criterio de inclusión C.I.4, se tomará en consideración los estudios desarrollados en los últimos 10 años, ya que el avance tecnológico es cambiante rápidamente en cada periodo de tiempo y los riesgos que éstos enfrentan del mismo modo, por ello se requiere esa cercanía.

Fuentes de Datos. Las librerías digitales indexadas consideradas por su distinción y sustento académico y científico para la selección de artículos fueron:

- ScienceDirect (https://www.sciencedirect.com/)
- IEEE Xplore (https://ieeexplore.ieee.org/Xplore/home.jsp)
- ACM Digital Library (https://dl.acm.org/)
- SciELO (https://scielo.org/)
- Google Scholar (https://scholar.google.com/)

Procedimientos para la selección de estudio. Se considera el siguiente procedimiento para la selección de artículos en la RSL:

- Paso 1: se procedió a ejecutar la cadena de búsqueda PICO, en las bases de datos indexadas definidas anteriormente, aplicando criterios de inclusión y exclusión referente a la tabla mostrada consecuentemente. Las cadenas de búsqueda fueron variando de acuerdo a la base de datos.
- Paso 2: se revisaron los títulos resultantes del Paso 1 y se excluyeron los que no guardaban relación con el objeto de estudio, y los que eran resúmenes o estudios secundarios. Del mismo modo se excluyeron artículos que no estaban en el idioma inglés o español.
- Paso 3: se revisaron los resúmenes de los artículos preliminarmente seleccionados en el Paso 2 para proceder con la exclusión establecida en la tabla XI. Se excluyeron artículos secundarios y los que no guardaban relación con el objeto de estudio.

- Paso 4: se realizó una revisión preliminar del contenido de los artículos seleccionados establecidos en el Paso 3, referentes a la introducción, marco teórico y conclusiones; y se aplicaron los criterios de la tabla XI.

TABLA XI. PROCEDIMIENTOS Y CRITERIOS DE SELECCIÓN

PROCEDIMIENTO	CRITERIO DE SELECCIÓN
Paso 1	CI.1, CI.2, CI.5, CE.1
Paso 2	CE.2, CE.4, CE.5
Paso 3	CE.3, CE.4
Paso 4	CI.3, CI.4

3.5 Criterios de calidad

Se procederá a la definición de un esquema de evaluación de calidad frente a los estudios seleccionados. Dentro del esquema se definió una lista de criterios para corroborar el cumplimiento de cada artículo, cada criterio será evaluado con un puntaje basado en una escala, de la siguiente manera: Si cumple (S) = 1, Cumple Parcialmente (P) = 0,5 y No Cumple (N) = 0 [15], el cual será definido en la tabla XII.

TABLA XII. CRITERIO DE EVALUACIÓN DE CALIDAD

Nro.	CRITERIO DE EVALUACIÓN DE CALIDAD
1	¿Se ha documentado adecuadamente el método selecto para el análisis de estudio?
	S: El método selecto ha sido documentado adecuadamente.
	P: El método selecto ha sido documentado parcialmente.
	N: No se ha documentado el método selecto.
2	¿El estudio ha abordado las amenazas frente a la validez?
	S: El estudio aborda las amenazas totalmente
	P: El estudio aborda las amenazas parcialmente
	N: No se detallan amenazas
3	¿Han sido descritos los aportes al estudio para los círculos científicos, académicos o para la industria?
	S: Han sido descritos los aportes al estudio claramente.
	P: Han sido descritos los aportes al estudio parcialmente.
	N: No se han mencionado aportes
4	¿Los resultados ayudan a responder las preguntas de investigación planteadas?
	S: Los resultados ayudaron a responder todas las preguntas de investigación.
	P: Los resultados ayudaron a responder algunas preguntas de investigación.
	N: Los resultados no ayudaron a responder las preguntas de investigación.

Estrategia para la extracción de datos. Con el propósito de extraer toda información relevante y necesaria para responder las preguntas de investigación planteadas, se elaboró un formulario que ayudará a la extracción de datos mostrados en la tabla XIII [16]:

TABLA XIII. FORMULARIO PARA LA EXTRACCIÓN DE DATOS

Criterio	Detalle	Relevancia
Identificador		
Fuente		
Título		
Autores		
Publicación		
Años de publicación		
Tipo de publicación		
Tipo de método difuso		
Objetivo del método		
Factores de evaluación de riesgo en Tecnologías de Información		
Dominio de aplicación		

Validar el protocolo de investigación. El protocolo utilizado para el desarrollo de la Revisión Sistemática de la Literatura fue revisado por la investigadora Norma Lucía Riquelme Challco y en segundo lugar revisado por el Mg. Fernando Manuel Asín Gomez.

4 Resultados

De acuerdo a la sustracción de datos obtenidos por los métodos de la RSL previamente determinados y dada la conformidad del protocolo de revisión se procederá a la descripción detallada de todos los pasos ejecutados.

4.1 Resultados de la búsqueda

Conforme a los pasos definidos en la sección 3, el primer paso para la selección de estudios consiste en ejecutar la cadena de búsqueda propuesta en las librerías digitales seleccionadas. En la siguiente tabla se muestran los resultados de las cadenas de búsqueda empleadas.

TABLA XIV. RESULTADOS DE LA BÚSQUEDA

BASE DE DATOS	FECHA	TOTAL
CADENA DE BÚSQUEDA		
SCIENCE DIRECT	Junio 2020	222
TITTLE (fuzzy logic methods OR techniques AND information technologies OR information security risk assessment OR security of the information risk OR cyber security risk OR vulnerability)		
IEEE Xplore	Junio 2020	36
(("All Metadata":fuzzy logic) AND "All Metadata":information security risk assessment)		
ACM	Junio 2020	19
(metho* OR techni*) AND ("fuzzy logic" AND fuzzy) AND (information tech* OR cyber*) AND ("information security risk") AND (information technologies risk*) AND (assess*)		
SCIELO	Junio 2020	10
fuzzy logic and IT risk		
GOOGLE SCHOLAR	Junio 2020	65
"lógica difusa" y tecnologías de la información o evaluación de riesgos de seguridad de la información o seguridad del riesgo de información o riesgo o vulnerabilidad de seguridad cibernética		

En la mayoría de casos fue necesario un ajuste a la cadena de búsqueda propuesta con variantes de acuerdo a la librería donde se hicieron las búsquedas pertinentes por la cantidad excesiva; y en algunos casos el escaso, de resultados obtenidos. Se realizaron los ajustes detallados posteriormente:

- La base de datos SciELO arrojaba escasos resultados frente a la cadena de búsqueda referente, por ello se moldeó a poner en búsqueda solo los términos principales de búsqueda.
- La base de datos Google Scholar presentaba muchos resultados no relevantes con el objetivo de estudio por lo que se tuvo que agregar términos secundarios para realizar la búsqueda más personalizada.

Para controlar mejor los términos que conforman la cadena de búsqueda, se seleccionó la opción "Búsqueda avanzada / Advanced Search" en algunas bibliotecas mencionadas a continuación:

- Science Direct
- IEEE Xplore
- ACM

Las referencias fueron procesadas con la herramienta gratuita Mendeley (https://www.mendeley.com) que fueron previamente exportadas en formato PDF para la revisión respectiva.

4.2 Resultados de filtros aplicados

4.2.1 Selección de estudios primarios

Los artículos encontrados en todas las bases de datos se exportan en formato PDF y se combinan en una tabla en un archivo de Excel (.xslx), que se utiliza como referencia para seleccionar la investigación principal propuesta anteriormente. A continuación, se muestra información detallada sobre la serie de pasos realizados para seleccionar el estudio.

Paso 1: La lista de artículos resultantes se obtuvo luego de ejecutar la cadena de búsqueda propuesta ordenada por “Más Relevancia” con la finalidad de obtener los artículos que tengan relación con la cadena de búsqueda ejecutada. La librería indexada que produjo la mayor cantidad de resultados fue ScienceDirect. Del mismo modo, sobre las listas de artículos obtenidos en cada librería se aplicaron los criterios de inclusión y exclusión definidos en la tabla XI.

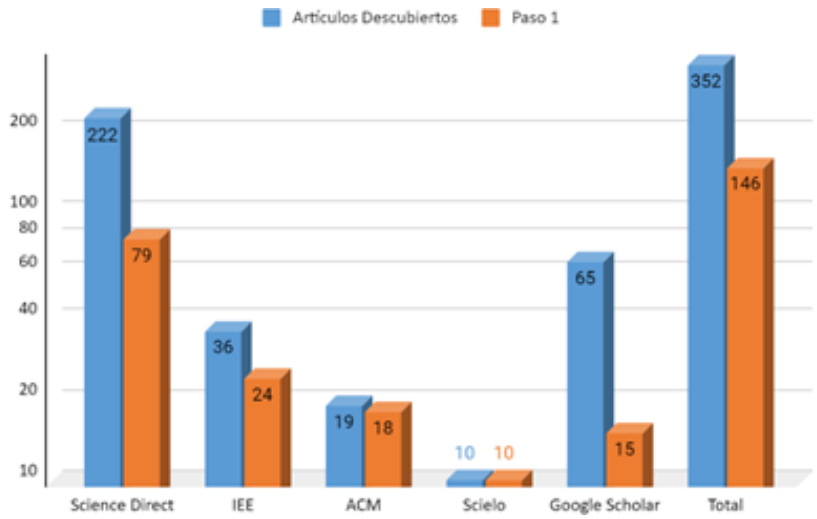

Fig. 1. Resultados por filtro: Paso 1

Paso 2: Sobre la lista de resultados del Paso 1, se revisaron los artículos para proceder con la exclusión de artículos no relevantes para el objeto de estudio para esta investigación de acuerdo a lo definido en los criterios descritos de la tabla XI.

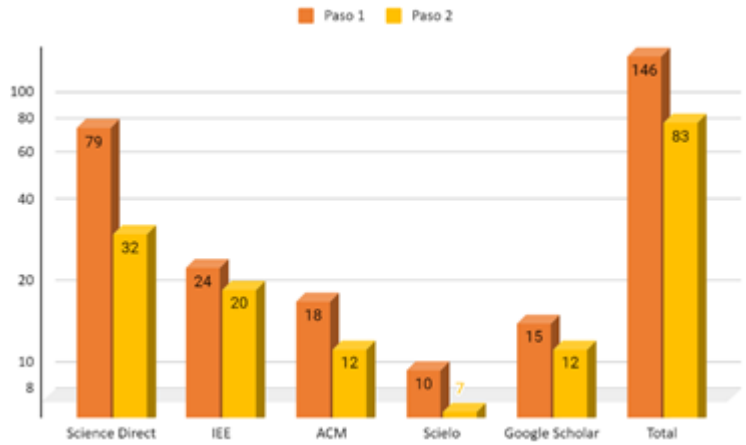

Fig. 2. Resultados por filtro: Paso 2

Paso 3: Los artículos provenientes del Paso 2, fueron revisados de acuerdo al campo Resumen y palabras clave y excluidos de acuerdo a lo definido en los criterios descritos en la tabla XI.

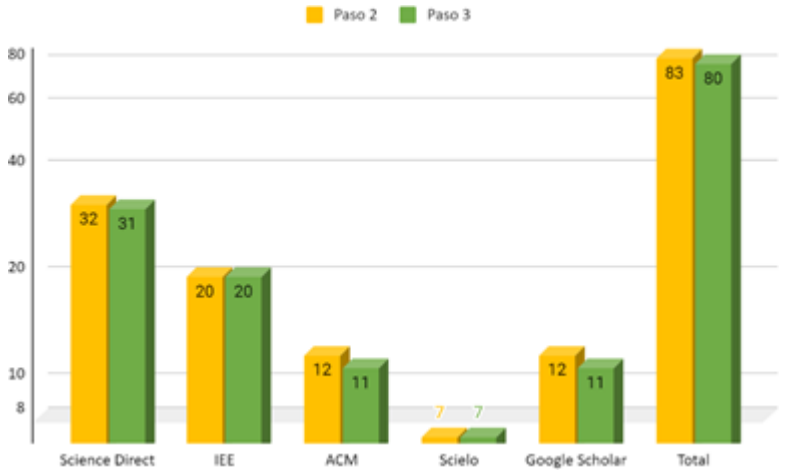

Fig. 3. Resultados por filtro: Paso 3

Paso 4: Para proceder con la revisión del contenido de los artículos restantes se procedió con la descarga de éstos de las librerías indexadas de donde provenían. Posteriormente, se realizó una revisión preliminar del contenido del artículo descargado, que consideró palabras clave, resúmenes, introducciones y conclusiones, así como artículos que no estaban relacionados con el contenido definido por los estándares descritos según la tabla XI.

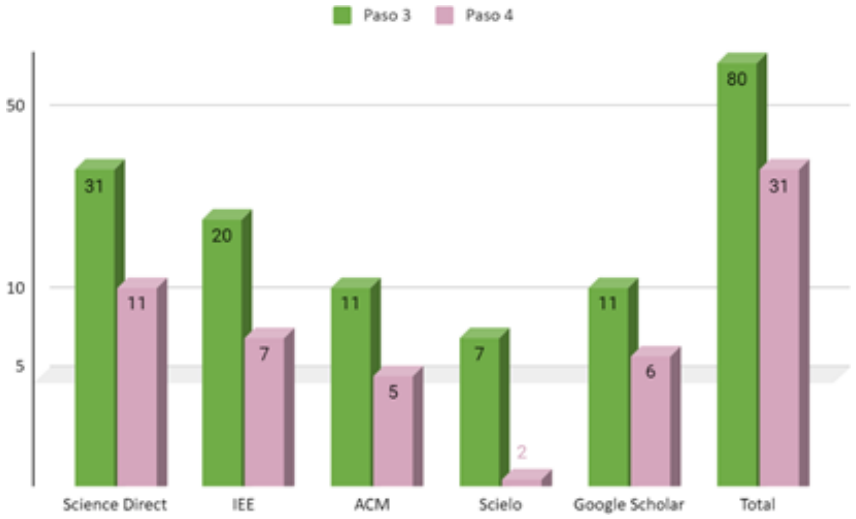

Fig. 4. Resultados por filtro: Paso 4

La tabla XV muestra los resultados de la selección del estudio, y el Apéndice A enumera todos los artículos resultantes de la selección.

TABLA XV. RESULTADOS DEL PROCESO DE SELECCIÓN DE ESTUDIOS

Base de Datos	**Artículos Descubiertos**	**Paso 1**	**Paso 2**	**Paso 3**	**Paso 4**
ScienceDirect	222	79	32	31	11
IEE	36	24	20	20	7
ACM	19	18	12	11	5
SciELO	10	10	7	7	2
Google Scholar	65	15	12	11	6
Total	352	146	83	80	31

4.2.2 Evaluar calidad de los estudios

Sobre el total de 31 artículos resultantes se aplicó la lista de criterios de comprobación definidos en la sección 3. Los resultados de la evaluación se muestran en la tabla XVI. A partir de la tabla se puede observar que sólo 3 artículos que equivalen al 9,7% de los 31 artículos obtuvieron una calificación menor al 50% del puntaje total, lo cual se puede considerar como un aceptable indicador de calidad de los estudios seleccionados para la Revisión Sistemática de la Literatura.

TABLA XVI. EVALUACIÓN DE CALIDAD DE LOS ESTUDIOS

ID	C1	C2	C3	C4	TOTAL	% Total
1	1	0	1	1	3	75%
2	1	0	1	0,5	2,5	62,50%
3	1	0	0,5	0,5	2	50%
4	0,5	0	1	0,5	2	50%
5	1	0	0,5	1	2,5	62,50%
6	0,5	0	1	0,5	2	50%
7	0,5	0	1	0,5	2	50%
8	1	0	0,5	0,5	2	50%
9	1	0	1	1	3	75%
10	1	0	1	1	3	75%
11	1	0	1	1	3	75%
12	1	0,5	0	1	2,5	62,50%
13	0,5	0	0,5	1	2	50%
14	0,5	0	0	1	1,5	37,50%
15	1	0	1	1	3	75%
16	0,5	0	0,5	1	2	50%
17	1	0	0,5	1	2,5	62,50%
18	1	0	0,5	1	2,5	62,50%

19

19	0,5	0	0,5	1	2	50%
20	1	0,5	1	1	3,5	87,50%
21	1	0	1	0,5	2,5	62,50%
22	0,5	0	1	0,5	2	50%
23	1	0	1	0,5	2,5	62,50%
24	0,5	0	0,5	0,5	1,5	37,50%
25	1	0	0	1	2	50%
26	0,5	0,5	0,5	0,5	2	50%
27	1	0,5	1	0,5	3	75%
28	1	0,5	1	0,5	3	75%
29	1	0,5	0,5	1	3	75%
30	1	1	1	1	4	100%
31	0,5	0	0	1	1,5	37,50%

4.2.3 Extraer resultados relevantes

Los formularios para la extracción de datos deben ser diseñados con la finalidad de recolectar la información necesaria para resolver las preguntas de investigación del estudio. Basado en lo ya mencionado, se diseñó el formulario descrito en la sección 3 para la recopilación de la información relevante de cada artículo. Cada uno de los artículos fue leído y simultáneamente se procedió con el llenado de su formulario respectivo, el cual se realizó en el mismo idioma en el que se encontraba dicho artículo. El detalle de los criterios para los cuales no se encontró información relevante fue llenado con una simbología (-).

En la tabla XVII, se observa un ejemplo de los datos extraídos como información relevante de cada uno de los artículos seleccionados. Los formularios de los otros artículos se encuentran descritos en el Apéndice B.

TABLA XVII. EJEMPLO DE EXTRACCIÓN DE DATOS DE UN ESTUDIO PRIMARIO

Criterio	**Detalle**	**Relevancia**
Identificador	1	-
Fuente	ScienceDirect	PB-01
Título	Risk assessment in IT outsourcing using fuzzy decision-making approach: An Indian perspective	PB-01
Autores	Samantra, Chitrasen; Datta, Saurav; Mahapatra, Siba Shankar	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2014	PB-02
Tipo de publicación	Elsevier Ltd	PB-01
Tipo de modelo difuso	Use of 'Incentre of Centroid' method	PI-01
Objetivo del modelo	An improved decision-making method using fuzzy set theory has been attempted for converting linguistic data into numeric risk ratings	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Likelihood of occurrence, and impact of risk	PI-02
Dominio de aplicación	Expert Systems with Applications	-

4.3 Análisis bibliométrico

Esta sección presenta el análisis de tendencias de los artículos seleccionados para esta RSL, teniendo en cuenta factores establecidos como el tiempo, tipo de artículo y tema abordado.

1. Pregunta bibliométrica 1 (PB-01)

¿Cuál es el número de publicaciones por tipo de artículo?

En la Fig., 5 se muestra el número de publicaciones por tipo de artículo representadas en porcentajes. Podemos observar que los artículos de revista (Journal Article) representan el 90,3% del total de artículos seleccionados para la RSL; luego tenemos a las tesis (Thesis) con un 9,7%. De este análisis se concluye que los artículos de revistas proporcionan mayores fuentes de estudios sobre la aplicación de lógica evaluada a los factores de riesgo de TI.

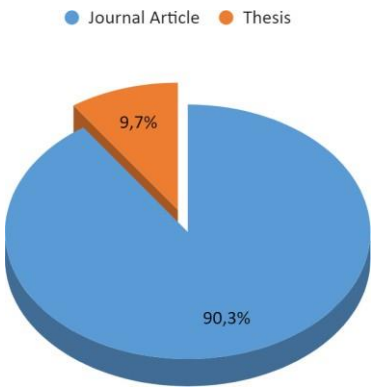

Fig. 5. Cantidad de publicaciones por tipo. Elaboración Propia

2. Pregunta bibliométrica 2 (PB-02)

¿Cuál es la frecuencia en la que se realizan publicaciones sobre este tema?

Al analizar los resultados obtenidos luego de ejecutar la cadena de búsqueda y la selección mostrada en la tabla XVI, se puede observar en la Fig. 6 un incremento en el número de publicaciones con respecto a la aplicación de la lógica difusa para la evaluación de factores de riesgos de TI siendo el 2018 el año donde hubo mayor número de publicaciones; partiendo del año 2010 al año 2020. De un total de 31 artículos.

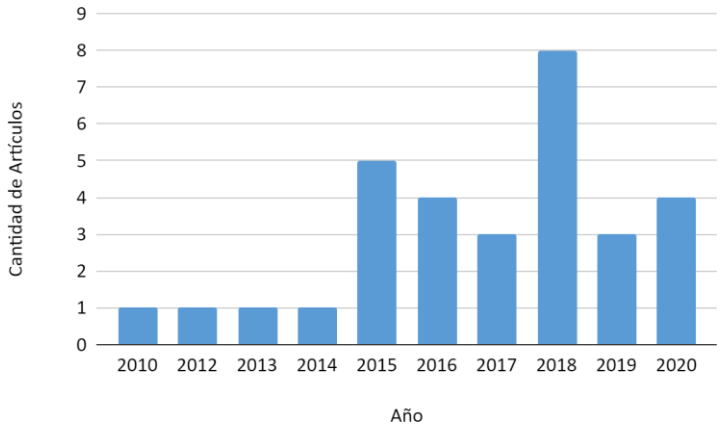

Fig. 6. Frecuencia de publicaciones. Elaboración propia.

3. Pregunta bibliométrica 3 (PB-03)

¿Cuáles son las publicaciones en las que se encontraron estudios relacionados al tema?

En la tabla XVIII se presentan las publicaciones de donde se han extraído los artículos seleccionados. A partir de ese análisis se puede observar la existencia de una recurrencia de publicaciones en la editorial Elsevier Ltd., del dominio de computación y seguridad donde se concentran la mayoría de los artículos elegidos. Asimismo, también se puede observar la presencia de otros dominios como: inteligencia artificial, matemáticas, seguridad de la información, entre otros.

TABLA XVIII. PUBLICACIONES CORRESPONDIENTES A LOS ARTÍCULOS SELECCIONADOS

Publicación	**Cantidad**
Elsevier Ltd.	11
ACM International Conference Proceeding Series	3
Entre Ciencia e Ingeniería	2
2016 Dynamics of Systems, Mechanisms and Machines, Dynamics 2016	1
2020 International Conference in Mathematics, Computer Engineering and Computer Science, ICMCECS 2020	1
2015 International Siberian Conference on Control and Communications, SIBCON 2015 - Proceedings	1
IEEE LATIN AMERICA TRANSACTIONS	1
2017 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2017 – Proceedings	1
Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015	1
2016 Annual Conference of the North American Fuzzy Information Processing Society (NAFIPS)	1
Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering	1
SIN'09 - Proceedings of the 2nd International Conference on Security of Information and Networks	1
Contaduría y Administración	1
Revista Científica Ciencia y Tecnología	1
Universidad Regional Autónoma de los Andes	1

Facultad de Ciencias Matemáticas y Físicas	1
Universidad Nacional del Santa	1
Revista Control, Cibernética y Automatización	1

4.4 Sintetizar los datos extraídos

Luego de la ejecución de la RSL según el procedimiento establecido en la sección 3 del presente estudio, se seleccionaron un total de 31 artículos en los que se presentan los métodos empleados en cuanto a lógica difusa, representada en la tabla ¿? en la cual se indica el método difuso, dominio de la aplicación y la fecha. Es preciso indicar, que se digitó la simbología (-) cuando no se encontró información referente al modelo difuso.

TABLA XIX. TIPOS DE MÉTODOS DIFUSOS IDENTIFICADOS EN LA REVISIÓN

ID	Dominio de Aplicación	Tipo de método difuso	Año
1	Expert Systems with Applications	Use of 'Incentre of Centroid' method	2014
2	Information Security and Applications	-	2020
3	Computers and Security	-	2016
4	Computers and Electrical Engineering		2018
5	Computers and Security	Mamdani Fuzzy model	2018
6	Reliability Engineering and System Safety	-	2018
7	Computers and Security	-	2015
8	Computers and Security		2020
9	Computers and Industrial Engineering	Mamdani-type FIS	2020
10	Information Management	Triangular Membership Fuzzy Set	2018
11	Information Security and Applications	Interval type-2 fuzzy logic controller (IT2FLC) - Mamdani fuzzy inference system	2018
12	Dynamics of Systems, Mechanisms and Machines	Fuzzy membership function	2017
13	Mathematics, Computer Engineering and Computer Science	Fuzzy cognitive maps and fuzzy inference system	2020
14	Communications	Fuzzy system inference	2015
15	Artificial Intelligence	Función trapezoidal	2018
16	Industrial Engineering, Applications and Manufacturing	Fuzzy inference method	2017
17	Computing and Communications	Fuzzy Inference - Mamdani	2015
18	Fuzzy Information	Fuzzy Associative Memory (FAM) - FLUF: Fuzzy logic utility framework	2016
19	Artificial Intelligence	Fuzzy logic and fuzzy inference scheme	2015
20	Artificial Intelligence	Fuzzy Delphi method	2019
21	Software Engineering	-	2013
22	Computer Systems and Technologies	-	2012
23	Security of Information and Networks	-	2010
24	Contaduría y Administración	Modelo en tiempo continuo fuzzy (MCF), Fuzzy pay-off method (FPOM), modelos en tiempo discreto fuzzy (MDF)	2017

25	Ciencia e Ingeniería	Método del centroide	2015
26	Ciencia y Tecnología	-	2018
27	Sistemas Mercantiles	-	2019
28	Ciencia e Ingeniería	-	2019
29	Ingeniería En Sistemas Computacionales	Mamdani - función de membresía trapezoidal	2018
30	Ingeniería de Sistemas e Informática	Modelo Mamdani	2016
31	Ciencias Informáticas	Mamdani - Membresía Triangular	2016

1. Pregunta de investigación 1 (PI-01)

   ¿Cuáles son los métodos que se utilizan en la construcción de un modelo difuso?

   A través de la extracción de información de cada artículo se pudo encontrar diferentes tipos de métodos difusos. Tal como se puede observar en la tabla XIX el modelo más usado fue Mamdani, del mismo modo se puede apreciar el uso de las distintas membresías tal como triangular y trapezoidal para su desarrollo.

   Método Mamdani: El método Mamdani es el más usado en la lógica difusa porque cuenta con una estructura simple en cuanto sus operaciones. Su desarrollo es simple solo se debe tener en cuenta las variables de entrada y de salida, una vez establecidas dichas variables, se procede a elegir el tipo de membresía a usar a la cual se definirán el rango y los parámetros, donde también se clasificarán en niveles cualitativos cada tipo de variable. Luego de ello, se configuran las reglas difusas para la evaluación respectiva.

2. Pregunta de investigación 2 (PI-02)

   ¿Cuáles son los factores que intervienen en la identificación de riesgos en Tecnologías de Información?

   Al analizar los resultados obtenidos en la extracción de datos de cada artículo se puede encontrar que en cuanto a las tecnologías de información, seguridad de la información y ciberseguridad existen muchas riesgos, amenazas y vulnerabilidades, en la RSL de los artículos se pudo encontrar que éstos varían desde la infección de virus hasta ataques a servidores o sistemas de información, las TI involucran elementos de configuración muy importantes para una empresa u organización, sobre todo en el caso de una entidad gubernamental donde se tienen grandes registros de información no solo del personal sino casi de toda la población de una ciudad o país, ante ello es necesario prevenir o anticiparse al riesgo ya que este puede verse involucrado en un activo lógico o físico. Los riesgos no solo se deben centralizar en los que los hombres desarrollan sino también en riesgos ambientales que pueden ocasionar grandes pérdidas si no se tiene un debido análisis de riesgos o plan de contingencia.
   Los principales factores que intervienen en la identificación de los antes mencionados son: probabilidad del riesgo, impacto de la amenaza y la severidad del daño que podría ocasionar.

4.5 Amenazas de Validez

Para la ejecución de la cadena de búsqueda se consideraron 5 bases de datos digitales, teniendo como referencia 31 artículos que cumplían parcialmente con los criterios de inclusión y exclusión. La selección de estudios primarios redujo en gran cantidad los artículos encontrados en primera instancia.

Todas las librerías digitales y artículos utilizados para la realización del presente estudio se encuentran debidamente referenciados y disponibles en internet. Todos los artículos que formaron parte de esta RSL se encuentran detallados en el Apéndice B.

4.6 Lecciones Aprendidas

Durante la elaboración de esta RSL se originaron las siguientes lecciones aprendidas:

El tema de estudio de esta revisión fue abordado parcialmente en cuanto a modelos difusos y factores de riesgos de TI, fueron pocos artículos encontrados referentes que relacionan el objetivo de estudio.

Referente a la cadena de búsqueda establecida fue necesaria su modificación en cuanto a la librería de búsqueda, no solo en la estructura, sino también en el lenguaje para cumplir de mejor manera la localización de artículos con referencia al objeto de estudio.

Se tomaron artículos que evidenciaban de manera separada el objetivo de estudio: modelos difusos y factores de riesgo de TI, con la finalidad de no dejar artículos fuera solo por no cumplir exactamente con el análisis del título y que servirían para el trabajo futuro.

5 Conclusiones

Este estudio presenta los resultados de una revisión sistemática de 31 artículos académicos; debidamente filtrados por los criterios de inclusión y exclusión, que se encontraron en 5 librerías digitales diferentes y bases de datos de indexadas que son altamente relevantes para los campos científicos y académicos. Del mismo modo, en el análisis bibliométrico, la investigación se clasifica por año de publicación, y se puede observar que la cantidad de investigaciones relacionadas ha aumentado entre los años 2010 a 2020. Esto muestra el interés en aplicar una lógica difusa a la toma de decisiones, especialmente en la evaluación de los factores de riesgo de TI relacionados con la seguridad de la información y ciberseguridad.

Dentro de los dominios de aplicación en donde se concentra la mayor cantidad de artículos seleccionados se encuentran computación y seguridad, así como también inteligencia artificial; lo cual indica la creciente necesidad de un marco metodológico para la realización de aplicación de métodos de lógica difusa con relación a los factores de riesgo de TI. Se pudieron evidenciar contenidos que sirvieron y servirán de gran aporte para diferentes investigaciones.

La Inteligencia Artificial se pone cada vez más en plataforma para su uso en distintas áreas, pero sobre todo en el área de la Ingeniería de Sistemas; siendo una de sus ramas la conocida lógica difusa que ayuda a la toma de decisiones puesto que es un semejante del pensamiento humano siendo de un nivel experto del área que se quiere abarcar.

Los riesgos en las Tecnologías de la Información aumentan tanto o igual como su avance a medida de los tiempos, muchas veces no se puede mitigar ello ocasionando muchas pérdidas; y teniendo como referente una organización, la pérdida económica. Estos riesgos deben ser identificados, clasificados y evaluados; es necesario que una organización cuente con un personal encargado de la seguridad de la información, así como también una adecuada gestión de riesgos y su debido plan de contingencia o de continuidad. Existen muchos factores de riesgo creados por el hombre; sin embargo, también se encuentran los factores de riesgo ambientales.

Este estudio busca resaltar la importancia de contar con un modelo difuso que permita evaluar los riesgos de tecnologías de la información con el fin de mitigar o evitar la posibilidad de ocurrencia de la amenaza y el impacto que podría ocasionar, por ello es importante identificarlos y valorarlos; permitiendo el cálculo de valores cualitativos en base a los factores de riesgo de TI y la aproximación en su medición en un rango numérico, capaz de mejorar la evaluación de éstos. El método difuso va ser capaz de producir y ofrecer datos más cercanos que la metodología tradicional.

Como trabajo futuro, se propone desarrollar un método empírico, teniendo como soporte el presente estudio; donde se pueda tomar como referente una organización gubernamental aplicando criterios de clasificación de riesgos en base a factores, aplicando normas técnicas y el método Mamdani para el uso de la lógica difusa.

Referencias

[1] I. V. Anikin, “Information security risk assessment and management method in computer networks,” *2015 Int. Sib. Conf. Control Commun. SIBCON 2015 - Proc.*, 2015, doi: 10.1109/SIBCON.2015.7146975.

[2] J. M. Velásquez Ruiz, “Software de aplicación web basado en lógica difusa, para mejorar la evaluación de riesgos en tecnologías de información, en la Oficina de Tecnologías de Información y Comunicaciones de la Universidad Nacional del Santa,” UNIVERSIDAD NACIONAL DEL SANTA FACULTAD DE INGENIERIA, 2016.

[3] M. Alali, A. Almogren, M. M. Hassan, I. A. L. Rassan, and M. Z. A. Bhuiyan, “Improving risk assessment model of cyber security using fuzzy logic inference system,” *Comput. Secur.*, vol. 74, pp. 323–339, 2018, doi: 10.1016/j.cose.2017.09.011.

[4] D. Upadhyay and S. Sampalli, “SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations,” *Comput. Secur.*, vol. 89, p. 101666, 2020, doi: 10.1016/j.cose.2019.101666.

[5] E. Zio, “The future of risk assessment,” *Reliab. Eng. Syst. Saf.*, vol. 177, pp. 176–190, 2018, doi: 10.1016/j.ress.2018.04.020.

[6] Grupo El Comercio, “Los cinco ciberataques más frecuentes en el Perú,” *Gestión Perú*, Lima, pp. 1–4, Aug. 07, 2020.

[7] Grupo El Comercio, “Sectores más propensos a sufrir un ciberataque,” *Gestión Perú*, Lima, pp. 1–2, Jul. 17, 2020.

[8] C. Samantra, S. Datta, and S. S. Mahapatra, “Risk assessment in IT outsourcing using fuzzy decision-making approach: An Indian perspective,” *Expert Syst. Appl.*, vol. 41, no. 8, pp. 4010–4022, 2014, doi: 10.1016/j.eswa.2013.12.024.

[9] A. P. Henriques de Gusmão, M. Mendonça Silva, T. Poleto, L. Camara e Silva, and A. P. Cabral Seixas Costa, “Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory,” *Int. J. Inf. Manage.*, vol. 43, no. August, pp. 248–260, 2018, doi: 10.1016/j.ijinfomgt.2018.08.008.

[10] D. K. Jana and R. Ghosh, “Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security,” *J. Inf. Secur. Appl.*, vol. 40, pp. 173–182, 2018, doi: 10.1016/j.jisa.2018.04.002.

[11] E. A. Newcomb and R. Hammell, “FLUF: Fuzzy logic utility framework to support computer network defense decision making,” *Annu. Conf. North Am. Fuzzy Inf. Process. Soc. - NAFIPS*, vol. 0, 2016, doi: 10.1109/NAFIPS.2016.7851582.

[12] B. M. Moreno-Cabezali and J. M. Fernandez-Crehuet, “Application of a fuzzy-logic based model for risk assessment in additive manufacturing R&D projects,” *Comput. Ind. Eng.*, vol. 145, p. 106529, 2020, doi: 10.1016/j.cie.2020.106529.

[13] Y. Azán Basallo, N. Martínez Sanchez, and V. Estrada Senti, “La lógica difusa para la evaluación del riesgo de seguridad informática a bases de batos,” *Rev. Control. Cibernética y Autom.*, vol. Vol. III, no. June, p. 5, 2016, [Online]. Available: https://www.researchgate.net/profile/Yasser_Azan_Basallo/publication/311592404_La_logica_difusa_para_la_evaluacion_del_riesgo_de_seguridad_informatica_a_bases_de_batos/links/58ddab71aca27206a8a1c0b3/La-logica-difusa-para-la-evaluacion-del-riesgo-de-seguri.

[14] S. M. Sulaman, K. Weyns, and M. Höst, “A Review of Research on Risk Analysis Methods for IT Systems Categories and Subject Descriptors,” *Proc. 17th Int. Conf. Eval. Assess. Softw. Eng.*, pp. 86–96, 2013.

[15] B. D. Rouhani, M. N. Z. R. Mahrin, F. Nikpay, R. B. Ahmad, and P. Nikfard, “A systematic literature review on Enterprise Architecture Implementation Methodologies,” *Inf. Softw. Technol.*, vol. 62, no. 1, pp. 1–20, 2015, doi: 10.1016/j.infsof.2015.01.012.

[16] B. Kitchenham, O. Pearl Brereton, D. Budgen, M. Turner, J. Bailey, and S. Linkman, “Systematic literature reviews in software engineering - A systematic literature review,” *Inf. Softw. Technol.*, vol. 51, no. 1, pp. 7–15, 2009, doi: 10.1016/j.infsof.2008.09.009.

APÉNDICE

A. Artículos Seleccionados

ID	Biblioteca	Título	Autor	Año	Tipo de Documento
1	ScienceDirect	Risk assessment in IT outsourcing using fuzzy decision-making approach: An Indian perspective	Samantra, Chitrasen; Datta, Saurav; Mahapatra, Siba Shankar	2014	Journal Article
2	ScienceDirect	synERGY: Cross-correlation of operational and contextual data to timely detect and mitigate attacks to cyber-physical systems	Skopik, Florian; Landauer, Max; Wurzenberger, Markus; Vormayr, Gernot; Milosevic, Jelena; Fabini, Joachim; Prüggler, Wolfgang; Kruschitz, Oskar; Widmann, Benjamin; Truckenthanner, Kevin; Rass, Stefan; Simmer, Michael; Zauner, Christoph	2020	Journal Article
3	ScienceDirect	A review of cyber security risk assessment methods for SCADA systems	Cherdantseva, Yulia; Burnap, Pete; Blyth, Andrew; Eden, Peter; Jones, Kevin; Soulsby, Hugh; Stoddart, Kristan	2016	Journal Article
4	ScienceDirect	Cyber-security in smart grid: Survey and challenges	Mrabet, Zakaria El; Kaabouch, Naima; Ghazi, Hassan El; Ghazi, Hamid El	2018	Journal Article
5	ScienceDirect	Improving risk assessment model of cyber security using fuzzy logic inference system	Alali, Mansour; Almogren, Ahmad; Hassan, Mohammad Mehedi; Rassan, Iehab A.L.; Bhuiyan, Md Zakirul Alam	2018	Journal Article
6	ScienceDirect	The future of risk assessment	Zio, E.	2018	Journal Article
7	ScienceDirect	Incorporating attacker capabilities in risk estimation and mitigation	Ben Othmane, Lotfi; Ranchal, Rohit; Fernando, Ruchith; Bhargava, Bharat; Bodden, Eric	2015	Journal Article
8	ScienceDirect	SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations	Upadhyay, Darshana; Sampalli, Srinivas	2020	Journal Article
9	ScienceDirect	Application of a fuzzy-logic based model for risk assessment in additive manufacturing R&D projects	Moreno-Cabezali, Belen Maria; Fernandez-Crehuet, Jose Maria	2020	Journal Article
10	ScienceDirect	Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory	Henriques de Gusmão, Ana Paula; Mendonça Silva, Maisa; Poleto, Thiago; Camara e Silva, Lúcio; Cabral Seixas Costa, Ana Paula	2018	Journal Article
11	ScienceDirect	Novel interval type-2 fuzzy logic controller for improving	Jana, Dipak Kumar; Ghosh, Ramkrishna	2018	Journal Article

		risk assessment model of cyber security			
12	IEEE Xplore	Information security risks assessment in telecommunication network of the university	Anikin, Igor V.	2017	Journal Article
13	IEEE Xplore	Information Asset Classification and Labelling Model Using Fuzzy Approach for Effective Security Risk Assessment	Alonge, Christianah Yetunde; Arogundade, Oluwasefunmi Tale; Adesemowo, Kayode; Ibrahalu, Friday Thomas; Adeniran, Olusola John; Mustapha, Abiodun Muyideen	2020	Journal Article
14	IEEE Xplore	Information security risk assessment and management method in computer networks	Anikin, Igor V.	2015	Journal Article
15	IEEE Xplore	Artificial Intelligence Techniques for Information Security Risk Assessment	Y. A. Basallo, V. E. Sentí, N. M. Sánchez	2018	Journal Article
16	IEEE Xplore	Using fuzzy logic for vulnerability assessment in telecommunication network	Anikin, I. V.	2017	Journal Article
17	IEEE Xplore	Countermeasure security risks management in the internet of things based on fuzzy logic inference	Kotenko, Igor; Saenko, Igor; Ageev, Sergey	2015	Journal Article
18	IEEE Xplore	FLUF: Fuzzy logic utility framework to support computer network defense decision making	Newcomb, E. Allison; Hammell, Robert	2016	Journal Article
19	ACM	Information security risk management in computer networks based on fuzzy logic and cost/benefit ratio estimation	Anikin, Igor; Emaletdinova, Lilia Yu	2015	Journal Article
20	ACM	Risks facing smart city information security in Hangzhou	Daniel, T. S.E.; Li, Rui; Zheng, Hanqi	2019	Journal Article
21	ACM	A Review of Research on Risk Analysis Methods for IT Systems Categories and Subject Descriptors	Sulaman, Sardar Muhammad; Weyns, Kim; Höst, Martin	2013	Journal Article
22	ACM	Towards a security evaluation model based on security metrics	Breier, Jakub; Hudec, Ladislav	2012	Journal Article
23	ACM	Improving risk assessment methodology: A statistical design of experiments approach	Singh, Anand; Lilja, David	2010	Journal Article
24	SciELO	Lógica difusa y el riesgo financiero. Una propuesta de clasificación de riesgo financiero al sector cooperativo	Díaz Córdova, Jaime Fabián; Coba Molina, Edisson; Navarrete, Paúl	2017	Journal Article
25	SciELO	Definición de un modelo de medición de análisis de riesgos de la seguridad de la información aplicando lógica difusa y sistemas basados en el conocimiento	Angarita, A A; Rios, C A Tabares J I	2015	Journal Article

29

26	Google Scholar	La seguridad de la información: Aspecto crucial que toda empresa del siglo XXI debe gestionar	MSc, Roxana Patricia Cedeño Villacís	2018	Journal Article
27	Google Scholar	Gestión de riesgos informáticos utilizando NIST SP-800 E ISO/IEC 27005 en la empresa International Forest Products Del Ecuador S.A.	Oña Garcés Mercedes Beatriz	2019	Thesis
28	Google Scholar	Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana	Carvajal, D. L.; Cardona, A.; Valencia, F. J.	2019	Journal Article
29	Google Scholar	Análisis de los mecanismos de seguridad lógicos y físicos en los centros de datos de entidades públicas ecuatorianas ante la ciberdelincuencia	Rodrigo, Danny; Calderón, Jaramillo	2018	Thesis
30	Google Scholar	Software de aplicación web basado en lógica difusa, para mejorar la evaluación de riesgos en tecnologías de información, en la Oficina de Tecnologías de Información y Comunicaciones de la Universidad Nacional del Santa	Velásquez Ruiz, José Martín	2016	Thesis
31	Google Scholar	La lógica difusa para la evaluación del riesgo de seguridad informática a bases de batos	Azán Basallo, Yasser; Martínez Sanchez, Natalia; Estrada Senti, Vivian	2016	Journal Article

B. Formularios de Extracción

A continuación, se presenta la información extraída de todos los artículos seleccionados que contribuyeron a responder las preguntas de investigación.

Criterio	**Detalle**	**Relevancia**
Identificador	1	-
Fuente	ScienceDirect	PB-01
Título	Risk assessment in IT outsourcing using fuzzy decision-making approach: An Indian perspective	PB-01
Autores	Samantra, Chitrasen; Datta, Saurav; Mahapatra, Siba Shankar	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2014	PB-02
Tipo de publicación	Elsevier Ltd	PB-01
Tipo de método difuso	Use of 'Incentre of Centroid' method	PI-01
Objetivo del método	An improved decision-making method using fuzzy set theory has been attempted for converting linguistic data into numeric risk ratings	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Likelihood of occurrence, and impact of risk	PI-02
Dominio de aplicación	Expert Systems with Applications	-

Criterio	Detalle	Relevancia
Identificador	2	-
Fuente	ScienceDirect	PB-01
Título	synERGY: Cross-correlation of operational and contextual data to timely detect and mitigate attacks to cyber-physical systems	PB-01
Autores	Skopik, Florian; Landauer, Max; Wurzenberger, Markus; Vormayr, Gernot; Milosevic, Jelena; Fabini, Joachim; Prüggler, Wolfgang; Kruschitz, Oskar; Widmann, Benjamin; Truckenthanner, Kevin; Rass, Stefan; Simmer, Michael; Zauner, Christoph	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2020	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Multiple types of anomalies	PI-02
Dominio de aplicación	Information Security and Applications	-

Criterio	Detalle	Relevancia
Identificador	3	-
Fuente	ScienceDirect	PB-01
Título	A review of cyber security risk assessment methods for SCADA systems	PB-01
Autores	Cherdantseva, Yulia; Burnap, Pete; Blyth, Andrew; Eden, Peter; Jones, Kevin; Soulsby, Hugh; Stoddart, Kristan	PB-01
Publicación	Elsevier	PB-03
Años de publicación	2016	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	Fuzzy methods seem promising in SCADA risk assessment their current application is limited	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Application domain; the stages of risk management addressed; key risk management concepts covered; impact measurement; sources of probabilistic data; evaluation and tool support.	PI-02
Dominio de aplicación	Computers and Security	-

Criterio	Detalle	Relevancia
Identificador	4	-
Fuente	ScienceDirect	PB-01
Título	Cyber-security in smart grid: Survey and challenges	PB-01
Autores	Mrabet, Zakaria El; Kaabouch, Naima; Ghazi, Hassan El; Ghazi, Hamid El	PB-01
Publicación	Elsevier Ltd	PB-03

Años de publicación	2018	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Review the security requirements, to provide descriptions of several severe cyber-attacks, and to propose a cyber-security strategy to detect and count these attacks.	PI-02
Dominio de aplicación	Computers and Electrical Engineering	-

Criterio	**Detalle**	**Relevancia**
Identificador	5	-
Fuente	ScienceDirect	PB-01
Título	Improving risk assessment model of cyber security using fuzzy logic inference system	PB-01
Autores	Alali, Mansour; Almogren, Ahmad; Hassan, Mohammad Mehedi; Rassan, Iehab A.L.; Bhuiyan, Md Zakirul Alam	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2018	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Mamdani Fuzzy model	PI-01
Objetivo del método	Vulnerability, threat, likelihood and impact	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	A threat, the vulnerability, likelihood of an event, impact	PI-02
Dominio de aplicación	Computers and Security	-

Criterio	**Detalle**	**Relevancia**
Identificador	6	-
Fuente	ScienceDirect	PB-01
Título	The future of risk assessment	PB-01
Autores	Zio E.	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2018	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Risk assessment, the safety and security assessment of cyber-physical systems.	PI-02
Dominio de aplicación	Reliability Engineering and System Safety	-

Criterio	**Detalle**	**Relevancia**
Identificador	7	-

Fuente	ScienceDirect	PB-01
Título	Incorporating attacker capabilities in risk estimation and mitigation	PB-01
Autores	Ben Othmane, Lotfi; Ranchal, Rohit; Fernando, Ruchith; Bhargava, Bharat; Bodden, Eric	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2015	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Sensitivity of the resources, the likelihood of the threats, and the severity of exploiting the vulnerabilities	PI-02
Dominio de aplicación	Computers and Security	-

Criterio	**Detalle**	**Relevancia**
Identificador	8	-
Fuente	ScienceDirect	PB-01
Título	SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations	PB-01
Autores	Upadhyay, Darshana; Sampalli, Srinivas	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2020	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	System/Asset, vulnerability, threat/attack, countermeasure, impact	PI-02
Dominio de aplicación	Computers and Security	-

Criterio	**Detalle**	**Relevancia**
Identificador	9	-
Fuente	ScienceDirect	PB-01
Título	Application of a fuzzy-logic based model for risk assessment in additive manufacturing R&D projects	PB-01
Autores	Moreno-Cabezali, Belen Maria; Fernandez-Crehuet, Jose Maria	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2020	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Mamdani-type FIS	PI-01
Objetivo del método	This research has developed a fuzzy logic-based model to estimate the relevance of each of the risks included in the survey and to identify which ones are the most critical.	PI-01

Factores de evaluación de riesgo en Tecnologías de Información	Relevance, probability, impact	PI-02
Dominio de aplicación	Computers and Industrial Engineering	-

Criterio	**Detalle**	**Relevancia**
Identificador	10	-
Fuente	ScienceDirect	PB-01
Título	Cybersecurity risk analysis model using fault tree analysis and fuzzy decision theory	PB-01
Autores	Henriques de Gusmão, Ana Paula; Mendonça Silva, Maisa; Poleto, Thiago; Camara e Silva, Lúcio; Cabral Seixas Costa, Ana Paula	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2018	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Triangular Membership Fuzzy Set	PI-01
Objetivo del método	To integrate of decision theory and fuzzy logic	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Financial losses and time for restoration	PI-02
Dominio de aplicación	Information Management	-

Criterio	**Detalle**	**Relevancia**
Identificador	11	-
Fuente	ScienceDirect	PB-01
Título	Novel interval type-2 fuzzy logic controller for improving risk assessment model of cyber security	PB-01
Autores	Jana D., Ghosh R.	PB-01
Publicación	Elsevier Ltd	PB-03
Años de publicación	2018	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Interval type-2 fuzzy logic controller (IT2FLC) - Mamdani fuzzy inference system	PI-01
Objetivo del método	To gain the total risk for the cybersecurity system which is combined with three sub models.	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Overall likelihood and impact	PI-02
Dominio de aplicación	Information Security and Applications	-

Criterio	**Detalle**	**Relevancia**
Identificador	12	-
Fuente	IEEE Xplore	PB-01
Título	Information security risks assessment in telecommunication network of the university	PB-01

Autores	Anikin, Igor V.	PB-01
Publicación	2016 Dynamics of Systems, Mechanisms and Machines, Dynamics 2016	PB-03
Años de publicación	2017	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Fuzzy membership function	PI-01
Objetivo del método	To evaluate risk factors for specific threats.	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Threat, impact, possibility	PI-02
Dominio de aplicación	Dynamics of Systems, Mechanisms and Machines	-

Criterio	**Detalle**	**Relevancia**
Identificador	13	-
Fuente	IEEE Xplore	PB-01
Título	Information Asset Classification and Labelling Model Using Fuzzy Approach for Effective Security Risk Assessment	PB-01
Autores	Alonge, Christianah Yetunde; Arogundade, Oluwasefunmi Tale; Adesemowo, Kayode; Ibrahalu, Friday Thomas; Adeniran, Olusola John; Mustapha, Abiodun Muyideen	PB-01
Publicación	2020 International Conference in Mathematics, Computer Engineering and Computer Science, ICMCECS 2020	PB-03
Años de publicación	2020	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Fuzzy cognitive maps and fuzzy inference system	PI-01
Objetivo del método	Employed fuzzy logic to classification of information	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Dependability, Threat, Vulnerability, Impact	PI-02
Dominio de aplicación	Mathematics, Computer Engineering and Computer Science	-

Criterio	**Detalle**	**Relevancia**
Identificador	14	-
Fuente	IEEE Xplore	PB-01
Título	Information security risk assessment and management method in computer networks	PB-01
Autores	Anikin, Igor V.	PB-01
Publicación	2015 International Siberian Conference on Control and Communications, SIBCON 2015 - Proceedings	PB-03
Años de publicación	2015	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Fuzzy system inference	PI-01
Objetivo del método	To evaluate quantitative risk values using fuzzy logic, expert judgments and analytic hierarchy process.	PI-01

Factores de evaluación de riesgo en Tecnologías de Información	Threat, Impact, Possibility	PI-02
Dominio de aplicación	Communications	-

Criterio	**Detalle**	**Relevancia**
Identificador	15	-
Fuente	IEEE Xplore	PB-01
Título	Artificial Intelligence Techniques for Information Security Risk Assessment	PB-01
Autores	Y. A. Basallo, V. E. Sentí, N. M. Sánchez	PB-01
Publicación	IEEE LATIN AMERICA TRANSACTIONS	PB-03
Años de publicación	2018	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Función trapezoidal	PI-01
Objetivo del método	Proponer una solución para mejorar la exactitud de los Riesgos de Seguridad de la Información	PI-01
Factores de evaluación de riesgo en Tecnologías de Información	Amenaza, probabilidad, vulnerabilidades	PI-02
Dominio de aplicación	Artificial Intelligence	-

Criterio	**Detalle**	**Relevancia**
Identificador	16	-
Fuente	IEEE Xplore	PB-01
Título	Using fuzzy logic for vulnerability assessment in telecommunication network	PB-01
Autores	Anikin, I. V.	PB-01
Publicación	2017 International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM 2017 - Proceedings	PB-03
Años de publicación	2017	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Fuzzy inference method	PI-01
Objetivo del método	To describe expert’s knowledge about risks	PI-01
Factores de riesgo en Tecnologías de Información	Vulnerability, risk level, attack, confidence degree	PI-02
Dominio de aplicación	Industrial Engineering, Applications and Manufacturing	-

Criterio	**Detalle**	**Relevancia**
Identificador	17	-
Fuente	IEEE Xplore	PB-01
Título	Countermeasure security risks management in the internet of things based on fuzzy logic inference	PB-01
Autores	Kotenko, Igor; Saenko, Igor; Ageev, Sergey	PB-01

Publicación	Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015	PB-03
Años de publicación	2015	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Fuzzy Inference - Mamdani	PI-01
Objetivo del método	Classification of security threats	PI-01
Factores de riesgo en Tecnologías de Información	Factors influencing new internet attacks: intrusion - traffic	PI-02
Dominio de aplicación	Computing and Communications	-

Criterio	**Detalle**	**Relevancia**
Identificador	18	-
Fuente	IEEE Xplore	PB-01
Título	FLUF: Fuzzy logic utility framework to support computer network defense decision making	PB-01
Autores	Newcomb, E. Allison; Hammell, Robert	PB-01
Publicación	2016 Annual Conference of the North American Fuzzy Information Processing Society (NAFIPS)	PB-03
Años de publicación	2016	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Fuzzy Associative Memory (FAM) - FLUF: Fuzzy logic utility framework	PI-01
Objetivo del método	To provide cyber defenders with decision support to improve their efficiency and ultimately increase mission assurance by placing focus on the most severe intrusion detection system alerts first.	PI-01
Factores de riesgo en Tecnologías de Información	Criticality and accessibility, impact, effect, alert priority	PI-02
Dominio de aplicación	Fuzzy Information	-

Criterio	**Detalle**	**Relevancia**
Identificador	19	-
Fuente	ACM	PB-01
Título	Information security risk management in computer networks based on fuzzy logic and cost/benefit ratio estimation	PB-01
Autores	Anikin, Igor; Emaletdinova, Lilia Yu	PB-01
Publicación	ACM International Conference Proceeding Series	PB-03
Años de publicación	2015	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Fuzzy logic and fuzzy inference scheme	PI-01
Objetivo del método	It makes the qualitative risk management process easier under considered challenges.	PI-01
Factores de riesgo en Tecnologías de Información	Impact, Exercising possibility, risk level, threat	PI-02
Dominio de aplicación	Artificial Intelligence	-

Criterio	Detalle	Relevancia
Identificador	20	-
Fuente	ACM	PB-01
Título	Risks facing smart city information security in Hangzhou	PB-01
Autores	Daniel, T. S.E.; Li, Rui; Zheng, Hanqi	PB-01
Publicación	ACM International Conference Proceeding Series	PB-03
Años de publicación	2019	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Fuzzy Delphi method	PI-01
Objetivo del método	Propose levels of indicators for risks	PI-01
Factores de riesgo en Tecnologías de Información	Probability, security, rating	PI-02
Dominio de aplicación	Artificial Intelligence	-

Criterio	Detalle	Relevancia
Identificador	21	-
Fuente	ACM	PB-01
Título	A Review of Research on Risk Analysis Methods for IT Systems Categories and Subject Descriptors	PB-01
Autores	Sulaman, Sardar Muhammad; Weyns, Kim; Höst, Martin	PB-01
Publicación	Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering	PB-03
Años de publicación	2013	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de riesgo en Tecnologías de Información	Risk analysis of IT systems requires different risk analysis techniques, or at least adaptations of traditional approaches.	PI-02
Dominio de aplicación	Software Engineering	-

Criterio	Detalle	Relevancia
Identificador	22	-
Fuente	ACM	PB-01
Título	Towards a security evaluation model based on security metrics	PB-01
Autores	Breier, Jakub; Hudec, Ladislav	PB-01
Publicación	ACM International Conference Proceeding Series	PB-03
Años de publicación	2012	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01

Factores de riesgo en Tecnologías de Información	Risk assessment according to ISO 27002: 2005 based on security risk metrics	PI-02
Dominio de aplicación	Computer Systems and Technologies	-

Criterio	**Detalle**	**Relevancia**
Identificador	23	-
Fuente	ACM	PB-01
Título	Improving risk assessment methodology: A statistical design of experiments approach	PB-01
Autores	Singh, Anand; Lilja, David	PB-01
Publicación	SIN'09 - Proceedings of the 2nd International Conference on Security of Information and Networks	PB-03
Años de publicación	2010	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de riesgo en Tecnologías de Información	Identify the subset of security controls that are critical to the enterprise	PI-02
Dominio de aplicación	Security of Information and Networks	-

Criterio	**Detalle**	**Relevancia**
Identificador	24	-
Fuente	SciELO	PB-01
Título	Lógica difusa y el riesgo financiero. Una propuesta de clasificación de riesgo financiero al sector cooperativo	PB-01
Autores	Díaz Córdova, Jaime Fabián; Coba Molina, Edisson; Navarrete, Paúl	PB-01
Publicación	Contaduría y Administración	PB-03
Años de publicación	2017	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Modelo en tiempo continuo fuzzy (MCF), Fuzzy pay-off method (FPOM), modelos en tiempo discreto fuzzy (MDF)	PI-01
Objetivo del método	Los indicadores de riesgo son los instrumentos indispensables para medir dicho desempeño a través de fórmulas y cálculos matemáticos	PI-01
Factores de riesgo en Tecnologías de Información	-	PI-02
Dominio de aplicación	Contaduría y Administración	-

Criterio	**Detalle**	**Relevancia**
Identificador	25	-
Fuente	SciELO	PB-01
Título	Definición de un modelo de medición de análisis de riesgos de la seguridad de la información aplicando lógica difusa y sistemas basados en el conocimiento	PB-01

Autores	Angarita, A A; Rios, C A Tabares J I	PB-01
Publicación	Entre Ciencia e Ingeniería	PB-03
Años de publicación	2015	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Método del centroide	PI-01
Objetivo del método	La teoría de la lógica difusa aplicada para realizar el análisis y evaluación de riesgos de seguridad en los activos de información, genera y entrega datos más exactos de nivel de riesgo	PI-01
Factores de riesgo en Tecnologías de Información	Probabilidad, impacto, nivel de riesgo	PI-02
Dominio de aplicación	Ciencia e Ingeniería	-

Criterio	**Detalle**	**Relevancia**
Identificador	26	-
Fuente	Google Scholar	PB-01
Título	La seguridad de la información: Aspecto crucial que toda empresa del siglo XXI debe gestionar	PB-01
Autores	MSc, Roxana Patricia Cedeño Villacís	PB-01
Publicación	Revista Científica Ciencia y Tecnología	PB-03
Años de publicación	2018	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de riesgo en Tecnologías de Información	Conceptualización de seguridad de la información, riesgo, amenaza y vulnerabilidad	PI-02
Dominio de aplicación	Ciencia y Tecnología	-

Criterio	**Detalle**	**Relevancia**
Identificador	27	-
Fuente	Google Scholar	PB-01
Título	Gestión de riesgos informáticos utilizando NIST SP-800 E ISO/IEC 27005 en la empresa International Forest Products Del Ecuador S.A.	PB-01
Autores	Oña Garcés Mercedes Beatriz	PB-01
Publicación	Universidad Regional Autónoma de los Andes	PB-03
Años de publicación	2019	PB-02
Tipo de publicación	Thesis	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de riesgo en Tecnologías de Información	Análisis y gestión de riesgos en los sistemas de información	PI-02
Dominio de aplicación	Sistemas Mercantiles	-

Criterio	Detalle	Relevancia
Identificador	28	-
Fuente	Google Scholar	PB-01
Título	Una propuesta de gestión de la seguridad de la información aplicado a una entidad pública colombiana	PB-01
Autores	Carvajal, D. L.; Cardona, A.; Valencia, F. J.	PB-01
Publicación	Entre ciencia e ingeniería	PB-03
Años de publicación	2019	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	-	PI-01
Objetivo del método	-	PI-01
Factores de riesgo en Tecnologías de Información	Incidente relacionado con la seguridad de la información en diferentes modalidades como phishing, ransomware, ataques de denegación de servicios, fraudes internos y externos, infección de malware y explotación de diferentes vulnerabilidades.	PI-02
Dominio de aplicación	Ciencia e Ingeniería	-

Criterio	Detalle	Relevancia
Identificador	29	-
Fuente	Google Scholar	PB-01
Título	Análisis de los mecanismos de seguridad lógicos y físicos en los centros de datos de entidades públicas ecuatorianas ante la ciberdelincuencia	PB-01
Autores	Rodrigo, Danny; Calderón, Jaramillo	PB-01
Publicación	Facultad de Ciencias Matemáticas y Físicas	PB-03
Años de publicación	2018	PB-02
Tipo de publicación	Thesis	PB-01
Tipo de método difuso	Mamdani - función de membresía trapezoidal	PI-01
Objetivo del método	Evaluar factores que detonan la acción de incidencia de posibles riesgos en centros de datos	PI-01
Factores de riesgo en Tecnologías de Información	Sistemas de detección de intrusos, Sistemas de prevención de intrusos, firewall, monitoreo de seguridad lógica, nivel de amenaza	PI-02
Dominio de aplicación	Ingeniería En Sistemas Computacionales	-

Criterio	Detalle	Relevancia
Identificador	30	-
Fuente	Google Scholar	PB-01
Título	Software de aplicación web basado en lógica difusa, para mejorar la evaluación de riesgos en tecnologías de información, en la Oficina de Tecnologías de Información y Comunicaciones de la Universidad Nacional del Santa	PB-01
Autores	Velásquez Ruiz, José Martín	PB-01

Publicación	Universidad Nacional del Santa	PB-03
Años de publicación	2016	PB-02
Tipo de publicación	Thesis	PB-01
Tipo de método difuso	Modelo Mamdani	PI-01
Objetivo del método	Mejorar la evaluación de riesgos en tecnologías de información	PI-01
Factores de riesgo en Tecnologías de Información	Vulnerabilidades y amenazas	PI-02
Dominio de aplicación	Ingeniería de Sistemas e Informática	-

Criterio	**Detalle**	**Relevancia**
Identificador	31	-
Fuente	Google Scholar	PB-01
Título	La lógica difusa para la evaluación del riesgo de seguridad informática a bases de batos	PB-01
Autores	Azán Basallo, Yasser; Martínez Sanchez, Natalia; Estrada Senti, Vivian	PB-01
Publicación	Revista Control, Cibernética y Automatización	PB-03
Años de publicación	2016	PB-02
Tipo de publicación	Journal Article	PB-01
Tipo de método difuso	Mamdani - Membresía Triangular	PI-01
Objetivo del método	Evaluación del impacto y del riesgo de seguridad informática a una base de datos	PI-01
Factores de riesgo en Tecnologías de Información	RM: Es el riesgo medio calculado en el componente anterior. RSI: Es el riesgo de seguridad de la información del servidor auditado.	PI-02
Dominio de aplicación	Ciencias Informáticas	-