UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERIA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

Metodologías para el análisis de riesgo de la seguridad de la información. Una revisión sistemática de la literatura

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

Por:

Lopez Rimari, Rosario Paula

Asesor:

Mg. Huanca López, Lizeth Geanina

Lima, 2020

DECLARACIÓN JURADA
DE AUTORIA DEL TRABAJO DE INVESTIGACIÓN

Mg. Lizeth Gianina Huanca López, 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: ***"Metodologías para el análisis de riesgo de la seguridad de la información. Una revisión sistemática de la literatura"*** constituye el trabajo que presenta la estudiante **Rosario Paula Lopez Rimari** para aspirar al Grado de Bachiller en Ingeniería de Sistemas, cuyo trabajo de investigación ha sido realizada 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, 22 de diciembre del año 2020

Asesor
Mg. Lizeth Gianina Huanca López

0025

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……10:40……horas, se reunieron los miembros del jurado en la Universidad Peruana Unión campus Lima, bajo la dirección del (de la) presidente(a): …… Dra. Erika Inés Acuña Salinas……, el (la) secretario(a): ….. Ing. Diana Lidia Sanchez Torpoco…… y los demás miembros:….. Mg. Fernando Manuel Asin Gomez …..y el (la) asesor(a): ….. Mg. Lizeth Geanina Huanca López…. con el propósito de administrar el acto académico de sustentación del trabajo de investigación titulado: "Metodologías para el análisis de riesgo de la seguridad de la información. Una revisión sistemática de la literatura" ……de los (las) egresados (as): a)…… Rosario Paula Lopez Rimari ……b)…… …… conducente a la obtención del grado académico de Bachiller 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): …… Rosario Paula Lopez Rimari ……

CALIFICACIÓN	ESCALAS			Mérito
	Vigesimal	Literal	Cualitativa	
Aprobado	17	B+	Con nominación de **Muy Bueno**	Sobresaliente

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 respectivas.

Presidente
Dra. Erika Inés Acuña Salinas

Secretario
Ing. Diana Lidia Sanchez Torpoco

Asesor
Mg. Lizeth Geanina Huanca López

Miembro

Miembro
Mg. Fernando Manuel Asin Gomez

Candidato/a (a)
Rosario Paula Lopez Rimari

Candidato/a (b)

ÍNDICE

Metodologías para el análisis de riesgo de la seguridad de la información. Una revisión sistemática de la literatura.

Methodologies for information security risk analysis A systematic review of the literature.

Rosario Paula Lopez Rimari [1]

[1] Ingeniería de sistemas, Universidad Peruana Unión, Perú
rosariolopez@upeu.edu.pe

Resumen. Cuando hablamos de riesgo nos referimos a la proximidad o posibilidad de un daño, peligro, etc. Asimismo, se puede identificar variados factores de riesgo que son manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo o tienden a aumentar la exposición, pueden ser interna o externa a la entidad. Actualmente cada organización utiliza diferentes metodologías para el análisis de los factores de riesgo de información. El objetivo principal de esta revisión sistemática es describir las metodologías para el análisis de riesgo de la seguridad de la información. Para la selección de metodologías se siguieron los pasos propuestos en el método de la Revisión Sistemática de la Literatura (RSL), en las diferentes fuentes bibliográficas virtuales consultadas. El resultado final es de 22 artículos que cumplen con los criterios establecidos para la investigación y que abordan información con relación de las metodologías relacionadas en el área de la seguridad de la información. Se concluye que, dentro de los factores existentes, el más relevante es el factor humano y dentro de las metodologías la más utilizada es Magerit.

Palabras claves: ISO 27005, metodologías de análisis riesgo, análisis de riesgos.

Abstract. When we speak of risk, we refer to the proximity or possibility of a damage, danger, etc. Likewise, it is possible to identify various risk factors that are measurable or observable manifestations or characteristics of a process that indicate the presence of risk or tend to increase exposure, they can be internal or external to the entity. Currently each organization uses different methodologies for the analysis of information risk factors. The main objective of this systematic review is to describe the methodologies for information security risk analysis. For the selection of methodologies, the steps proposed in the method of the Systematic Review of Literature (RSL) were followed, in the different virtual bibliographic sources consulted. The final result is 22 articles that meet the criteria established for the research and that address information in relation to related methodologies in the area of information security. It is concluded that, within the existing factors, the most relevant is the human factor and within the methodologies the most used is Magerit.

Keywords: ISO 27005, risk analysis methodologies, risk analysis

1. Introducción

En el mundo de las organizaciones los sistemas de información están cambiando la forma en que operan sus procesos, actividades, tareas, entre otros. *"Las nuevas tecnologías en las empresas se han vuelto esenciales, y cuando estas no optan por implementarlas en los diferentes procesos, las probabilidades de estancarse y perder posicionamiento aumentan considerablemente y más si se encuentran en pleno crecimiento."* [1]. Mediante la aplicación de la tecnología de la información en la mayoría de las esferas de actividad del estado, la economía y la sociedad, genera muchas oportunidades en cuanto a la automatización de los procesos de gestión y el aumento de la eficiencia y la calidad de los servicios realizados. [2] , por lo que se infiere que con la aplicación de tecnologías de información mejora los procesos tanto operativos como estratégicos y de soporte que una organización tiene y ayudan en la toma de decisiones estratégicas tanto de corto, mediano y largo plazo al proporcionarles información relevante, lo cual ayudará a ganar una ventaja competitiva frente a las demás entidades.

En la actualidad toda empresa se basa en la gestión de la información para tomar decisiones que permitan la continuidad del negocio, transformándose así en un activo importante para las organizaciones, siendo necesario protegerla ante cualquier evento que puede causar corrupción en los datos. Dada la importancia de la información, organizaciones internacionales de estandarización han elaborado normas de buenas prácticas para el resguardo y buen uso de la información y de los activos en general. [3]. En este sentido, las estadísticas indican que el 50% de los ciberataques ahora usan el aro de la isla para apuntar sus víctimas infiltrándose en las más pequeños empresas para acceder a las grandes organizaciones. [4], por lo que las fallas y defectos de seguridad de los sistemas abren puertas para que los hackers entren y accedan a información sensible. Los defectos de software tienen diversas ramificaciones de seguridad, tales como errores de implementación, desbordamientos de buffer, defectos de diseño, mal manejo de errores, etc. Con demasiada frecuencia, intrusos maliciosos pueden introducirse en los sistemas mediante la explotación de algunos de estos defectos de software. [5], por consiguiente, los desarrolladores necesitan considerar la confidencialidad de la información y la integridad de los datos para verificar la seguridad al principio del ciclo de vida del desarrollo en lugar de arreglar los agujeros de seguridad después de los ataques y las fugas de datos.

Las estadísticas del riesgo de los ataques informáticos masivos, que constituye un gran riesgo para la seguridad de la información empresarial, han tenido un crecimiento exponencial según el último informe realizado por la firma PwC a nivel mundial. Un ejemplo es España, que registra que el 67,7% de los directivos encuestados consideran "probable" o "muy probable" que sus empresas vayan a ser objeto del algún tipo de ciberataque en los próximos meses.[6]

El objetivo principal de esta revisión sistemática es describir las metodologías para el análisis de riesgo de la seguridad de la información .Este artículo está organizado de la siguiente manera: En el segundo apartado se explica la revisión de la literatura, contemplando los siguientes tópicos: Seguridad de la información, riesgos; el tercer apartado comprende el método de la revisión sistemática de la literatura, explicando la necesidad, las preguntas, los criterios de inclusión y exclusión y los criterios de calidad; en el cuarto apartado se describe los resultados de la revisión y finalmente en el quinto apartado se describe las conclusiones.

2. Revisión de la literatura

En esta sección se presentan algunos conceptos del contexto sobre el cual se realiza el estudio y el objeto de análisis.

2.1. Seguridad

Según el Modelo de la seguridad de los derechos se concibe a la seguridad como: *"Una necesidad y un derecho de carácter secundario, respecto a todas las otras necesidades básicas o reales, que pueden definirse como primarias (alimento, vestimenta y abrigo)"*[7]. Se entiende la seguridad como un derecho, que es menester para el ser humano y una función del sistema jurídico. [7]. En relevancia en los atentados contra la propiedad: robo y hurto, está estrechamente conectado con la percepción social del miedo. Por otro lado, esta política comprende un área extremadamente más compleja que la limitada prospectiva de la "lucha" contra la criminalidad. [8] . Por consiguiente, también se puede definir como una cualidad o estado de seguro. Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo. Se dice también de todos aquellos objetos, dispositivos, medidas, entre otros que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa.[9]

2.2. Seguridad de la información

La seguridad de la información tiene la finalidad de resguardar y conservar el activo más importante de toda la organización bajo los tres pilares de la seguridad de la información: confidencialidad, disponibilidad e integridad. Debido a esto está relacionado con las medidas preventivas aplicables. La información se puede evidenciar en distintos medios tanto electrónicos, como físicos y formatos. Por ello, las entidades deben adoptar y adaptar metodologías para proteger los registros y archivos, para mantener en funcionamiento una infraestructura tecnológica adecuada que sirva y salvaguarde la información. [10]. ISO Tools Excellence [11], define a la seguridad de la información como: "Una enseñanza que está a cargo de la

implementación técnica de la protección de la información, el despliegue de las tecnologías que establecen de manera que se aseguran las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo, es la disciplina que nos habla de los riesgos, de las amenazas, de los estudios de contextos, de las buenas prácticas, recomendaciones y los esquemas normativos, que demandan niveles de aseguramiento de procesos y de tecnología para incrementar el nivel de confianza en la construcción, uso, almacenaje, transmisión, recuperación y disposición final de la información". En general, se puede afirmar que el tema de Seguridad de la Información no es sólo un tema eminentemente técnico, sino que también involucra procesos del negocio y actividades de gobierno corporativo, que aseguren una continua gestión de los riesgos y aseguramiento de los niveles de seguridad requeridos por la organización. [10]

Según Taherdoost, [12] la seguridad de la información es la protección de información de diferentes amenazas para posibilitar la continuidad de los procesos organizacionales, disminuir el riesgo y subir el retorno de oportunidades de inversión y de negocios. Los pilares de la seguridad de la información son:

1. **Confidencialidad:** Es garantizar la confidencialidad de la información o los datos y asegurar que sólo las autoridades puedan acceder a la información.[11]

2. **Integridad:** Significa que los datos no pueden ser alterados sin la autorización de las autoridades competentes, salvaguardar la integridad de la información y protegerse contra los daños u otras amenazas que puedan causar cambios en la información o los datos originales.[11]

3. **Disponibilidad:** Aspectos que garantizan que los datos estarán disponibles cuando se necesiten y aseguran que el usuario pueda acceder a la información sin interrupciones.[11]

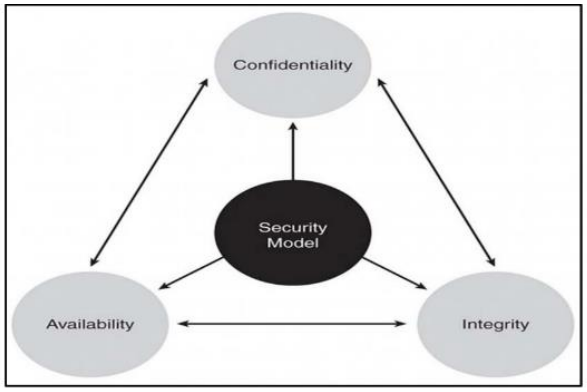


Figura 1: IT security model CIA

2.3. Gestión de riesgos

La gestión de riesgos trata en la elaboración de las acciones de seguridad para satisfacer las necesidades encontradas durante la examinación. Comprende las actividades: (Elegir una estrategia para mitigar el impacto y riesgo, determinar las salvaguardas oportunas para el objetivo anterior, determinar la calidad necesaria para dichas salvaguardas, diseñar un plan de seguridad, plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables, llevar a cabo el plan de seguridad. [13] En esta medida, la identificación, análisis, evaluación y tratamiento, son aspectos claves para gestionar el riesgo, eso sí, teniendo muy presente una serie de principios para que el proceso sea eficaz.[14]

2.3.1.**Activo**

En términos simples se define un activo como todo aquello que una entidad posee para realizar el procesamiento de la información, entre estos están (software, hardware, recurso humano entre otros). Se identifican los activos de información de mayor relevancia relacionados a cada Sistema de Procesamiento de la Información en su respectivo proceso, con sus responsables y su locación, para luego desarrollar un inventario con referida información. Este activo es considerado para las actividades de la empresa y debe ser protegida de acuerdo con los principios de confidencialidad, integridad y disponibilidad. Cuando se procede a la identificación del "activo" en el campo de la seguridad de la información, referencia a todo tipo de documentos, repositorios, CD´S, USB, entre otros. De modo que en estos activos se encuentran almacenados datos que son etiquetados al interior de una organización como fundamentales, para el cumplimiento de su respectiva actividad económica [14]. Esto se relaciona con este artículo porque el activo de información juega un papel relevante en las organizaciones por ello se debe optar por las medidas de seguridad correspondientes para salvaguardar todo lo confidencial y para ello se debe analizar cualquier fuga de información.

2.3.2. **Riesgo**

En relación a la definición propuesta por el diccionario de la Real Academia Española, la palabra riesgo representa una contingencia o proximidad de un daño. [15] Cabe resaltar que, el término riesgo suele ser utilizado cuando se desea hablar de una circunstancia de peligro, a pesar de ello, se percibe una marcada diferencia entre estas dos palabras, ya que el peligro es una posibilidad de accidente y riesgo es la probabilidad de un daño. [14] . Asimismo la definición de la ISO refiere que el riesgo es "la probabilidad de que una amenaza determinada se materialice explotando las vulnerabilidades de un activo o grupo de activos y por lo tanto causar daño o pérdidas a la organización" [16]. De los dos conceptos anteriores se deduce que un riesgo es la posibilidad de una amenaza a la perdida que puede explotar ante cualquier

vulnerabilidad de un activo de información, también los riesgos o amenazas puede surgir de factores externos o internos.

2.3.3. **Riesgos Informáticos**

Los riesgos informáticos son problemas potenciales que vulneran a los sistemas de información o a los equipos de informática. Si no se tienen las medidas adecuadas para proteger los datos y la información, dichos riesgos se pueden materializar a través de las vulnerabilidades y amenazas que están presentes en la gestión de activos de una determinada organización. Por ende, los riesgos se clasifican en: Riesgos de integridad, Riesgos de relación, Riesgos de acceso, Riesgos de utilidad, Riesgo de infraestructura. [10]. Todos los programas informáticos presentan una serie de vulnerabilidades que se constituyen en debilidades del software que inesperadamente permiten operaciones peligrosas y/o maliciosas. Si la vulnerabilidad se encuentra en un servicio de red, representa graves amenazas de seguridad porque un ciberataque puede explotarlo para ganar acceso no autorizado al sistema. Por ello, el descubrimiento y la inmediata reparación de las vulnerabilidades de la red son cuestiones críticas para la seguridad de la red. En el dinámico entorno actual de la tecnología de la información, es práctica común que una organización de prioridad a la neutralización de las vulnerabilidades descubiertas de acuerdo con sus niveles de riesgo. [17] .Cuanto más compleja es la infraestructura de la información, más riesgo surge en el campo de la ciberseguridad.[18]

2.4. Análisis de riesgos

El análisis de riesgo es un elemento indispensable para determinar las medidas de seguridad ante un activo de información o sistema, ya que identifica los riesgos y determina probabilidades de ocurrencia y el impacto potencial que supone su propia destrucción o la pérdida de la información o mayor aun una afectación en cuanto a la disponibilidad, confidencialidad, integridad y no repudio de la información, esto en concordancia con lo planteado por Royal [19], quien menciona que: *"No todas las exposiciones necesitan ser o deberían ser controladas, el control total no es un costo eficaz y generalmente es muy ineficiente, sin embargo, si el diseñador no tiene idea de que la exposición presenta el mayor riesgo en términos de frecuencia de ocurrencia y costo, no tiene otra alternativa que controlar cada exposición."* Por otro lado, se dice que cuando se identifican los riesgos de seguridad la empresa lo que hace, es evaluar el proceso para reducir a un nivel aceptable e implementar mecanismos apropiados para que el nivel de riesgos se encuentre en un nivel admisible, por lo que se debe establecer criterios de aceptación del riesgo e identificar los controles para mitigar y por último evaluar el costo beneficio de las contramedidas. [20]

En este artículo se hace muy presente el análisis de riesgo ya que por los conceptos anteriores se infiere que está relacionado con el estudio cuidadoso de uno de los activos más relevantes que es la información, con el objetivo de establecer, identificar y estimar las causas de posibles sucesos que pueden afectar el bienestar de la organización o entidad ya sea pública o privada.

Umaya [21], explica que el análisis de riesgo es el proceso cuantitativo o cualitativo que permite evaluar los riesgos. El primer paso del análisis es identificar los activos a proteger o evaluar. La evaluación de riesgos involucra comparar el nivel de riesgo detectado durante el proceso de análisis con criterios de riesgo establecidos previamente. La función de la evaluación consiste en ayudar a alcanzar un nivel razonable de consenso en torno a los objetivos en cuestión, y asegurar un nivel mínimo que permita desarrollar indicadores operacionales a partir de los cuales medir y evaluar. Los resultados obtenidos del análisis, van a permitir aplicar alguno de los métodos para el tratamiento de los riesgos, que involucra identificar el conjunto de opciones que existen para tratar los riesgos, evaluarlas, preparar planes para este tratamiento y ejecutarlos. Dentro del tema de análisis de riesgo se ven reflejados cinco elementos muy importantes dentro del concepto estos son los siguientes: probabilidad, amenazas, vulnerabilidades, activos e impactos.

2.4.1. **Objetivos del análisis de riesgo** Mujica[19], expresa que el proceso de análisis de riesgo deber ser efectuado en cualquier momento y cumplir con los siguientes objetivos: Identificar, evaluar, y manejar los riesgos de seguridad; debe estimar la exposición de un recurso a una amenaza específica; determinar cuál combinación de medidas de seguridad proporcionar ‘a un nivel de seguridad razonable a un costo aceptable; tomar mejores decisiones en seguridad informática y enfocar recursos y esfuerzos en la protección de los activos de información.

2.4.2. **Beneficios del análisis de riesgo** El realizar un análisis de riesgos en las organizaciones trae consigo una serie de beneficios que se ven reflejados en el costo-beneficio de la misma, ´estos varían de organización en organización y van de acuerdo a las políticas de cada una, pero en líneas generales se resumen de la siguiente manera:

- Asegurar la continuidad operacional de la empresa.
- Saber manejar las amenazas y riesgos críticos.
- Mantener una estrategia de protección y de reducción de riesgos
- Justificar una mejora continua de la seguridad informática.
- Costos de seguridad justificados.
- Permitir que la seguridad se convierta en parte de la cultura de la organización.
- Apoyar la comunicación y facilitar la toma de decisiones, certeza económica/financiera.

2.4.3. **Fases del análisis de riesgo. -** El proceso de análisis de riesgos según lo expresa Mujica [19], debe cumplir con tres etapas:

Fase 1: Construir perfiles de amenazas basados en activos: activos críticos, requerimientos de seguridad para los activos críticos, amenazas a los activos críticos, prácticas de seguridad actuales, vulnerabilidades actuales de la organización.

Fase 2: Identificar vulnerabilidades de infraestructura: componentes clave, vulnerabilidades actuales de la tecnología.

Fase 3: Desarrollar planes y estrategias de seguridad: riesgos de los activos críticos, medidas de riesgo, estrategias de protección, planes de mitigación de riesgos.

2.5. Metodologías de análisis de riesgo

Las metodologías de análisis de riesgos tienen como función principal la identificación de los controles y mecanismos en un plan de salvaguardas, se pueden encontrar dos clases, las cualitativas y las cuantitativas, la metodología es flexible en el momento de su implementación, esto quiere decir que no se requiere de su implementación total para que esta brinde resultados satisfactorios, se pude hacer una adopción a la norma de forma parcial.[22]

2.5.1. **MAGERIT**

Umaya [21], menciona que es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.

- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

- Que, una vez concluido el análisis de riesgos, los resultados obtenidos se pongan en práctica para evitar incidentes dentro del entorno. [23]

2.5.1.1. **Objetivos de MAGERIT:** Concienciar a los responsables de todas las organizaciones de la existencia de riesgos, dando a conocer la necesidad de gestionar los mismos. Cuenca [23]

- Ofrecer un método sistemático para analizar los riesgos (Dirección General de Modernización Administrativa, 2012).
- Ayudar a descubrir y planificar el tratamiento oportuno en caso de que los riesgos ataquen los activos de información.
- Preparar a cada organización para procesos de evaluación, auditoría o certificación ISO 27001 (Dirección General de Modernización Administrativa, 2012).

2.5.2. **CRAMM**

Esta metodología fue desarrollada en el Reino Unido por la Agencia Central de Cómputo y Telecomunicaciones. Está destinado a proteger la confidencialidad, integridad y disponibilidad de un sistema de información y sus activos. CRAMM puede definirse como una metodología para el análisis y gestión de riesgos, orientado a proteger la confidencialidad, la integridad y disponibilidad de un sistema y sus activos. Puede ser aplicable en todo tipo de sistemas y redes de información en la etapa de estudio de factibilidad, donde el alto nivel del riesgo puede ser requerido para identificar los requisitos de seguridad general, la contingencia y los costos asociados de las distintas opciones. Durante el análisis detallado del negocio y de entornos técnicos donde los problemas de seguridad o contingencia asociados con la opción tomada pueden ser investigados o refinados. Antes de la ejecución, para garantizar que todos los requerimientos físicos, el personal, técnicas y contramedidas de seguridad se han identificado e implementado. [23]

2.5.2.1. **Objetivo:**

Identificar las amenazas, vulnerabilidades y evaluar los niveles de riesgos, dando orientación a los responsables de la seguridad para evitar los riesgos individuales, reduciéndolos a un nivel aceptable en las siguientes etapas:

1. Identificación y valoración de activos.
2. Evaluación de amenazas y vulnerabilidad.
3. Selección y recomendación de contramedidas.

2.5.3. **OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation)**

Es una metodología desarrollada por el CERT/CC2 que tiene por objeto facilitar la evaluación de riesgos en una organización. En esta parte del artículo, presentaremos una visión general de OCTAVE y mostraremos de manera global el modo cómo se desarrolla.

OCTAVE se centra en el estudio de riesgos organizacionales [24] y se focaliza principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto como los elementos de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas, entre otros). De esta forma, OCTAVE estudia la infraestructura de información y, más importante aún, la manera como dicha infraestructura se usa en el día a día. En OCTAVE se considera que, con el fin de que una organización pueda cumplir su misión, los empleados a todo nivel necesitan entender qué activos relacionados con la información son importantes y cómo deben protegerlos; para ello, es fundamental que en la evaluación estén directamente involucradas personas de diferente nivel de la organización. OCTAVE es un estudio auto dirigido, desarrollado por un equipo interdisciplinario llamado el equipo de análisis, el cual se compone de personas de las áreas de negocio y del área de TI. [25]

OCTAVE se elabora mediante una serie de talleres en los que el equipo de análisis y el personal clave de los diferentes niveles de la organización adelantan el levantamiento y análisis de la información. Este pro- ceso se divide en tres fases:

- Fase 1- Construir perfiles de amenazas basados en los activos.
- Fase 2- Identificar vulnerabilidades en la infraestructura.
- Fase 3- Desarrollar estrategias y planes de seguridad.

2.5.4. **MEHARI (Method for Harmonized Analysis of Risk):**

Es definida por la organización francesa especializada en la seguridad de los sistemas de información como una metodología que proporciona un conjunto de herramientas que permiten hacer un análisis de riesgos cualitativo y cuantitativo, cuando sea necesario para tener una adecuada gestión de seguridad [24]. De lo anterior, se deduce que está diseñada para acompañar los procesos de análisis de riesgos empresariales tanto actuales como futuros. En la

metodología MEHARI se hace un análisis de la seguridad basado en tres criterios básicos: confidencialidad, integridad y disponibilidad. Está comprendida por tres fases a partir de las cuales las empresas pueden tomar medidas oportunas para asegurar la continuidad del negocio.[26]

2.5.4.1. **Fases:**

- **Análisis o evaluación de riesgos:** Una situación de riesgo se puede caracterizar por diferentes factores, como, factores estructurales (u organizacionales), los cuales no dependen de las medidas de seguridad, sino de la actividad principal de la organización, su entorno y su contexto y factores de la reducción de riesgo, que son función directa de las medidas de seguridad implementadas. Para ello, integra herramientas (como criterios de evaluación, fórmulas, etc.) y bases de datos de conocimiento (en particular para el diagnóstico de las medidas de seguridad), como complemento esencial al marco de análisis de riesgos. Es necesario realizar un enfoque estructurado que permita identificar todas las situaciones potenciales de riesgo, con el fin de analizar las más críticas y poder identificar las acciones para reducir el riesgo a niveles aceptables. [27]

- **Evaluaciones de seguridad:** MEHARI integra cuestionarios de controles de seguridad, lo que permite evaluar el nivel de calidad de los mecanismos y soluciones encaminadas a la reducción del riesgo. Los controles o medidas de seguridad se agrupan en servicios y en dominios de seguridad. Para realizar esta evaluación es necesario seguir los siguientes pasos: *Revisión de vulnerabilidades o evaluación de los servicios de seguridad:* [28] MEHARI proporciona un modelo de riesgos estructurado que considera los factores de reducción del riesgo en forma de servicios de seguridad. El resultado de la evaluación de la vulnerabilidad tendrá el fin de garantizar que los servicios de seguridad cumplen realmente su cometido. La evaluación se basa en una base de datos experta de conocimientos proporcionada por MEHARI para evaluar el nivel de calidad de las medidas de seguridad. *Planes de seguridad basados en la revisión de vulnerabilidades:* se realizará la confección de planes de seguridad como resultado directo de la evaluación del estado de los servicios de seguridad. El proceso de gestión de la seguridad se enfoca en ejecutar una evaluación y decidir mejorar todos aquellos servicios que no tienen un suficiente nivel de calidad. *Apoyo en las BBDD en la creación de un marco de referencia de seguridad:* las bases de datos de conocimiento de MEHARI se pueden utilizar directamente para crear un marco de referencia de seguridad que contendrá y describirá el conjunto de reglas e instrucciones de seguridad que debe seguir la organización. Los cuestionarios de evaluación de esta metodología son una buena base de trabajo para los responsables de seguridad para

decidir lo que debe ser aplicado en la organización. La creación de un conjunto de reglas, a través de un marco de referencia de seguridad, se enfrenta a menudo a dificultades en la implementación local, por lo que se deben gestionar exenciones y excepciones. *Dominios cubiertos por el módulo de evaluación de vulnerabilidades:* desde un punto de vista de análisis de riesgo, en base a la identificación de todas las situaciones de riesgo y con el deseo de cubrir todos aquellos riesgos inaceptables, MEHARI no se limita simplemente al dominio IT. El módulo de evaluación cubre, además de los sistemas de información, todo el conjunto de la organización, como la protección del sitio en general, el entorno de trabajo y los aspectos legales y regulatorios.[27]

- **Análisis de amenazas:** Sea cual sea la orientación de la política de seguridad, hay un principio en el que coinciden todos los responsables: debe existir un equilibrio entre las inversiones de seguridad por un lado y la importancia de los principales retos empresariales por el otro. Esto significa que la comprensión de las amenazas del negocio es fundamental, y que el análisis del contexto de seguridad merece un nivel prioritario y un método estricto y riguroso de evaluación. [27]

2.5.5. **ISO 27005**

Es el estándar internacional que se encarga de la gestión de riesgos de seguridad de información. La norma es denominada formalmente como Tecnología de la información – Técnicas de seguridad – Gestión del riesgo en la seguridad de la información [29]. Asimismo emplea las directrices para la gestión de riesgos de seguridad de la información en una empresa, sin proporcionar metodologías concretas para tal fin, de modo que busca apoyar particularmente los requerimientos del sistema de gestión de seguridad de la información definidos en ISO 27001.[28]

También es aplicable a todo tipo de organizaciones que trabajen en la meta de la identificación, análisis y tratamiento de riesgos que puedan complicar la seguridad de la información de la entidad. Cada metodología para ser implementada, dependerá de una serie de factores, como el alcance real del Sistema de Gestión de Seguridad de la Información (SGSI), o el sector comercial de la propia industria. [28]

2.5.5.1. **Objetivo de la norma ISO 27005:**

El objetivo de la norma ISO 27005 es proporcionar directrices para la gestión de riesgos de seguridad de la información. Esta norma está en relación con las definiciones generales formuladas en la norma ISO

27001 y está elaborado para colaborar a la implementación y satisfacción de la seguridad de la información en función de un enfoque de gestión de riesgos. La norma ISO 27005 no aconseja métodos específicos de análisis de riesgos, aunque es cierto que especifica un proceso estructurado, sistemático y riguroso desde el análisis de riesgos hasta la creación del plan de tratamiento de riesgos.[28]

3. Método de la revisión sistemática de la literatura

Las revisiones sistemáticas (RS) nos permiten estar al día en diversos temas de interés sin invertir demasiado tiempo; pero, no siempre este tipo de estudio se asocia a un nivel de evidencia, garantiza validez o veracidad, calidad metodológica, y confiabilidad o reproducibilidad de resultados. [30] Para lo cual, se requiere de una adecuada elaboración de la pregunta de investigación y de la revisión de la literatura. La Revisión Sistemática de la Literatura surge de la necesidad de los investigadores de recolectar y sintetizar toda la información existente sobre algún tema de manera exhaustiva e imparcial. De esta manera se puede obtener una conclusión más general sobre el tema a investigar y tener un sustento teórico para otras actividades de investigación. [31] El método de la revisión sistemática de la literatura tiene como objetivo de resumir la información existente respecto a un tema de investigación en particular.

3.1. Necesidad de la revisión sistemática

Esta revisión sistemática de la literatura que se presenta en este estudio surge a partir de la necesidad de querer describir las metodologías para el análisis de riesgo de la seguridad de la información. Esta necesidad se fundamenta en tener un sustento teórico que avale si es viable el realizar la implementación de un sistema de seguridad de información en el sector público o privado.

Tabla 1: Elaboración del objetivo de la investigación

Campo/criterios	Valor
Objeto de estudio	Metodologías para el análisis de riesgo de la información
Propósito	Describir
Foco	Metodologías, Factores
Involucrados	Riesgos de la seguridad de la información, seguridad de la información
Factores de contexto	Ninguno para este caso

3.2. Preguntas para la revisión sistemática

Para la definición y estructuración de las preguntas de investigación se tomó como referencia la sección anterior. A continuación, se muestra Tabla 2 con las preguntas de investigación y en la Tabla 3 las preguntas bibliométricas.

Tabla 2:Preguntas de investigación y motivación

IDs	Pregunta	Motivación
PI-01	¿Qué metodologías para el análisis de riesgo de la seguridad de la información existen en los estudios obtenidos?	Describir metodologías para el análisis de riesgo de la seguridad de la información.
PI-02	¿Cuáles son las fases de las principales metodologías existentes sobre el análisis de riesgo de información, en los estudios obtenidos?	Identificar las fases de las principales metodologías en el análisis de riesgo de la seguridad de la información, en los estudios obtenidos.
PI-03	¿Qué categorías de activos de información consideran las principales metodologías de análisis de riesgo para la seguridad de la información?	Identificar categorías de activos de información que están presentes en el análisis de riesgo de la seguridad de información en los estudios obtenidos.

Tabla 3: Preguntas de bibliometría

IDs	Pregunta	Motivación
PB-01	¿Cuál es la cantidad de publicaciones por tipo de artículo sobre el análisis de riesgo de la seguridad de la información?	Determinar la cantidad de estudios publicados por tipo de articulo para identificar la concentración de los mismos.
PB-02	¿Cómo ha evolucionado en el tiempo la frecuencia de las publicaciones sobre el análisis de	Identificar la frecuencia de las publicaciones sobre este tema.

	riesgo de la seguridad de la información?	
PB-03	¿Cuáles son las publicaciones en las que se han encontrado estudios relacionados al análisis de riesgo de la seguridad de la información?	Identificar en qué bibliotecas virtuales se concentra mayor cantidad de publicaciones sobre este tema.

3.3. Definición de las cadenas de búsqueda

La estrategia seleccionada para la elaboración de la cadena de búsqueda en esta investigación fue PICO[31], permite mejorar la especificidad y claridad conceptual del tema o problema a estudiar.

A continuación, se muestran las palabras clave con cada elemento de PICO con respecto al problema establecido.

Población:

Término principal: Metodologías
Términos alternos: Modelos, métodos
Justificante: Describir qué metodologías de riesgo existen para el análisis de riesgo de seguridad de información

Intervención:

Término principal: Seguridad de la Información
Término alterno: Riesgos de la seguridad de la información
Justificante: Se selecciona el término por ser el elemento sobre el cual se realizará el análisis comparativo y se obtienen dichos términos alternos por ser aquellos los tipos de objetos.

Resultado:

Entidad: Propuestas y experiencia para el análisis de riesgos en la Seguridad de la información
Término principal: Propuestas
Términos alternos: Implementación, experiencias, análisis
Justificante: Se seleccionan dichos términos para identificar las propuestas y experiencias de análisis de riesgos de seguridad de información.

Idioma. El idioma elegido para establecer la cadena de búsqueda ha sido el inglés puesto que es usado para la elaboración más frecuentemente seleccionadas de acuerdo a su importancia en el aspecto científico. Siguiendo por lo propuesto por PICO, se obtiene como resultado la cadena de búsqueda a partir del uso de operadores

booleanos (and y or) entre los elementos definidos previamente: (Población) AND (Intervención) AND (Comparación) AND (Resultado) AND (Contexto).

Tabla 4: Términos en inglés y conectores lógicos a ser usados en la búsqueda

Concepto	Términos
Población	Methodology* model
Intervención	"risk analysis" or "information security"
Comparación	No aplica
Resultado	information security analysis proposals

3.4. Criterios de inclusión y exclusión

Siguiendo los lineamiento elaborados por Kitchenham[31], luego de realizar la cadena de búsqueda en las librerías indexadas, los resultados deberán ser sometidos a evaluación con el objetivo de determinar los estudios primarios que responden directamente las preguntas de investigación planteadas. Se tomó en consideración los siguientes criterios para la evaluación de los estudios:

Tabla 5: Criterios de inclusión

Criterios de Inclusión	
C.I.1	Se consideran todos aquellos artículos provenientes de librerías digitales indexadas. (IEE Xplore, Science Direct, Springer Link, Google Scholar)
C.I.2	Se consideran los artículos que provienen del área de Seguridad de la Información.
C.I.3	Se aceptarán artículos que contengan estudios, análisis o metodologías de riesgos de la seguridad de la información.
C.I.4	Se considerarán todos los artículos que se encuentren dentro del rango 2014-2020
C.I.5	Se aceptarán artículos provenientes de revistas científicas y conferencias.
C.I.6	Se incluirá solo los documentos de tipo: artículos de revisión y artículos de investigación.

Criterios de Exclusión	
C.E.1	Serán excluidos los artículos duplicados.
C.E.2	Serán rechazados los artículos diferentes al idioma inglés y español.
C.E.3	Serán rechazados los artículos de contenido similar, quedándose solo los que tengan el contenido más completo.
C.E.4	Serán excluidos los estudios secundarios, estudios terciarios y resúmenes.
C.E.5	Serán excluidos los artículos cuyo título no tenga relación con el objeto de estudio

Tabla 6: Criterios de exclusión

Temporalidad. Se consideró los estudios desarrollados en los últimos 6 años dado que se requiere describir las metodologías de análisis de riesgo de seguridad de información con un enfoque más actual.

Fuente de Datos. Las librerías digitales indexadas consideradas por su relevancia científica para la selección de artículos fueron:

- ScienceDirect (http://www.sciencedirect.com)
- IEEE Xplore Digital Library(https://ieeexplore.ieee.org/Xplore/home.jsp)
- Springer Link (https://link.springer.com/)
- Google Scholar (https://scholar.google.com)

Procedimientos para la selección de estudios:

Se considera el siguiente procedimiento para la selección de artículos en la revisión sistemática:

- **Paso 1:** Se procedió a ejecutar la cadena de búsqueda PICO, en los buscadores de las bases de datos indexadas seleccionadas

previamente empleando los criterios de inclusión y exclusión de acuerdo a la Tabla 5 y 6

- **Paso 2:** Se revisaron los títulos de los artículos resultantes de la ejecución del Paso 1 excluyendo solamente los que fueran totalmente no relevantes con el objeto de estudio de la revisión.
- **Paso 3:** Se revisaron los resúmenes de los artículos previamente seleccionados en el Paso 2 para proceder con la exclusión de todos los estudios según los criterios definidos en la Tabla 6. Solamente se excluyeron los artículos que fueron totalmente relacionados con el objeto de estudio.
- **Paso 4:** Se procedió con la realización de una revisión de una revisión preliminar del contenido de los artículos seleccionados luego del Paso 3, enfocando la revisión a las secciones de introducción y conclusiones; para luego aplicar los criterios de selección según la Tabla 5 y 6.

Tabla 7: Procedimiento y criterios de exclusión e inclusión

Procedimiento	Criterio de selección
Paso 1	C.I.4 - C.E.2 - C.I.6 - C.I.1
Paso 2	C.E.5 - C.E.1 - C.I.5 - C.I.2
Paso 3	C.E.4 - C.E.3
Paso 4	C.I.3

3.5. Definición del Protocolo de Investigación

Esquema de evaluación de calidad de estudios:
Cada criterio está acompañado de un puntaje basado en la escala de, el cual consiste en los siguientes puntajes: Si cumple (S) = 1, Cumple parcialmente (P) = 0.5 y No cumple (N) = 0. Los resultados obtenidos serán presentados según el esquema de la Tabla 8

Tabla 8: Criterios de evaluación de calidad

N°	Criterio de evaluación
1	**¿El método seleccionado para llevar a cabo el estudio ha sido documentado apropiadamente?** S: El método seleccionado ha sido documentado apropiadamente. P: El método seleccionado ha sido documentado parcialmente. N: No se ha documentado el método seleccionado.
2	**¿Se han documentado las limitaciones del estudio de manera clara?** S: Las limitaciones se han documentado claramente. P: Las limitaciones se han documentado parcialmente. N: No se han documentado limitaciones.
3	**¿Los aportes del estudio comunidades científicas académicas o para la industria ha sido descritos?** S: Los aportes del estudio han sido mencionados claramente. P: Los aportes del estudio han sido mencionados claramente. N: No se han mencionado aportes.
4	**¿Los resultados han contribuido a responder las preguntas de investigación planteadas?** S: Los resultados han contribuido a responder todas las preguntas de investigación. P: Los resultados han contribuido a responder algunas preguntas de investigación. N: Los resultados no han contribuido a responder las preguntas de investigación.

4. Resultados

4.1. Resultados de la búsqueda

Las cadenas de búsqueda de acuerdo a los pasos definidos en la sección anterior. En la tabla siguiente se pueden visualizar los resultados.

Tabla 9: Resultados de búsqueda

CADENA DE BÚSQUEDA		
Base de Datos	**Fecha**	**Total**
SCIENCE DIRECT	**Jun-20**	**221**
("Methodology" OR "methodology for") AND ("risk analysis OR "information security") AND ("Octave" OR "magerit" OR "mehari" OR "cramm")		
IEEE XPLORE	**Jun-20**	**619**
"methodology for" AND ("risk analysis" OR "information security") OR "information security risk management"		
Google Scholar	**Jun-20**	**217**
("methodology for information") AND ("risk analysis OR "information security") AND ("Octave" OR "magerit" OR "mehari" OR "cramm")		
Springer Link	**Jun-20**	**212**
("Methodology" OR "methodology for") AND ("information risk analysis" OR "information security risk management")		

4.2. Selección de estudios primarios

Los artículos encontrados en las bases de datos fueron seleccionados siguiendo los lineamientos planteados en la sección IV (Procedimientos y criterios de inclusión).

Tabla 10: Resultados del proceso de selección de estudios

Base de datos	Artículos descubiertos	Paso 1	Paso 2	Paso 3	Paso 4
Google Scholar	217	95	55	23	6
IEEE Xplore	619	151	44	35	5
Science Direct	221	73	55	30	6
Springer Link	212	109	51	38	5
	1269	428	205	126	22

4.3. Evaluar calidad de los estudios

Sobre el total de 22 artículos resultantes se aplicó la serie de requisitos de comprobación definidos en la sección III. En la Tabla 11 se muestran los resultados de la evaluación de la calidad de los artículos encontrados, donde se puede observar que solamente el 10% de los artículos obtuvieron una puntuación menor al 50% del puntaje total, lo cual nos lleva a determinar como un buen indicador de la calidad de los estudios elegidos para la RSL.

Tabla 11: Criterios de calidad

ID	C1	C2	C3	C4	C5	Total
1	1	1	0	1	0.5	3.5
2	0.5	1	0.5	1	1	4
3	1	0	0	1	1	3
4	1	0	0	1	0.5	2.5
5	1	0	0	1	1	3
6	1	0	1	1	0.5	3.5
7	1	0	0	1	1	3
8	1	1	0	1	1	4
9	1	1	0	1	1	4
10	1	1	0	0.5	0.5	4
11	1	0	0	1	0.5	2.5
12	1	1	0	1	0.5	3.5
13	1	0	0	1	1	3
14	1	0	0	1	1	3

15	1	1	0	1	1	4
16	1	0.5	0	1	1	3.5
17	1	0	0	1	1	3
18	1	0	0	1	1	3
19	1	0	0	1	0.5	2.5
20	1	0	0.5	1	0.5	3
21	1	0	0.5	1	0.5	3
22	1	0	0	1	1	3

4.4. Extraer resultados relevantes

De acuerdo con lo descrito[30]. Se diseñó formularios con el objetivo de recolectar toda la información que nos ayude a responder las preguntas de investigación planteadas en el presente estudio. Cada uno de los artículos seleccionados fue leído y simultáneamente se procedió con el llenado de su formulario correspondiente, el cual se realizó en el mismo idioma del artículo. El detalle de los criterios para los cuales no se encontró información relevante fue llenado con las siglas NI (No se encontró información).

Tabla 12: Formulario para la extracción de datos

Criterio	Detalle	Relevancia
Titulo		
Autor		
Tipo de articulo		
Tipo de Formato		
País		
Año		
Metodologías de riesgo		
Base de datos		
Publicación		
Fases		
Categorización		

4.5. Análisis bibliométrico

En esta sección se describe el análisis de la tendencia de los artículos seleccionados para esta Revisión sistemática de la literatura (RSL) de acuerdo a factores como tiempo, tipo de articulo y tema tratado.

4.5.1. **Pregunta de bibliometría 1(PB-1)**

¿Cuál es la cantidad de publicaciones por tipo de artículo sobre el análisis de riesgo de la seguridad de la información?
Mediante la selección de la información de los estudios se pudo hallar diferentes tipos de documentos de investigación. En la Fig. 2 se puede observar un 95% de incidencia de articulo de revisión y un 5 % correspondiente a los documentos de conferencia. Al final se puede concluir que los artículos de revisión son la mayor fuente para realizar el análisis de los riesgos de seguridad de la información.

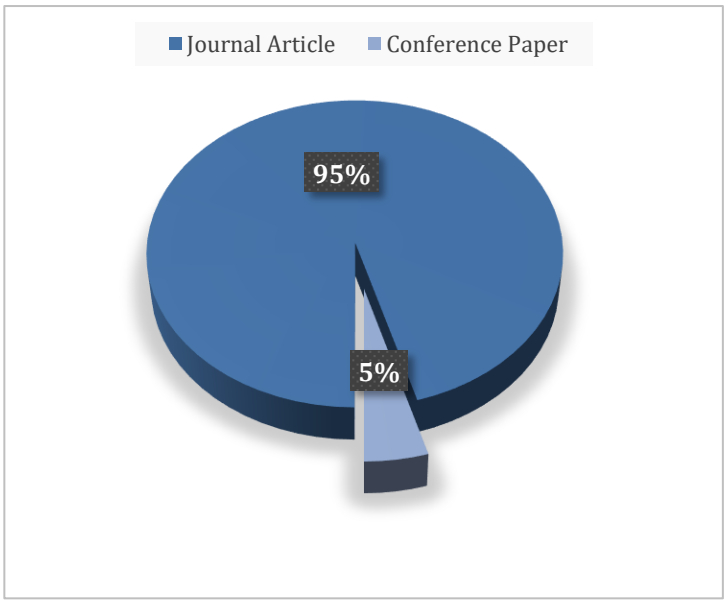


Figura 2: Cantidad de estudios por tipo.

4.5.2. **Pregunta de bibliometría 2(PB-2)**

¿Cómo ha evolucionado en el tiempo la frecuencia de las publicaciones sobre el análisis de riesgo de la seguridad de la información?

Al examinar todos los resultados que se tienen producto de la ejecución de las cadenas de búsqueda mostrados en la Tabla 9, como se puede ver en la Fig. 3 hay un incremento en los años 2018 y 2020 del número de publicaciones que detallan las propuestas de metodologías para el análisis

de riesgo de seguridad de la información, sin embargo, hay un decrecimiento en el año 2019. De un total de 22 artículos el 50 % han sido publicados en los años más resaltantes en cuanto a crecimiento de publicaciones. Por eso, podemos concluir que la relevancia que se le da a esta temática se mantiene vigente.

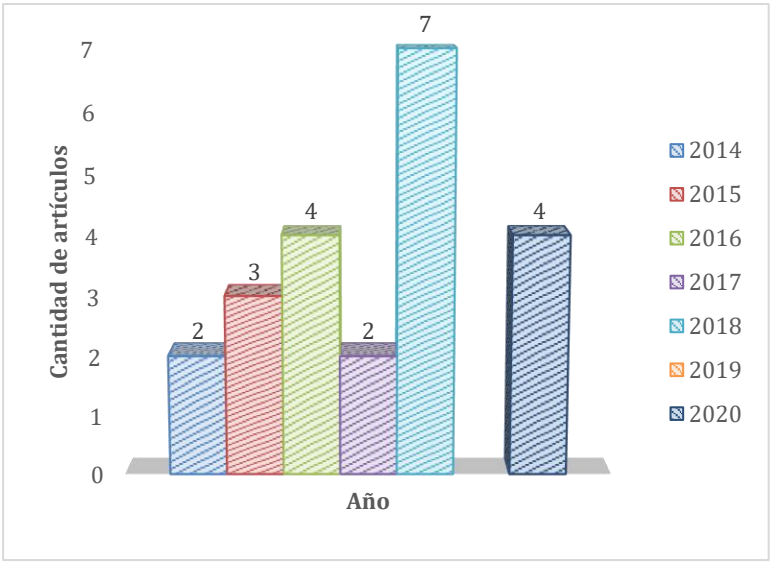


Figura 3: Frecuencia de publicaciones

4.5.3. **Pregunta de bibliometría 3(PB-3)**

¿Cuáles son las publicaciones en las que se han encontrado estudios relacionados al análisis de riesgo de la seguridad de la información?

Las publicaciones han sido seleccionadas y se ha ejecutado el método correspondiente para encontrar reincidencias en cuanto a dominio de publicación, obteniéndose datos muy importantes. En la Tabla 12, se visualizan las publicaciones de donde se han escogido los estudios seleccionados. A partir de este examen se observa que hay una fuerte recurrencia de publicaciones del dominio de *"Computers and Security"* y *"Knowledge-Based Systems"*. Adicionalmente, se muestran otros dominios como: *"Journals in Information Systems and Applications - Springer"*, entre otros.

Tabla 13: Publicaciones correspondientes a los artículos seleccionados.

ID	Publicación	Cantidad
1	Computers and Security	3
2	Knowledge-Based Systems	3
3	Journals in Information Systems and Applications - Springer	2
4	2016 6th International Conference on Innovative Computing Technology, INTECH 2016	1
5	Communications in Computer and Information Science	1
6	Contribuciones a las Ciencias Sociales	1
7	Heliyon	1
8	IEEE World Forum on Internet of Things, WF-IoT 2018 - Proceedings	1
9	Information Technology – New Generations, Advances in Intelligent Systems and Computing	1
10	International Journal of Computer Applications	1
11	Journal of King Saud University - Computer and Information Sciences	1
12	Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)	1
13	Procedia Computer Science	1
14	Proceedings - Annual Reliability and Maintainability Symposium	1

15	Proceedings of the 2018 IEEE Sciences and Humanities International Research Conference, SHIRCON 2018	1
16	Proceedings of the IADIS International Conference Information Systems 2015, IS 2015	1
17	Proceedings of the International Conference on Intelligent Computing and Control Systems, ICICCS 2020	1

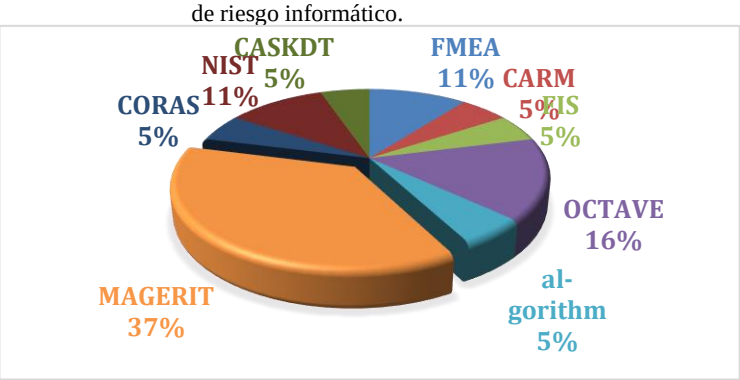
4.6. Sintetizar los datos extraídos

4.6.1. Pregunta de Investigación 1 (PI-1)

¿Qué metodologías para el análisis de riesgo de la seguridad de la información existen en los estudios obtenidos?

En el marco de las principales metodologías para el análisis del riesgo informático de la información y tras haber examinado los resultados, producto de la aplicación del método RSL, se tiene que el 37 % usan la metodología MAGERIT, seguido de un 16% que han elegido utilizar la metodología OCTAVE, seguido la metodología NIST Y FMEA con 11% respectivamente, entre otros. Por lo cual se puede concluir que la principal metodología para el análisis de riesgo es el MAGERIT. Los detalles se pueden visualizar en la Fig. 4.

Figura 4: Principales metodologías para el análisis de riesgo informático.



4.6.2. **Pregunta de Investigación 2 (PI-2)**

¿Cuáles son las fases de las principales metodologías existentes sobre el análisis de riesgo de información, en los estudios obtenidos?

Tabla 14: Fases de metodologías de análisis s de riesgo de la seguridad de la información

PHASES	MAGERIT	OCTAVE-S	NIST	CARM
PHASE 1	Assets	Construction of the threat profile	System Characterization	Plan
PHASE 2	Threats	Identify infrastructure vulnerabilities	Threat Identification Vulnerability Identification Control Analysis	Identify
PHASE 3	Safeguards	Security plans and strategies	Likelihood Determination Impact Analysis Risk Determination	Evaluate
PHASE 4	Residual Impact		Control Recommendations	Threats
PHASE 5	Residual Risk		Control Evaluation Cost/Benefit Analysis Control Selection Safeguard Implementation Plan Development Control Implementation	Monitoring and control

4.6.3. **Pregunta de Investigación 3 (PI-3)**

¿Qué categorías de activos de información consideran las principales metodologías de análisis de riesgo para la seguridad de la información?

Tabla 15: Categorías de activos

MAGERIT	OCTAVE-S	Otro
Hardware	Information	
Software	Systems	
Electronic information	Software	
People	Hardware	Data
Facilities	People	
Support media		
Data communication elements		

5. Conclusiones

En este artículo de revisión se ha realizado mediante la aplicación de instrumentos y la estrategia de Revisión Sistemática de la Literatura, junto con el método PICO, empleado por la mencionada estrategia. Todo esto con la finalidad de identificar las diferentes metodologías, las fases y categorías de activos de información para el análisis de riesgo de seguridad de la información en distintas organizaciones. Para ello, se tomaron en cuenta 22 artículos primarios, que después de una rigurosa examinación a producido las siguientes conclusiones:

- El 95% de todos los estudios empleados para la RSL se encontró que eran de tipo ‘artículo de revisión’, y un 5% corresponde al tipo de ‘artículo de conferencia’, lo cual nos llevó a afirmar que ‘artículo de revisión’ es el factor principal para los respectivos análisis posteriores de la temática.
- Las publicaciones del tema de seguridad de la información experimentaron un crecimiento considerable entre los años 2018 y 2020, lo que nos lleva a concluir que la relevancia que se le da a esta temática se mantiene vigente y es de interés actual.
- Dentro de los dominios de publicación el más recurrente procede de “Computers and Security”, por lo que representa uno de los principales proveedores de estudios sobre el tema tratado en la presente RSL.
- La metodología con mayor presencia en el presente estudio para el análisis de riesgo de seguridad de información es “MAGERIT” que se esfuerza por centrarse en separar los activos de la organización en múltiples grupos con la finalidad de identificar la mayor cantidad de riesgos posibles y a partir de esta base establecer y desarrollar contra medidas para prevenir cualquier inconveniente futuro que se pueda presentar.
- En el presente estudio se ha identificado las fases que involucra las principales metodologías para el análisis de riesgo de seguridad de información, encontrándose lo siguiente:
    - MAGERIT: Assets, Threats, Safeguards, Residual Impact, Residual Risk
    - OCTAVE-S: Construction of the threat profile, Identify infrastructure vulnerabilities, Security plans and strategies
    - NIST: System Characterization, Threat Identification Vulnerability Identification Control Analysis, Likelihood Determination Impact Analysis Risk Determination, Control Recommendations, Control Evaluation Cost/Benefit Analysis Control Selection Safeguard Implementation Plan Development Control Implementation.
    - CARM: Plan, Identify, Evaluate, Threats, Monitoring and control

- En la presente revisión desarrollada también se ha identificado la categorización de los activos de información por parte de las principales metodologías para el análisis de riesgo para la seguridad de la información, los cuales se describen a continuación:
    - MAGERIT: Hardware, Software, Electronic information, People, Facilities, Support media.
    - OCTAVE-S: Information, Systems, Hardware, Software, People.
    - OTROS: Data.

Como proyecto en un futuro, se recomienda establecer un sistema de pasos formalizado para el análisis de las metodologías de riesgo de seguridad de la información, en el que se contemple el examen generalizado del mismo. Por consiguiente, dicha metodología a aplicar debe tener la mayor posibilidad de establecer e identificar las vulnerabilidades y amenazas en los activos de la información, además del análisis de las metodologías ya mencionadas.

Referencias

[1] Mateo Figueroba, “La Importancia de la Tecnología en las Empresas - Fundación Barredo,” 2018. https://www.fund-barredo.es/la-importancia-de-la-tecnologia-en-las-empresas/ (accessed Jul. 02, 2020).

[2] E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, “Information security assessment in public administration,” *Comput. Secur.*, vol. 90, 2020, doi: 10.1016/j.cose.2019.101709.

[3] K. G. B. M. SÁNCHEZ, “ANÁLISIS EN SEGURIDAD INFORMÁTICA Y SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001- SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DIRIGIDO A UNA EMPRESA DE SERVICIOS FINANCIEROS.,” UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL, 2015.

[4] A. Yeboah-Ofori and D. Opoku-Akyea, “Mitigating cyber supply chain risks in cyber physical systems organizational landscape,” *Proc. - 2019 Int. Conf. Cyber Secur. Internet Things, ICSIoT 2019*, pp. 74–81, 2019, doi: 10.1109/ICSIoT47925.2019.00020.

[5] “Tres tipos de seguridad informática que debes conocer | VIU,” *Ciencia y tecnología*, 2018. https://www.universidadviu.com/tres-tipos-seguridad-informatica-debes-conocer/ (accessed Jul. 02, 2020).

[6] “Encuesta Mundial sobre el Estado de la Seguridad de la Información 2018.” https://www.pwc.es/es/digital/encuesta-mundial-ciberseguridad-2018.html (accessed Jul. 02, 2020).

[7] A. Baratta, “SEGURIDAD,” vol. 29, 2001.

[8] F. DE Ciencias De La Salud Carrera De Enfermería, B. Vicente Campoverde Luna Tutora, and L. Miladys Placencia López, “DISEÑO DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA LA COOPERATIVA DE AHORRO Y CRÉDITO,” 2018.

[9] B. A. N. S. María Gabriela Hernández Pinto, “DISEÑO DE UN PLAN ESTRATÉGICO DE SEGURIDAD DE INFORMACIÓN EN UNA EMPRESA DEL SECTOR COMERCIAL,” *Soil Mech. Found. Eng.*, vol. 54, no. 10, pp. 39–46, 2006.

[10] F. N. J. Solarte Solarte, E. R. Enriquez Rosero, and M. del C. Benavides Ruano, “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.,” *Rev. Tecnológica - ESPOL*, vol. 28, no. 5, pp. 492–507, 2015, [Online]. Available: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321.

[11] J. A. Figueroa-Suárez, R. F. Rodríguez-Andrade, C. C. Bone-Obando, and J. A. Saltos-Gómez, “La seguridad informática y la seguridad de la información,” *Polo del Conoc.*, vol. 2, no. 12, p. 145, 2018, doi: 10.23857/pc.v2i12.420.

[12] S. S. Chaeikar, M. Jafari, and H. Taherdoost, “Definitions and Criteria of CIA Security,” *Int. J. Adv. Comput. Sci. Inf. Technol.*, vol. 1, no. 1, pp. 14–23, 2012.

[13] M. Marcos, S. Bedón, J. T. Utrilla, and J. R. Ortega, “Un Proceso Práctico de Análisis de Riesgos de Activos de Información Estándar Australiano,” 2012.

[14] S. Youtricha, “ANÁLISIS Y PLAN DE TRATAMIENTO DE RIESGOS PARA LOS ACTIVOS DE LA INFORMACIÓN DEL CUERPO DE BOMBEROS VOLUNTARIOS DE TUNJA,” *Duke Law J.*, vol. 1, no. 1, pp. 1–13, 2019, doi: 10.1017/CBO9781107415324.004.

[15] “riesgo | Definición | Diccionario de la lengua española | RAE - ASALE.” https://dle.rae.es/riesgo (accessed Jul. 09, 2020).

[16] “ISO - ISO/IEC 27001:2013 - Information technology — Security techniques — Information security management systems — Requirements.” https://www.iso.org/standard/54534.html (accessed Jul. 09, 2020).

[17] C. Suh-Lee and J. Jo, “Quantifying security risk by measuring network risk conditions,” *2015 IEEE/ACIS 14th Int. Conf. Comput. Inf. Sci. ICIS 2015 - Proc.*, pp. 9–14, 2015, doi: 10.1109/ICIS.2015.7166562.

[18] G. Breda and M. Kiss, “Overview of Information Security Standards in the Field of Special Protected Industry 4.0 Areas & Industrial Security,” *Procedia Manuf.*, vol. 46, no. 2019, pp. 580–590, 2020, doi: 10.1016/j.promfg.2020.03.084.

[19] A. De Clase, “El Análisis de Riesgo en la seguridad de la información,” vol. 4, pp. 1–4, 2015.

[20] Y. de la N. Cruz-Gavilánez and C. J. Martinez-Santander, “ISO / IEC 27001 aseguramiento de la calidad de la información: Línea de tiempo,” *Polo del Conoc.*, vol. 3, no. 6, p. 478, 2018, doi: 10.23857/pc.v3i6.641.

[21] I. Umaya, “DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA,” *Univ. Nusant. PGRI Kediri*, vol. 01, pp. 1–7, 2017, [Online]. Available: http://www.albayan.ae.

[22] D. P. C. C. L. E. Y. N. to K. in 20 Weeks, “ANALISIS DE ACTIVOS DE INFORMACION PARA

UN SISTEMA MISIONAL BASADOS EN LA METODOLOGIA MAGERIT V3 Y LA NORMA ISO 27001:2013. Rafael," *Dk*, vol. 53, no. 9, pp. 1689–1699, 2015, doi: 10.1017/CBO9781107415324.004.

[23] G. Cordero Torres Director and M. Esteban Crespo Cuenca, "Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información. Tesis de grado previo a la obtención del título de Ingeniera de Sistemas y Telemática," 2015.

[24] A. Abril, P. Jarol, and B. John, "Risk Analysis in Security of Information," *Risk Anal. Secur. Inf.*, pp. 39–53, 2013.

[25] J. S. Suroso and M. A. Fakhrozi, "Assessment of Information System Risk Management with Octave Allegro at Education Institution," *Procedia Comput. Sci.*, vol. 135, pp. 202–213, 2018, doi: 10.1016/j.procs.2018.08.167.

[26] A. Syalim, Y. Hori, and K. Sakurai, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," *Proc. - Int. Conf. Availability, Reliab. Secur. ARES 2009*, pp. 726–731, 2015, doi: 10.1109/ARES.2009.75.

[27] CLUSIF, "Mehari 2010 Introduction," no. April, pp. 1–308, 2010.

[28] J. E. Quispe Loarte and D. L. Pacheco Pedemonte, "Modelo de evaluación de riesgos de seguridad de la información basado en la ISO/IEC 27005 para analizar la viabilidad de adoptar un servicio en la nube," 2018, [Online]. Available: https://repositorioacademico.upc.edu.pe/handle/10757/625879.

[29] E. N. La *et al.*, "MSA CONSULTING GROUP BASADO," 2020.

[30] C. Manterola, P. Astudillo, E. Arias, and N. Claros, "Revisiones sistemáticas de la literatura. Qué se debe saber acerca de ellas," *Cir. Esp.*, vol. 91, no. 3, pp. 149–155, 2013, doi: 10.1016/j.ciresp.2011.07.009.

[31] R. F. Binyousef, A. M. Al-Gahmi, Z. R. Khan, and E. Rawah, "A rare case of Erdheim-Chester disease in the breast," *Ann. Saudi Med.*, vol. 37, no. 1, pp. 79–83, 2017, doi: 10.5144/0256-4947.2017.79.