UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS

“Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la Información en el marco de la NTP - ISO/IEC 27001:2014”

TESIS

Presentada para optar el Grado Académico de Maestro en Ingeniería de Sistemas con mención en Gerencia de Tecnologías de la Información y Gestión del Software

AUTOR:

Bach. Llauce Valdera, Luciano

ASESOR:

Dr. Diaz Plaza, Regis Jorge Alberto

LAMBAYEQUE - PERÚ

2022

"Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la Información en el marco de la NTP - ISO/IEC 27001:2014"

Bach. Luciano Llauce Valdera
Autor

Dr. Regis Jorge Alberto Diaz Plaza
Asesor

Tesis presentada a la Escuela de Posgrado de la Universidad Nacional Pedro Ruiz Gallo para optar el Grado Académico de **Maestro en Ingeniería de Sistemas con Mención en Gerencia de Tecnologías de la Información y Gestión del Software**.
Aprobado por:

Dra. Giuliana Fiorella Lecca Orrego
Presidenta

M.Sc. Pilar del Rosario Ríos Campos
Secretaria

M.Sc. Juan Elías Villegas Cubas
Vocal

Lambayeque, 2022

Acta de Sustentación

UNPRG UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	ESCUELA DE POSGRADO *M.Sc. Francis Villena Rodríguez*	Versión:	01
		Fecha de Aprobación	29-8-2020
UNIDAD DE INVESTIGACION	FORMATO DE ACTA DE SUSTENTACIÓN VIRTUAL DE TESIS	Pág. 1 de 3	

ACTA DE SUSTENTACIÓN VIRTUAL DE TESIS

Siendo las 10:00 a.m. del miércoles 22 de junio de 2022, se dio inicio a la Sustentación Virtual de Tesis soportado por el sistema Google Meet, preparado y controlado por la Unidad de Tele Educación de la Escuela de Posgrado de la Universidad Nacional Pedro Ruiz Gallo de Lambayeque, con la participación en la Video Conferencia de los miembros del Jurado, nombrados con Resolución N°2144-2018-EPG, de fecha 20 de octubre de 2018, conformado por:

Dra. GIULIANA FIORELLA LECCA ORREGO	Presidenta
Mg. PILAR DEL ROSARIO RÍOS CAMPOS	Secretaria
Mg. JUAN ELÍAS VILLEGAS CUBAS	Vocal
Dr. REGIS JORGE ALBERTO DÍAZ PLAZA	Asesor

Para evaluar el informe de tesis del tesista LUCIANO LLAUCE VALDERA, candidato a optar el grado de MAESTRO EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE, con la tesis titulada "ANÁLISIS COMPARATIVO DE METODOLOGÍAS DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE LA INFORMACIÓN EN EL MARCO DE LA NTP-ISO/IEC 27001:2014".

La Sra. Presidenta, después de transmitir el saludo a todos los participantes en la Video Conferencia de la Sustentación Virtual ordenó la lectura de la Resolución N°638-2022-EPG de fecha 15 de junio de 2022, que autoriza la Sustentación Virtual del Informe de tesis correspondiente, luego de lo cual autorizó al candidato a efectuar la Sustentación Virtual, otorgándole 30 minutos de tiempo y autorizando también compartir su pantalla.

Culminada la exposición del candidato, se procedió a la intervención de los miembros del jurado, exponiendo sus opiniones y observaciones correspondientes, posteriormente se realizaron las preguntas al candidato.

Culminadas las preguntas y respuestas, la Sra. Presidenta, autorizó el pase de los miembros del Jurado a la sala de video conferencia reservada para el debate sobre la Sustentación Virtual del Informe de tesis realizada por el candidato, evaluando en base a la rúbrica de sustentación y determinando el resultado total de la tesis con 16.80 puntos, equivalente a Bueno, quedando el candidato apto para optar el Grado de MAESTRO EN INGENIERÍA DE

SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN Y GESTIÓN DEL SOFTWARE.

Se retornó a la Video Conferencia de Sustentación Virtual, se dio a conocer el resultado, dando lectura del acta y se culminó con los actos finales en la Video Conferencia de Sustentación Virtual.

Siendo las 11:25 a.m. se dio por concluido el acto de Sustentación Virtual.

Dra. GIULIANA FIORELLA LECCA ORREGO
PRESIDENTA

Mg. PILAR DEL ROSARIO RÍOS CAMPOS
SECRETARIA

Mg. JUAN ELÍAS VILLEGAS CUBAS
VOCAL

Dr. REGIS JORGE ALBERTO DÍAZ PLAZA
ASESOR

CERTIFICO: Que, es copia fiel del Original
Fecha: 09/07/2022
Lic. Gloria Luisa Carranza Velásquez
Unidad de Investigación - EPG
VALIDO PARA TRAMITES INTERNOS DE LA UNPRG

Declaración Jurada de originalidad

Yo, **Luciano Llauce Valdera**, investigador principal y el **Dr. Regis Jorge Alberto Diaz Plaza**, asesor del trabajo de investigación **"Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la información en el marco de la NTP – ISO/IEC 27001:2014"**, declaro bajo juramento que este trabajo no ha sido plagiado, ni contiene datos falsos. En caso se demuestre lo contrario, asumo responsablemente la anulación de este trabajo, y por ende el proceso administrativo a que hubiere lugar que puede conducir a la anulación del grado emitido como consecuencia de este trabajo de investigación.

Lambayeque, 20 de marzo de 2022

Luciano Llauce Valdera
Autor

Dr. Regis Jorge Alberto Diaz Plaza
Asesor

Dedicatoria

A mi padre Florencio, por su ejemplo y guía constante, en numerosas e incansables jornadas de enseñanzas empíricas; conocimientos que me van permitiendo alcanzar mis sueños.

A mi primavera y sol, mi madre Julia, por enseñarme los más altos valores como la vida misma, eres mi fuente de sabiduría y bondad, sustento y base de mis anhelos.

A mis hermanos y hermanas, por su apoyo y sobre todo por la calidez de familia.

Agradecimiento

Agradezco a Dios, padre y todopoderoso por su inmensa sabiduría al darme la vida, al Dr. Regis Jorge Alberto Diaz Plaza por sus conocimientos, guía y ayuda en la presente investigación, a los docentes de la escuela de Pos Grado por la impartición de sus enseñanzas.

Índice

Índice de tablas

Índice de Figuras

Resumen

Mediante Resolución n.º 004-2016-PCM, el Estado Peruano aprobó el uso obligatorio de la Norma Técnica Peruana *"NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición"*, en todas las entidades integrantes del sistema nacional de informática, con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, pero ésta no especifica la metodología de gestión de riesgos a utilizar; en ese sentido, al no tener en claro que metodología de gestión de riesgos de tecnologías de información se encuentra relacionada con la NTP ISO/IEC 27001:2014, podría generar deficiencias significativas en la gestión de riesgos, y podría estar incidiendo en las entidades y en efecto, no estar invirtiendo correctamente los recursos del estado peruano.

El objetivo de la investigación fue determinar una metodología de gestión de riesgos de tecnología de información que mejor se relacione con la Norma Técnica Peruana NTP - ISO/IEC 27001:2014.

El tipo de investigación fue de nivel cualitativo, bajo el diseño de teoría fundamentada de tipo emergente. La evidencia fue la documentación oficial de la Norma Técnica Peruana NTP - ISO/IEC 27001:2014, revisión de las metodologías de gestión de riegos de TI y el Método de Estudio de Similitudes entre modelos y Estándares (MSSS).

Se adaptó el Método de Estudio de Similitudes entre Modelos y Estándares (MSSS) que incluyó definir criterios de selección, seleccionar metodologías, elegir estándares de referencia, identificar características, establecer nivel de detalle, definir

plantillas de comparación, identificar similitudes, sistematizar información y determinar el grado de similitud.

En ese sentido, se determinó que la metodología Magerit V3, es la metodología de gestión de riesgos de tecnologías de información que más se relaciona con la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, al presentar un 96% de similitud.

Asimismo, se estableció que la metodología Magerit V3 se constituye en una metodología de madurez en la Gestión de riesgos de tecnologías de información para instituciones estatales.

Palabras claves: Riesgos de tecnologías de información, Comparación de metodologías de riesgos de TI, Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

ABSTRACT

Through Resolution n.° 004-2016-PCM, the Peruvian State approved the mandatory use of the Peruvian Technical Standard “NTP ISO / IEC 27001: 2014 Information Technology. Security Techniques. Information Security Management Systems. Requirements. 2nd. Edition”, in all the entities that make up the national computer system, with the aim of minimizing the risks in the event of suffering some type of incident in the computer resources of the State, establishing the guidelines for information security; but it does not specify the risk management methodology to be used; In this sense, not being clear about which information technology risk management methodology is related to the ISO / IEC 27001: 2014 NTP could generate significant deficiencies in risk management, which could be affecting entities and in effect, it is not correctly investing the resources of the Peruvian state.

The objective of the research was to determine an information technology risk management methodology that best relates to the Peruvian Technical Standard NTP - ISO / IEC 27001: 2014.

The type of research was qualitative level and grounded theory design at the emergent level. The evidence was the official documentation of the Peruvian Technical Standard NTP - ISO / IEC 27001: 2014, review of IT risk management methodologies and the Method of Study of Similarities between models and Standards (MSSS).

The Method for the Study of Similarities between Models and Standards (MSSS) was adapted, which included defining selection criteria, selecting methodologies, choosing reference standards, identifying characteristics, establishing

a level of detail, defining comparison templates, identifying similarities, systematizing information and determining the degree of similarity.

It was determined that the Magerit V3 methodology is the Information Technology Risk Management Methodology that is most related to the Peruvian Technical Standard NTP-ISO / IEC 27001: 2014, presenting 96% similarity.

It was established that the Magerit V3 methodology constitutes a Mature methodology in Information Technology Risk Management for state institutions.

Keywords: Information technology risks, Comparison of IT risk methodologies, Peruvian Technical Standard NTP-ISO / IEC 27001: 2014.

INTRODUCCIÓN

En la actualidad no existe organización pública o privada que no utilice algún servicio relacionado con tecnologías de información, como medio para facilitar procesos, servicios o productos a nivel de clientes, usuarios y/o ciudadanos; y en el caso de las entidades públicas peruanas, la dependencia de las tecnologías de información se incrementan cada vez más, en virtud de responder a la transformación digital, las necesidades de comunicación, teletrabajo, teleducación, así como, la integración de servicios entre las entidades del estado; las cuales presentan innumerables ventajas, no obstante, las tecnologías y los activos de información presentan diferentes niveles de riesgos, que en muchos casos, se efectivizan por la falta de conocimientos, controles y/o deficientes normas internas de las empresas y/o instituciones; lo que facilita la aparición de vulnerabilidades y amenazas informáticas relacionadas con los recursos humanos, incidentes naturales, fallas técnicas y/o malware.

Por otro lado, tenemos que, en el 2016, según la Resolución Nº 004-2016-PCM, el Estado Peruano aprobó el uso obligatorio de la Norma Técnica Peruana *"NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición"*, en todas las entidades integrantes del Sistema Nacional de Informática, con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, estableciéndose los lineamientos para la seguridad de la información; pero esta no especifica la metodología de gestión de riesgos a utilizar, dando libertad de elegir cualquier metodología de gestión de riesgos (Del Carpio

Wong, 2016), no obstante, muchas de estas metodologías no se relacionan completamente con la NTP ISO/IEC 27001:2014.

En ese sentido, se planteó determinar una metodología de gestión de riesgos de tecnologías de la información de acuerdo al marco de la NTP - ISO/IEC 27001:2014, que implique analizar metodologías de gestión de riesgos de tecnologías de la información, disminuir la incertidumbre en la selección de metodologías de gestión de riesgos de tecnologías de información en el marco de la NTP - ISO/IEC 27001:2014, especificar una metodología de madurez en gestión de riesgos de tecnologías de información que mejor se relacione con la NTP - ISO/IEC 27001:2014.

En atención a ello, se revisó el marco teórico vinculado a la Norma Técnica Peruana NTP - ISO/IEC 27001:2014, metodologías de gestión de riesgos de tecnologías de información, igualmente, se adaptó el Método de Estudio de Similitudes entre Modelos y Estándares (MSSS), el cual estableció la estructura y secuencias formales de comparación; asimismo, se establecieron criterios de identificación y selección de metodologías de gestión de riesgos.

Dentro de este marco, en el capítulo I, se realizaron los antecedentes de la investigación, las bases teóricas y las definiciones conceptuales.

En el capítulo II, se describió el tipo de investigación, el método de investigación y los materiales utilizados.

En el capítulo III, se presentaron los resultados a través de tablas estructuradas de comparación de las metodologías de gestión de riesgos de

tecnologías de información y la Norma Técnica Peruana NTP - ISO/IEC 27001:2014.

En el capítulo IV, se discutieron los resultados obtenidos de la investigación.

Capitulo I: Diseño Teórico

1.1 Antecedentes de la investigación

1.1.1 Antecedentes internacionales

En una primera investigación realizada por Crespo (2016), denominada "Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES" del sector Ecuatoriano; estableció un modelo de gestión de riesgos basado en metodologías de gestión de riesgos de tecnologías de la información, como Magerit, CRAMM, OCTAVE-S, Microsoft Risk Guide, COBIT 5 y COSO III; para lo cual, planteó 5 procesos de gestión: determinación del contexto, identificación de activos de información, identificación de riesgos, análisis de riesgos, evaluación y tratamiento de los riesgos, identificación de contramedidas; 1 Proceso de monitoreo y control: Monitoreo y revisión y 1 proceso comunicacional: Comunicar y consultar. El objetivo de su investigación fue desarrollar una metodología de seguridad de la información para la gestión del riesgo informático de las organizaciones del sector MPYME, aplicable al entorno ecuatoriano; en ese sentido, utilizó el método no probabilístico de muestreo por conveniencia para una población de 66 551 empresas ecuatorianas, tomando como muestra a 50 de ellas; utilizando como instrumento la guía especificada en Magerit; generando como resultado la metodología ECU@Risk; asimismo, concluyó que la Metodología Magerit es la más completa, al proporcionar un marco de trabajo para la toma de decisiones en gestión de riesgos.

La relación con esta investigación es que, permitirá delinear los mecanismos para realizar el análisis de metodologías de gestión de riesgos de tecnologías de información, y establecer los factores críticos a tomar en cuenta para una correcta

administración de riesgos de TI; para ello, es necesario estudiar las metodologías de gestión de riesgos de tecnologías de información existentes.

En una segunda investigación, Prieto, Meneses, & Vega, (2015) en su tesis "Análisis comparativo de modelos de madurez en inteligencia de negocios", planteó la no existencia de una comparación cuantitativa o cualitativa de modelos de inteligencia de negocios, basado en argumentos para la selección de uno de ellos como referencia para una organización.

En esta investigación se aplicó el método de estudio de similitudes y estándares (MESME) y la técnica de análisis envolvente de datos (DEA), con la finalidad de poder caracterizar y comparar los modelos de madurez de BI. Con el método MESME se logró realizar un análisis cualitativo de las similitudes de las metodologías de BI, y con la técnica DEA se realizó una comparación cuantitativa de las diferentes fases de los modelos seleccionados, permitiéndole comparar la composición estructural en cada nivel de madurez, lo que posibilitó reconocer los cambios en la relación entre entradas y salidas en todos los niveles de madurez. Con la técnica DEA, el investigador logró identificar los modelos que presentan unas estructuras rígidas o flexibles en sus niveles de madurez; como resultado de esta investigación se obtuvo la obtención de un análisis comparativo cualitativo y cuantitativo de un conjunto de modelos de madurez.

Esta investigación contribuye con la técnica MESME, la cual tiene una gran similitud con el método MSSS; en igual forma, proporciona mecanismos y perspectivas de análisis comparativos, que permitirán realizar una adaptación en la investigación propuesta.

En una tercera investigación vinculada al análisis comparativo, Gasca (2011) planteó un “Estudio de similitud del proceso de gestión de riesgos en proyectos de outsourcing de software: utilización de un método”, estudio que fue realizado con el fin de determinar el enfoque que los estándares y modelos tienen respecto a la gestión de riesgos en outsourcing de software; para lo cual, el investigador adaptó un método de mapeo de estándares y modelos, lo que le permitió tener una visión general del estado de la gestión de riesgos en outsourcing de software. El investigador utilizó el Método de estudio de similitud entre modelos y estándares (MSSS), el cual permite realizar un análisis y mapeo profundo, en la selección y análisis de los estándares y/o modelos de manera formal.

Por consiguiente, el método MSSS establece una serie de pasos mínimos o fases que permiten formalizar y organizar el estudio, siendo estas: 1) Seleccionar posibles estándares y modelos a analizar, 2) Seleccionar o definir el modelo de referencia, 3) Seleccionar el o los procesos que se van a analizar, 4) Establecer el nivel de detalle, 5) Crear una plantilla de correspondencia, 6) Identificar las similitudes entre los modelos, 7) Presentar resultados obtenidos; sin embargo el autor considera que estos son pasos generales, por lo que, realizó una adaptación del método, y como consecuencia, generó un conjunto de pasos para comparación especifica en gestión de riesgos en outsourcing de software, siendo estos: 1) Definir criterios para seleccionar modelos y estándares, 2) Seleccionar estándares y modelos, 3) Definir los aspectos a analizar de cada uno de los modelos y estándares, 4) Identificar procesos a analizar, 5) Establecer el objetivo del análisis, 6) Definir la estructura para presentar el análisis realizado, 7) Identificar similitudes, sintetizar información y recoger resultados.

Como resultado obtuvo que el modelo CMMI-ACQ, es el que más características relacionadas tiene con la gestión de riesgos dentro del outsourcing de software.

Esta investigación presenta los pasos generales del método de estudio de similitud entre modelos y estándares (MSSS), que servirá de base para realizar una adaptación para análisis comparativo de metodologías de gestión de riesgos de tecnologías de información en el marco de la NTP - ISO/IEC 27001:2014, y además presenta un enfoque metodológico de una adaptación en particular.

1.1.2 Antecedentes nacionales

Una cuarta investigación realizado por Seclén (2016) en su trabajo "Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001"; El autor plantea una investigación cualitativa para determinar las causas que impiden implantar un correcto sistema de gestión de seguridad de tecnologías de información; para ello, tomo como población de estudio, a los organismos públicos descentralizados que conforman el sistema nacional de informática adscritos a la Presidencia del Consejo de Ministros (PCM) del Gobierno Central, seleccionando una muestra de siete instituciones del estado.

La recopilación de información se realizó mediante entrevistas a oficiales de seguridad de la información en entidades públicas de acuerdo a la NTP - ISO/IEC 27001:2014, y como resultado de su investigación, se obtuvo que existen diferentes factores que afectan la implementación del SGSI, los cuales fueron divididos en 3 niveles: nivel estratégico, operativo y técnico.

La relación con esta investigación, es que proporciona indicios de aquellos factores vinculados al éxito / fracaso de la implementación de la NTP-ISO/IEC 27001 en las instituciones públicas, lo que evidencia la ausencia de una metodología de gestión de riesgos de tecnologías de información que ayude a gestionar tales riesgos (factores).

De acuerdo a los antecedentes analizados, se llega a determinar que existe una deficiencia en la determinación de una metodología de gestión de riesgos de tecnologías de información que mejor se relacione Norma Técnica Peruana NTP-ISO/IEC 27001:2014 para las instituciones públicas peruanas, sin embargo, existen investigaciones que presentan diferentes perspectivas de análisis, así como, métodos formales de comparación, los cuales representan aportes valiosos para esta investigación.

1.2 Base teórica

1.2.1 Norma Técnica Peruana NTP – ISO/IEC 27001:2014

El estado peruano ha establecido un conjunto de normas y estándares para mejorar la gestión de las instituciones públicas, y como parte de estas políticas, estableció la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, publicada en el año 2014, norma que ha sido adaptada por el comité técnico de normalización de codificación e intercambio electrónico de datos; y proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información.

Asimismo, la Norma Técnica Peruana incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las

necesidades de la organización; tales requisitos son genéricos y están hechos para aplicarse a todas las organizaciones, sin importar su tipo, tamaño o naturaleza.

La NTP-ISO/IEC 27001:2014; está constituida por 14 dominios, 35 objetivos de control y 114 controles.

Dominios:

- Política de seguridad.
- Organización de la seguridad de la información.
- Seguridad ligada a los recursos humanos.
- Gestión de activos.
- Control de accesos.
- Criptografía.
- Seguridad física y del medio ambiente.
- Seguridad en las operaciones.
- Seguridad en las comunicaciones.
- Relaciones con los proveedores.
- Adquisición, desarrollo y mantenimiento de sistemas.
- Gestión de incidentes de seguridad de la información.
- Gestión de la continuidad del negocio.
- Cumplimiento.

1.2.2 Riesgos de tecnologías de información

Las tecnologías de información están presentes en todas las organizaciones independientemente de su tamaño y sector; según Valencia, Marulanda, & López (2016), los riesgos derivados de su operación se convierten en aspectos críticos que

requieren ser tratados a través de un adecuado gobierno y gestión, en ese sentido, los riesgos de tecnologías de información tienen implicancias y consecuencias en todos los aspectos y niveles organizativos.

En habidas cuentas, el riesgo es la probabilidad de ocurrencia de un evento no deseado que podría perjudicar o afectar adversamente a la entidad o a su entorno.

Dentro de este marco, Ramírez & Ortiz (2011) plantea realizar una valoración de riesgos tecnológicos, a través de la identificación de los activos que se necesiten proteger, reconocer las debilidades, asimismo, las amenazas a las cuales se encuentran expuestos. En este punto, los referidos autores, recomiendan implementar controles para la mitigación de los riesgos. Cabe considerar que, para realizar una correcta valoración, se deben tener en cuenta los activos más relevantes para la organización, que incluyan, personas, procesos, información, datos y activos de soporte.

En ese sentido, la valoración de activos de soporte debe incluir costos por adquisición, renovación o reposición, mantenimiento, así también, tener en cuenta los factores de depreciación.

Bajo esta perspectiva, es de vital importancia establecer el listado de los activos organizacionales, sus mecanismos de validación, identificación del nivel de alcance, así como, los mecanismos de monitorización, que permitan evaluar si lo implementado, es correcto o debe ser ajustado para cumplir con los propósitos diseñados.

Por otro lado, se deben tener en cuenta los tipos de amenazas y su evolución en el tiempo, toda vez, que estas generalmente, son del tipo físico, lógico o estratégico, no obstante, no deberían dejarse de lado el origen de las mismas; y de acuerdo al core del negocio, pueden estar vinculadas a amenazas de origen natural, técnico, humano accidental o intencional; en ese sentido, en caso de la materialización de las amenazas, las organizaciones deberían estar en la capacidad de poder estimar los daños y la determinación de las pérdidas en términos de impacto.

La gestión de riesgos de TI implica una monitorización constante de los mismos, con la finalidad de priorizarlos y medirlos, conforme a las políticas y controles diseñados para cada organización.

1.2.2.1 Directrices de evaluación de riesgos

Las directrices son un conjunto de normas que permiten evaluar y monitorizar los diferentes riesgos, asimismo, permiten definir planes de acción y protección, teniendo en cuenta aspectos relacionados a seguridad de la información y cultura organizacional; en ese sentido, las directrices para la evaluación de riesgos informáticos deben estar acorde a las amenazas y vulnerabilidades actuales y futuras a fin de asegurar la operatividad y continuidad de la organización.

En el Perú existe la norma NTP-ISO 27001-2014: Tecnologías de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos; creada con el propósito de brindar lineamientos para establecer, implementar, mantener y mejorar continuamente un sistema de seguridad de la información dentro del contexto de la organización.

De acuerdo a las buenas prácticas para el aseguramiento de la información, se deben tomar en cuenta con tres (3) aspectos fundamentales en la creación e implementación directrices de seguridad de la información:

- Políticas a nivel estratégico.
- Políticas a nivel operacional.
- Políticas a nivel de usuario final.

1.2.3 Metodologías

Las metodologías para implementar y gestionar riesgos de tecnologías de información pueden variar en formas, mecanismos de evaluación y presentación de resultados, dado que, algunas son difíciles de implementar y cuantificar, tanto en sus resultados como en sus logros, asimismo, existen otras que se prestan para un diagnóstico numérico.

En ese sentido, es de primordial importancia en la gestión de riesgos de tecnologías de información, que la máxima autoridad, el nivel directivo y todo el personal de la entidad sean responsables de efectuar el proceso de administración de riesgos, independientemente de la metodología utilizada, no obstante, la metodología proporciona técnicas y procedimientos, a través de los cuales las unidades administrativas identificarán, analizarán y tratarán los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos.

Actualmente existen diversas metodologías para gestión de riesgos de tecnologías de la información; que analizan la gestión de riesgos de TI bajo diferentes perspectivas y enfoques; por lo que, es necesario analizarlas para determinar los factores más importantes que se deben tomar en cuenta en la gestión

de riesgos de TI y así establecer una metodología con alineación a la NTP-ISO 27001-2014.

Las metodologías más relevantes que se estudiaran en la gestión de riesgos de tecnologías de información son:

1.2.3.1 Metodología Magerit V3.0

Según el consejo de la administración pública (CSAE), Magerit es una metodología que establece los principios para el uso eficaz, eficiente y aceptable de las tecnologías de la información, garantizando a las organizaciones que, bajo estos principios, se ayudará a los directores a equilibrar riesgos y oportunidades derivados del uso de las TI.

La metodología Magerit implementa el proceso de gestión de riesgos dentro de un marco de trabajo que involucra dos grandes actividades: el análisis de los riesgos y el tratamiento de los riesgos; que combinadas la denomina Gestión de Riesgos.

En ese contexto, la metodología de análisis de riesgo de Magerit plantea cinco (5) pasos, que se describen a continuación:

1. **Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de que perjuicio (costo) supondrá su degradación**

   La metodología Magerit utiliza la definición de activo de UNE 71504:2008, la cual señala que, el activo es un componente o funcionalidad de un sistema de información susceptible de ser atacado

deliberada o accidentalmente con consecuencia para la organización, incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Asimismo, establece que los activos deben ser evaluados de acuerdo a criterios vinculados a:

Dependencia: los activos dependen de otros activos, de tal forma que tienden a formar árboles o grafos de dependencias. Estas estructuras reflejan de arriba hacia abajo las dependencias, mientras que, de abajo hacia arriba la propagación del daño, en caso de materializarse las amenazas.

> Toda organización es particular y única, no obstante, los activos pueden clasificarse en capas: activos esenciales, servicios internos y equipamientos informáticos.

Dimensiones: los activos pueden tener diferentes dimensiones, entre ellas, la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Valoración: es una perspectiva para determinar cuan valioso es un activo, en función de las dimensiones de seguridad. El valor puede ser propio o puede ser acumulado, en ese sentido, se realizan valoraciones cuantitativas y cualitativas; así mismo, se determina la valoración de la interrupción del servicio.

2. **Determinar a qué amenazas están expuestos aquellos activos**: en este aspecto plantea lo siguiente:

   Identificación de las amenazas: en función de las amenazas físicas, del entorno, defecto de aplicaciones, causadas por las personas de forma accidental y causadas por personas de forma deliberada.

   Valoración de las amenazas: permite determinar las amenazas en un activo y su influencia en el valor del activo, y plantea una evaluación en dos sentidos:

   - **Degradación:** cuan perjudicado resultaría el [valor del] activo.
   - **Probabilidad**: Cuan probable o improbable es que se materialice la amenaza. En este sentido, la probabilidad se modela cualitativamente o cuantitativamente.

3. **Determinación del impacto potencial**: es la medida del daño sobre el activo derivado de la materialización de una amenaza; para lo cual se analiza en:

   Impacto acumulado: calculado sobre un activo teniendo en cuenta:

   - Su valor acumulado (el propio más el acumulado de los activos que depende de él).
   - Las amenazas a que está expuesto.

   Impacto repercutido: calculado sobre un activo teniendo en cuenta:

- Su valor propio
- Las amenazas a que están expuestos los activos.

4. **Determinación del riesgo potencial**

La metodología plantea evaluar el riesgo en función del impacto y la probabilidad, pudiéndose distinguirse zonas a tener en cuenta en el tratamiento del riesgo.

- Zona 1 - Riesgos muy probables y de muy alto impacto.
- Zona 2 - franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo a muy bajo.
- Zona 3 - riesgos improbables y de bajo impacto.
- Zona 4 - riesgos improbables, pero de muy alto impacto.

Asimismo, plantea un análisis y evaluación de riesgos en función de:

- Riesgo Acumulado: es calculado sobre un activo teniendo en cuenta el impacto acumulado sobre un activo debido a una amenaza y la probabilidad de la amenaza.
- Riesgo repercutido: es calculado sobre un activo teniendo en cuenta el impacto repercutido sobre un activo debido a una amenaza y la probabilidad de la amenaza.

5. **Determinar salvaguardas**

Las salvaguardas o contramedidas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

Selección de salvaguardas: realizar un análisis inicial con el fin de establecer las más relevantes, teniendo en cuenta los siguientes aspectos:

- Tipos de activos a proteger, pues cada tipo se protege de una forma específica.
- Dimensión o dimensiones de seguridad que requieren protección.
- Amenazas de las que necesitamos protegernos.
- Si existen salvaguardas alternativas.

Efecto de las salvaguardas: las salvaguardas entran en el cálculo del riesgo en dos formas:

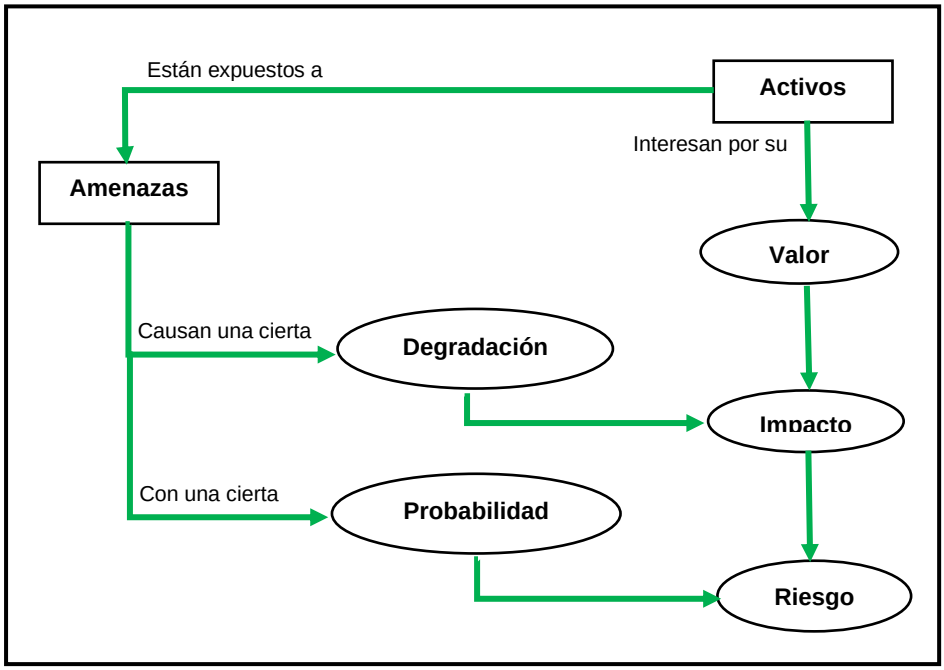
- Reduciendo la probabilidad de las amenazas, llamadas salvaguardas preventivas.

- Limitando el daño causado, las que limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para detener la degradación.

La siguiente figura presenta los elementos planteados en la metodología Magerit para análisis de riesgos.

Figura 1

Elementos del análisis de riesgos potenciales.



Fuente: MAGERIT - versión 3.0 - Libro I Método.

En ese sentido, la metodología Magerit persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

- Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

1.2.3.2 Metodología Octave

Según el programa CERT y la Universidad Carnegie Mellón, Octave es una metodología que tiene como propósito ayudar a las organizaciones en la gestión de riesgos informáticos, centrado en riesgos organizacionales; principalmente en los aspectos relacionados con el día a día de las empresas; para ello divide la gestión de riesgos en tres (3) fases:

Visión organizativa: en esta primera fase, se identifican los activos de información y su clasificación en función al nivel de criticidad para la organización, asimismo, se identifican a las amenazas de esos activos y las estrategias de protección basada en el conocimiento del personal conforme a los múltiples niveles en la organización, asimismo, de los documentos que contienen las buenas prácticas propias de la entidad. Esta información permitirá establecer los requisitos de seguridad de la empresa, que es el objetivo de la primera fase de OCTAVE. (Alberts, Behrens, Pethia, & Wilson, 1999).

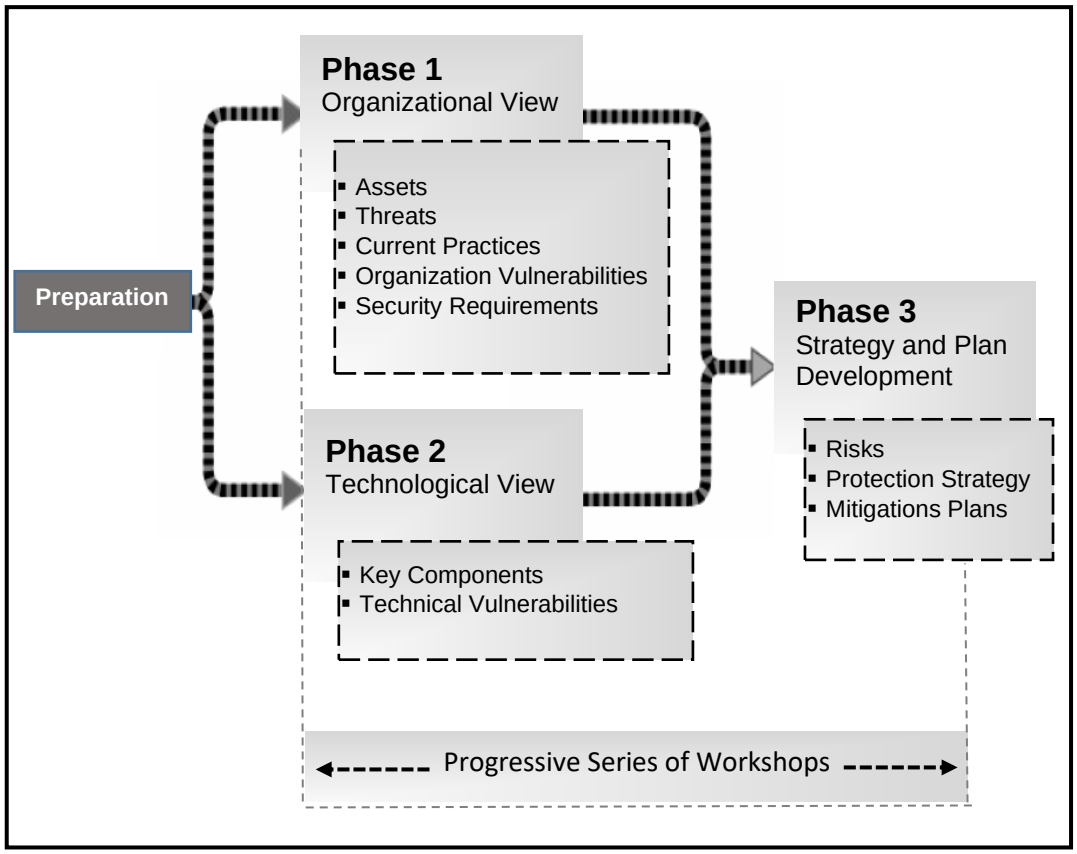
Visión tecnológica: se realiza una evaluación de los componentes de infraestructura de información para complementar el análisis de amenazas realizado en la fase 1, y determinar la infraestructura de alta prioridad e informar las decisiones de mitigación en la siguiente fase. Al concluir la fase

2, la organización ha identificado los componentes de la infraestructura de información de alta prioridad, las políticas y prácticas faltantes. (Alberts, Behrens, Pethia, & Wilson, 1999).

Estrategia y plan de desarrollo: el equipo de análisis realiza actividades de identificación de riesgos y desarrolla un plan de mitigación de riesgos para los activos críticos. (Caralli, Stevens, Young, & Wilson, 2007).

Figura 2

Fases del Método Octave.



Fuente: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.

El núcleo central de la metodología Octave es un conjunto de criterios (principios, atributos y resultados) a partir de los cuales se pueden

desarrollar diversas metodologías. Octave divide los activos en dos tipos: Sistemas (Hardware, Software y Datos) y Personas.

En ese contexto, la metodología Octave presenta versiones, las cuales están en función a la cantidad de personas en las organizaciones; así tenemos:

- Octave - S
- Octave Allegro

Octave S

Está diseñado para evaluar riesgos en organizaciones pequeñas, de hasta 100 personas, y consta de tres fases similares a la de Octave, para lo cual se debe tener un amplio conocimiento de los activos importantes relacionados con la información, los requisitos de seguridad, las amenazas y prácticas de seguridad de la organización. (Caralli, Stevens, Young, & Wilson, 2007).

Octave Allegro

Diseñado para permitir una evaluación amplia del entorno de riesgo operativo de una organización con el objetivo de producir resultados más sólidos sin la necesidad de un amplio conocimiento de la evaluación de riesgos. Este enfoque difiere de los enfoques anteriores de OCTAVE al centrarse principalmente en los activos de información en el contexto de cómo se usan, dónde se almacenan, transportan y procesan, y cómo están expuestos a amenazas, vulnerabilidades e interrupciones como resultado. (Caralli, Stevens, Young, & Wilson, 2007).

Octave Allegro divide la gestión de riesgos en cuatro (4) fases, las cuales presentan en total ocho (8) pasos, de acuerdo al siguiente detalle:

Paso 1 - Establecer criterios de medición de riesgos: se establecen las entradas activadoras o factores organizacionales que se utilizarán para evaluar los efectos de un riesgo en la misión y los objetivos comerciales de una organización. Estas entradas activadoras constituyen un conjunto de criterios de medición de riesgos.

Los criterios de medición del riesgo son un conjunto de medidas cualitativas para evaluar y formar la base de una evaluación de riesgos de activos de información. (Caralli, Stevens, Young, & Wilson, 2007)

En ese sentido, los criterios de medición del riesgo deben ser consistentes, de tal forma que reflejen con precisión la visión organizacional sobre cómo mitigar los riesgos en los activos de información y unidades operativas o departamentales; asimismo, deben ser capaces de evaluar el impacto.

Paso 2 - Desarrollar un perfil de activos de información: un perfil es una representación de un activo de información que describen sus características, cualidades, características y valores únicos. El proceso de elaboración del perfil de la metodología garantiza que un activo se describa en forma clara y coherente y, sobre todo, que haya una definición inequívoca de los límites del activo y de los requisitos de seguridad para los activos adecuadamente definidos.

El perfil de cada activo se captura en una sola hoja de trabajo que forma la base para la identificación de amenazas y riesgos en los pasos posteriores. (Caralli, Stevens, Young, & Wilson, 2007)

Paso 3 - Identificar la ubicación de los Activos de información: se describen y ubican los lugares en donde se almacenan, transportan y procesan los activos de información, ya sea dentro de la organización (interno) o fuera de ella, en caso de activos que se encuentren bajo el dominio de proveedores (externo); independientemente de ello, se deben establecer y tener claros los límites y riesgos asociados.

Cualquier riesgo para los contenedores en los que vive el activo de información son heredados por el activo de información. (Caralli, Stevens, Young, & Wilson, 2007)

Paso 4 - Identificar áreas de preocupación: el equipo de análisis de riesgos de TI, identificara las posibles situaciones adversas o condiciones que podrían amenazar a los activos de información. La metodología recomienda iniciar con una lluvia de ideas.

Las áreas de preocupación constituyen escenarios del mundo real, en donde se advierten situaciones que pueden representar amenazas y sus correspondientes resultados indeseables.

El propósito de este paso no es capturar una lista completa de todos los posibles escenarios de amenazas para un activo de información; en cambio, la idea es capturar rápidamente aquellas situaciones o condiciones

que vienen inmediatamente a la mente del equipo de análisis. (Caralli, Stevens, Young, & Wilson, 2007).

Paso 5 - Identificar escenarios de amenazas: este paso expande y detalla las amenazas advertidas en las áreas de preocupación capturadas en el paso anterior, en el sentido que, en este paso, se considera una amplia gama de amenazas adicionales al examinar detalladamente los escenarios de amenazas.

Los escenarios de amenazas se pueden representar visualmente en una estructura de árbol comúnmente conocida como árbol de amenazas. Los árboles de amenaza provienen del método OCTAVE. (Caralli, Stevens, Young, & Wilson, 2007).

Los árboles de amenazas incluyen personas, recursos técnicos, desastres naturales, entre otros, los cuales se detallan a continuación:

- Humanos que utilizan medios técnicos.
- Humanos que utilizan el acceso físico.
- Problemas técnicos.
- Otros problemas como desastres naturales, infraestructura critica, etc.

Paso 6 - Identificar riesgos: en este paso, se capturan las consecuencias para una organización, en caso se materialice una amenaza, completando de esta forma el escenario para un riesgo.

Las actividades involucradas en este paso aseguran que se capturen las diversas consecuencias del riesgo.

Paso 7 - Análisis de riesgos: se realizan cálculos cuantitativos en la medida que la organización se ve afectada por una amenaza. Se aplica una puntuación de riesgo relativo, en función a la probabilidad de ocurrencia y el nivel de impacto en el área de la organización.

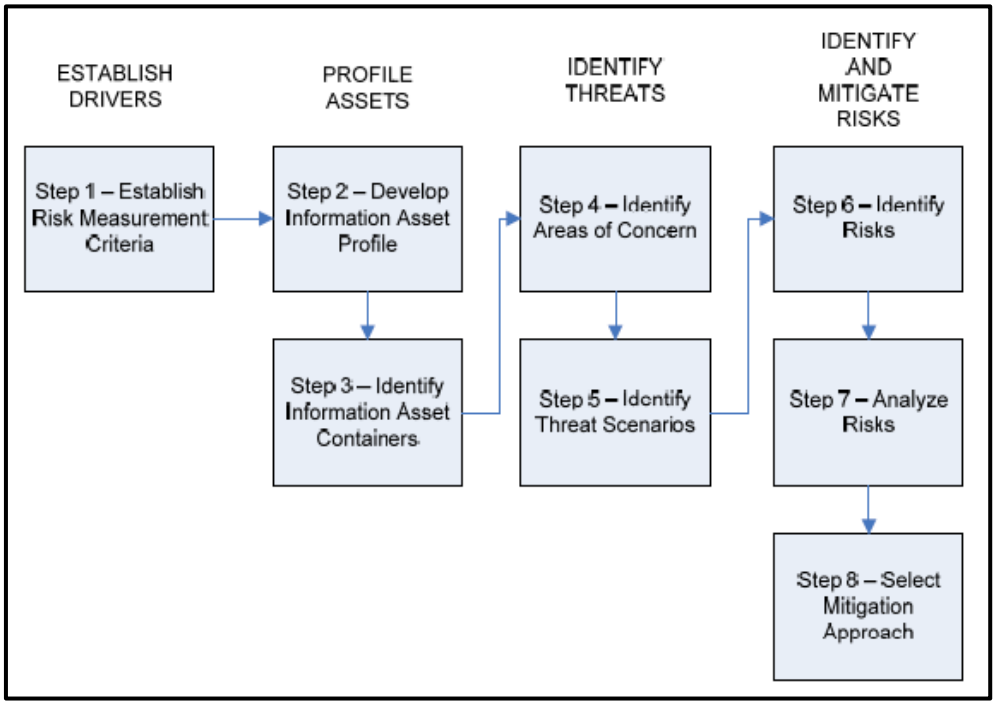
Paso 8 - Seleccionar el enfoque de mitigación: en este paso, las organizaciones determinan cuáles de los riesgos que han sido identificados, requieren mitigación y desarrollan una estrategia para ello.

Esto se logra priorizando primero los riesgos en función de su puntuación de riesgo relativo y se desarrollan estrategias de mitigación que consideran el valor del activo y sus requisitos de seguridad, los contenedores en los que vive y el entorno operativo único de la organización. (Caralli, Stevens, Young, & Wilson, 2007)

La siguiente figura presenta los ocho (8) pasos planteados en la Metodología Octave Allegro.

Figura 3

Hoja de ruta de Octave Allegro.



Fuente: Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.

1.2.3.3 Metodología CORAS

El Método CORAS (Construc a plataforn for Risk Analysis of Security critical system) proporciona la gestión de riesgos de seguridad basado en modelos, y fue desarrollada por el grupo de investigación Noruego SINTEF (Stiftelsen for industriell og teknisk forskning) en el año 2001.

CORAS proporciona un lenguaje personalizado para el modelado de amenazas y riesgos, y viene con pautas detalladas que explican cómo se debe usar el lenguaje para capturar y modelar información relevante durante las diversas etapas del análisis de seguridad. En este sentido, CORAS se basa en modelos. (CORAS, 2020).

CORAS proporciona múltiples artefactos para análisis de riesgos:

- El lenguaje CORAS, es un lenguaje de modelado gráfico para la comunicación, documentación y análisis de escenarios de riesgos y amenazas de seguridad. (CORAS, 2020).
- Lenguaje de Modelado Unificado (UML), utilizado para realizar el modelado del objetivo de análisis (activos de información, amenazas, riesgos y salvaguardas).
- Diagramas CORAS, usado para documentar los resultados intermedios y conclusiones finales.

El método CORAS divide la gestión de riesgos en ocho pasos; los cuatro (4) primeros, están referidos a conocer el entorno y la comprensión del objetivo; los cuatro (4) restantes, están dedicados a realizar un análisis detallado de los riesgos, evaluación y posibles tratamientos.

Paso 1, Preparación para el análisis: obtención de información inicial para establecer una idea básica del objetivo, alcance y enfoque, para que el equipo de análisis desarrolle los preparativos necesarios.

Paso 2, Reunión introductoria con el cliente: permite lograr una comprensión común con los representantes del cliente, respecto al objetivo de análisis, enfoque y alcance; por lo que, se recopilará información basada en las presentaciones y discusiones con el cliente.

Paso 3, Refinar la descripción del objetivo utilizando diagramas de activos: permite obtener la comprensión correcta y refinada del objetivo del cliente, mediante el análisis y discusión de la presentación del objetivo

tal como lo entienden los analistas, la identificación de activos y el análisis de riesgos de alto nivel.

Paso 4, Aprobación de la descripción del objetivo: el cliente debe aprobar la documentación completa vinculada al objetivo del análisis, alcance y enfoque, así como, la escala de probabilidades, consecuencias y criterios de evaluación de riesgos.

Paso 5, Identificación de riesgos mediante diagramas de amenazas: se utiliza la lluvia de ideas estructurada, así como, el uso del lenguaje CORAS, para la identificación de riesgos, amenazas, incidentes no deseados, escenarios de amenazas y vulnerabilidades con respecto a los activos identificados.

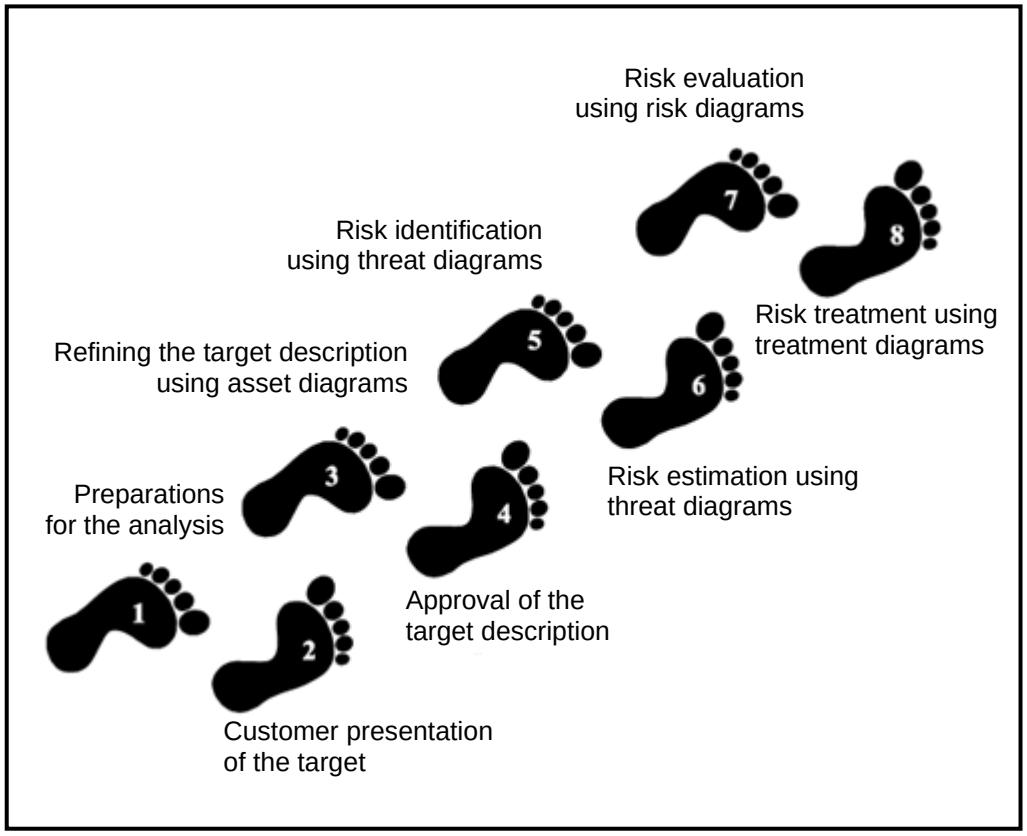
Paso 6, Estimación del riesgo mediante diagramas de amenazas: uso de diagramas de amenazas para estimar las probabilidades y las consecuencias.

Paso 7, Evaluación de riesgos mediante diagramas de riesgos: permite identificar los riesgos aceptables que deben ser pasibles de tratamientos, así como, los criterios de estimación y evaluación de riesgos respecto a los activos indirectos.

Paso 8, Tratamiento de riesgo utilizando diagramas de tratamiento: escenario vinculado a la identificación y análisis de tratamiento de riesgos, así como, la evaluación del costo - beneficio de los tratamientos.

Figura 4

Los ocho pasos del Método CORAS.



Fuente: obtenido de http://coras.sourceforge.net/index.html

1.2.3.4 Metodología Mehari

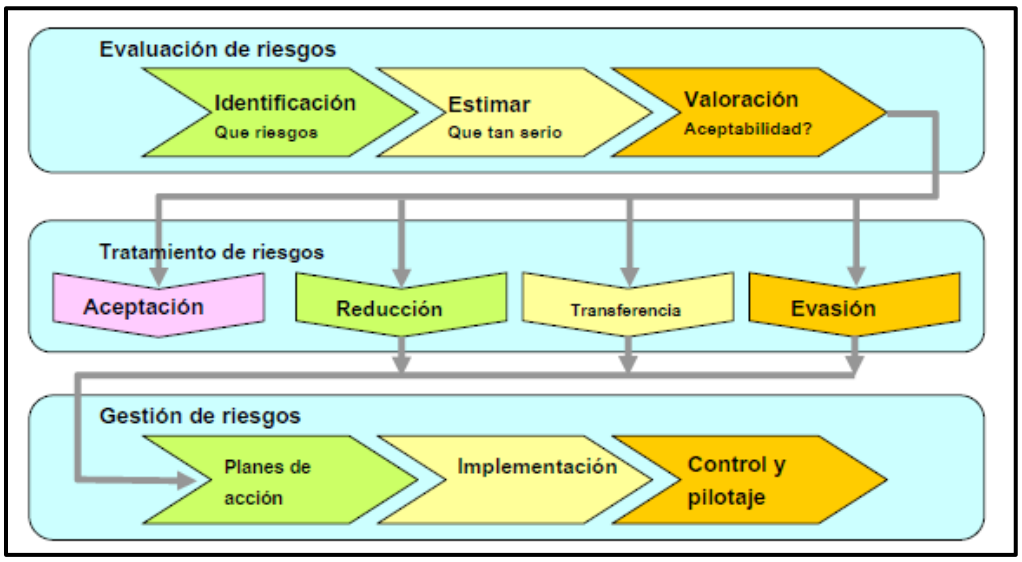
Mehari es una metodología para la evaluación y gestión de riesgos asociados a la información y sus tratamientos. Mehari es Open Source y gratuita, desarrollada y actualizada desde 1996 por CLUSIF y CLUSIQ.

Mehari cumple con las directrices establecidas por la norma ISO 27005: 2011, alineada a su vez con la ISO 31000, y permite la integración perfecta del riesgo en un proceso ISMS de ISO 27001: 2013, gracias a la participación de la dirección y la conciencia de los usuarios, partes interesadas y gerentes de operaciones. (MEHARIPEDIA, 2017).

En ese contexto, plantea la capacidad para evaluar riesgos actuales y futuros en base a una base de datos experta de conocimientos que permitirá evaluar el estado de los servicios de seguridad.

Figura 5

Enfoque Mehari.



Fuente: Mehari - Guía de análisis y tratamiento de riesgo.

El diagrama anterior muestra las tres (3) fases principales, las dos (2) primeras consisten en la evaluación de riesgos y el desarrollo de planes de tratamiento de riesgos correspondientes a la parte de planificación (plan) de ISO / IEC 27001 y una fase de implementación, cuyos aspectos son: hacer (“do”), control (“check”), y finalmente mejora y posible corrección (“act”) (Jouas, y otros, 2017).

En ese contexto, se describen cada una de las fases y sus componentes:

1. **Evaluación de riesgos**

   a) **Identificación de riesgos**: permite determinar situaciones que presentan ciertos tipos de riesgos, para caracterizarlos con suficiente precisión y que permitan estimar su gravedad; en ese contexto, se describen los elementos presentes en los riesgos:

      Activo: principales objetos del riesgo, susceptibles de algún daño en particular, en tal sentido, las consecuencias y gravedad del riesgo depende de la naturaleza del activo.

      Los principales activos se describirán según las categorías de servicios, datos y procesos de gestión y, dentro de cada categoría, según los tipos correspondientes a las necesidades funcionales. (MEHARI 2010 - Conceptos fundamentales y especificaciones funcionales, 2010).

      Vulnerabilidad intrínseca del activo dañado: definida en términos de procesos de seguridad y sus posibles deficiencias o fallas que podrían ser aprovechadas por una amenaza; en tal sentido, deben identificarse.

      El daño del activo: cada riesgo identificado debe especificar el tipo de daño al activo, en determinados casos se especificará en función de la disponibilidad, integridad o confidencialidad o de acuerdo a criterios de consecuencia.

- **La amenaza:** no puede existir riesgo sin causa que explote una vulnerabilidad intrínseca, en consecuencia, se deberá tener en consideración lo siguiente:

    - El evento que origina el riesgo que ocurre: se presenta en tres (3) categorías (accidentes, errores y actos voluntarios o maliciosos); asimismo, dentro de las mismas, estos pueden ser internas o externas a la entidad, así como, materiales o inmateriales.

    - Si este evento es voluntario o accidental.

    - El actor: si las amenazas son originadas por personas, es importante distinguir las categorías de las personas de acuerdo con sus derechos y privilegios. (MEHARI 2010 - Conceptos fundamentales y especificaciones funcionales, 2010).

    - Las circunstancias en que ocurre este evento: las circunstancias pueden incluir los siguientes factores: procesos o pasos del proceso, ubicación y tiempo.

Asimismo, para el proceso de identificación de riesgos presenta los siguientes pasos:

- Listado de los elementos característicos de los riesgos.

- Enumerar los riesgos que son teóricamente posibles.
- Desarrollar una base de conocimientos de riesgos típicos.
- Seleccionar riesgos a tener en cuenta.

b) Estimando riesgos: tiene como objetivo estimar la gravedad de cada riesgo previamente identificado, teniendo en cuenta las diferentes medidas de seguridad implementadas. (MEHARI 2010 - Conceptos fundamentales y especificaciones funcionales, 2010).

En ese sentido, es de vital importancia definir y estimar la seriedad intrínseca y residual del riesgo.

El riesgo se mide en base al grado de seriedad de las consecuencias (impacto) y la probabilidad de ocurrencia.

El impacto intrínseco de un riesgo se define por el máximo nivel de consecuencia en el que puede incurrir la organización, en ausencia de cualquier medida de seguridad diseñada específicamente para reducir estas consecuencias. (MEHARI 2010 - Conceptos fundamentales y especificaciones funcionales, 2010).

El proceso de estimación de riesgos consiste en dos (2) fases: la estratégica, que implica definir referencias de evaluación y bases de conocimiento y la fase más operativa, que implica estimar los

riesgos de acuerdo a la base de conocimientos y las referencias definidas anteriormente.

c) **Valoración de riesgos:** evaluado en función de la probabilidad e impacto, sin embargo, no es solo un simple cálculo matemático basado en estos dos (2) valores, sino, más bien, es un juicio sobre la aceptabilidad (o inaceptabilidad) de la situación; por lo que, es esencial desarrollar una tabla de decisiones que garantice la coherencia entre las decisiones tomadas en diferentes momentos. (MEHARI 2010 - Conceptos fundamentales y especificaciones funcionales, 2010).

2. **Tratamientos de riesgos:** se plantean cuatro (4) opciones de tratamiento de riesgos.

a) **Retener el riesgo:** significa aceptar la situación del riesgo sin hacer nada para cambiar dicha situación.

b) **Reduciendo el riesgo:** significa reducir la probabilidad o el impacto, o ambos simultáneamente, mediante la implementación de medidas de seguridad, en ese sentido, se plantean tener en consideración lo siguiente:

- Servicios de seguridad relevantes: tener en cuenta que el proceso de toma de decisiones debe tener en cuenta una base de conocimientos que debe considerar:

    - Una lista de los servicios de seguridad.

- El propósito (u objetivos) de cada servicio.
- Los mecanismos técnicos y organizativos que pueden preverse para implementar el servicio.

- Elegir el nivel de calidad objetivo para el servicio de seguridad que se implementara.
- Evaluación del efecto combinado de múltiples servicios de seguridad.
- Proceso de toma de decisiones para reducir los riesgos.

c) Transfiriendo el riesgo: significa observar el riesgo desde un punto de vista financiero desde un tercero.

d) Evitando el riesgo: establece parámetros de descripción detallada del escenario del riesgo para cambiar estos parámetros.

3. Gestión de riesgos: la gestión de riesgos involucra todos los procesos que facilitan la implementación de las decisiones previamente tomadas con respecto al tratamiento de riesgos, el monitoreo del efecto de estas decisiones y su mejora. (MEHARI 2010 - Conceptos fundamentales y especificaciones funcionales, 2010).

a) Desarrollar planes de acción: los planes de acción deben desarrollarse de acuerdo con los siguientes pasos:

- Elección de objetivos prioritarios y optimización.
- Elección de soluciones: mecanismos organizativos y técnicos.

- Elegir medidas estructurales y medidas para evitar riesgos.

b) Seguimiento y dirección de la gestión directa de riesgos: aplicar verificaciones directas de los riesgos, para ello se plantea lo siguiente:

- Verificar la calidad del servicio.
- Verificar la implementación de los servicios de seguridad.
- Dirección general para la gestión directa de los riesgos.

1.2.4 Análisis de Riesgos Informáticos.

El análisis de riesgos tiene como propósito determinar los componentes de un sistema que requiera protección, así como, determinar las vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar el grado de riesgo e impacto en la organización.

1.2.4.1 Amenazas.

"Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema, en el caso de la seguridad informática, los elementos de información. Debido a que la seguridad informática tiene como propósito la de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones, las amenazas y los consecuentes daños que puede causar un evento exitoso, también hay que ver en relación con la confidencialidad, integridad, disponibilidad y autenticidad de los datos e informaciones." (Markus Erb, "s.f.", http://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/).

Por lo que, se entiende como amenaza a una condición del entorno del sistema de información que, dada una oportunidad, podría dar lugar a que se produjese una violación de seguridad.

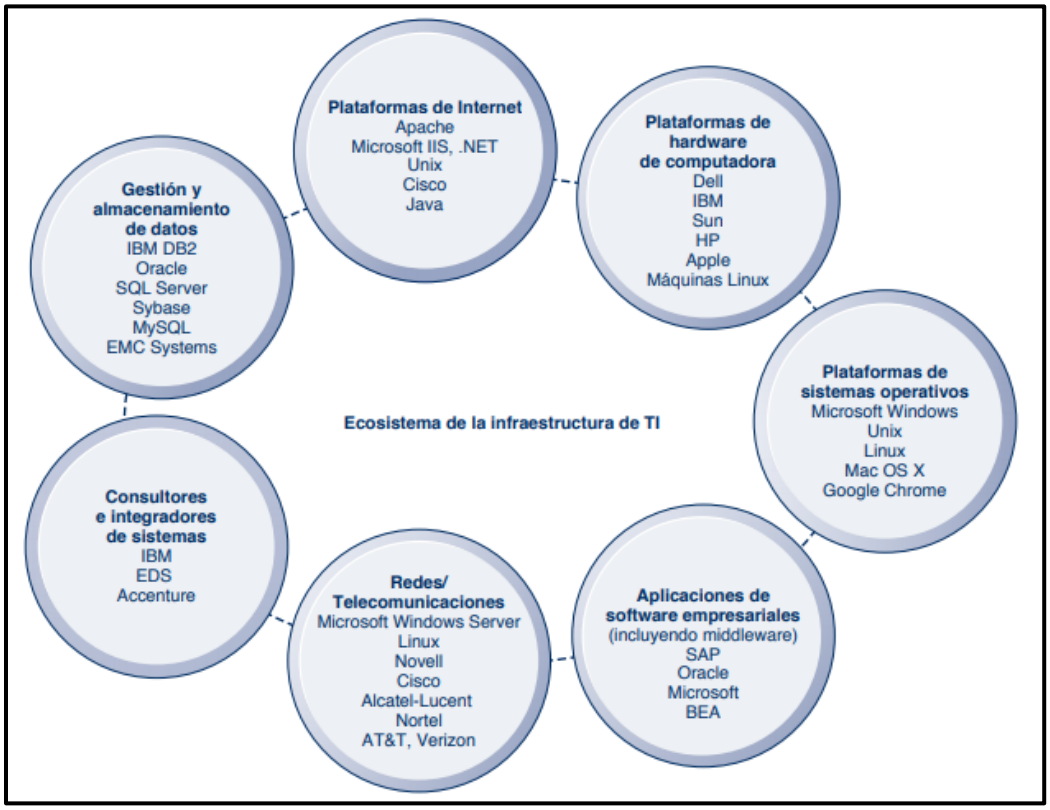
1.2.4.2 Infraestructuras tecnológicas.

La infraestructura tecnológica de las que disponen las organizaciones, se clasifica en: hardware, software, redes de comunicaciones.; y que según Laudon & Laudon (2012), el ecosistema de la infraestructura tecnológica básicamente está compuesto por siete (7) componentes principales:

- Plataformas de hardware de computadoras.
- Plataformas de sistemas operativos.
- Aplicaciones de software empresariales.
- Redes / telecomunicaciones.
- Integradores de sistemas.
- Gestión y almacenamiento de datos.
- Plataformas de internet.

Figura 6

Ecosistema de la infraestructura de TI.



Fuente: Sistemas de Información Gerencial.

1.2.5 Método de Estudio de Similitudes entre modelos y Estándares (MSSS)

Método desarrollado a través de un "análisis exhaustivo de diferentes estudios disponibles sobre mapeo de estándares y modelos, que proporcionan los pasos mínimos para encontrar las similitudes entre modelos y criterios" (Gasca Hurtado, 2010) establecidos dentro del ámbito de la investigación.

Propuesto por el grupo de investigación de la Universidad Politécnica de Madrid (MPSEI) y validado por distintos autores en distintas áreas de investigación para la realización de comparaciones formales (Calvo-Manzano, Cuevas Augustin, San Feliu Gilabert, & Muñoz, 2008).

El método MSSS está compuesto por los siguientes pasos:

- Seleccionar estándares y modelos.
- Elegir modelo de referencia.
- Seleccionar los procesos a analizar.
- Establecer el nivel de detalle del análisis.
- Definir una plantilla de comparación.
- Identificar similitudes.
- Recoger resultados.

1.3 Definiciones conceptuales

- **Activos de información:** se refiere a cualquier información o elemento que genera valor para la organización y que sea susceptible de ser afectado por riesgos de tecnologías de información, relacionado con software, hardware, datos, soportes, redes y comunicaciones.

- **Control:** es una medida que modifica el riesgo. Utilizado como sinónimo de salvaguarda o contramedida.

- **Directriz:** es una descripción que clarifica qué debería ser hecho y cómo para una adecuada gestión de riesgos de tecnologías de información, con el propósito de alcanzar los objetivos establecidos en las políticas.

1.4 Formulación del problema

No se ha determinado una metodología de gestión de riesgos de tecnologías de la información de acuerdo al marco de la NTP - ISO/IEC 27001:2014.

1.5 Objetivos

1.5.1 Objetivo general

Realizar un estudio analítico y crítico desde el punto de vista de la gestión de riesgos de tecnologías de la información en el marco de la NTP - ISO/IEC 27001:2014.

1.5.2 Objetivos específicos

- Analizar metodologías de gestión de riesgos de tecnologías de la información.
- Disminuir la incertidumbre en la selección de metodologías de gestión de riesgos de tecnologías de información en el marco de la NTP – ISO/IEC 27001:2014.
- Especificar una metodología de madurez en gestión de riesgos de tecnologías de información que mejor se relacione con la NTP – ISO/IEC 27001:2014.

1.6 Justificación

1.6.1 Implicancia práctica

Se plantea esta investigación, porque existe la necesidad de mejorar la selección de una metodología de gestión de riesgos de tecnologías de la información en el marco de la NTP - ISO/IEC 27001:2014 para las instituciones públicas peruanas.

1.6.2 Utilidad metodológica

La investigación usa métodos formales para comparar metodologías de gestión de riesgos de tecnologías de la información, y que, una vez se demuestre la fiabilidad en el uso de los métodos y herramientas, estos podrán ser usados por

otros investigadores para la selección de estándares y/ metodologías de madurez en el marco de la transformación digital del estado peruano.

Capitulo II: Métodos y Materiales

2.1 Metodología de la investigación

2.1.1 Tipo de investigación

2.1.1.1 Según su alcance

Descriptiva: la investigación analizará varias metodologías de gestión de riesgos de tecnologías de la información, para realizar una comparación basada en un método y determinar la mejor metodología que se relacione con la NTP-ISO 27001/IEC: 2014.

2.1.1.2 Según el propósito

Aplicada: utilización de conocimientos adquiridos en el desarrollo y dominio profesional, para identificar, evaluar y desarrollar los mecanismos para la resolución del problema planteado en la investigación, articulándose de forma metódica, práctica y concreta.

2.1.1.3 Según la naturaleza de la información que se recoge para responder al problema de investigación.

Investigación cualitativa: se analizará información mediante una perspectiva holística, multi-metódica e interpretativa, enfocada en comprender el objeto de estudio, bajo un contexto documental, con la finalidad de conocer la materia bajo investigación y obtener datos descriptivos, que permitan generar soluciones prácticas.

2.1.2 Diseño metodológico.

La investigación se realizará bajo el diseño de teoría fundamentada de tipo emergente, para lo cual se diseñaron procedimientos que guiaran el desarrollo de la investigación, con el propósito de establecer las condiciones para un mejor análisis y presentación de los resultados; en ese contexto, se establecieron los siguientes procedimientos:

- **Identificación del problema.**

  De la revisión y análisis de la Norma Técnica Peruana NTP-ISO 27001/IEC: 2014, se evidenció la ausencia de una metodología que permita gestionar los riesgos de tecnologías de información en las entidades del estado, por lo que, en esta investigación se plantea identificar una metodología que mejor se relacione con la norma antes mencionada.

- **Análisis de la Norma Técnica Peruana NTP-ISO 27001/IEC:2014 y factores de riesgos.**

  Se analizará Norma Técnica Peruana NTP-ISO 27001/IEC:2014 con la finalidad de identificar los aspectos y características significas para la gestión de riesgos de tecnologías de información; asimismo, su relación con las acciones y mecanismos de control definidos en la referida norma, del mismo modo, se identificarán los factores externos e internos generadores de riesgos en las entidades públicas y su vínculo con las tecnologías de información.

- **Elección del método comparativo.**

Se identificará un método comparativo formal que permita cotejar las diversas metodologías vinculadas a la gestión de riesgos de tecnologías de la información, por lo que, para su selección, se utilizaran aquellos métodos que hayan sido validados en investigaciones internacionales; no obstante, al ser las investigaciones únicas en su contexto y alcance, se realizará una adaptación del método seleccionado, lo que permitirá adoptar y fijar los procedimientos formales de comparación.

  - **Adaptación de método comparativo**: permitirá contextualizar los procedimientos para la selección y comparación de las metodologías de gestión de riesgos de tecnologías de información; así como, la elección de metodología de madurez que se mejor se relacione con la Norma Técnica Peruana NTP-ISO 27001/IEC: 2014.

- **Categorización de la información.**

Esta sección desarrollará cada uno de los procedimientos del método comparativo adaptado.

  - **Desarrollo de los pasos del método comparativo seleccionado**: se desarrollarán los procedimientos de manera secuencial, de tal forma que, el flujo de información de salida de un procedimiento condiciona la entrada del siguiente.

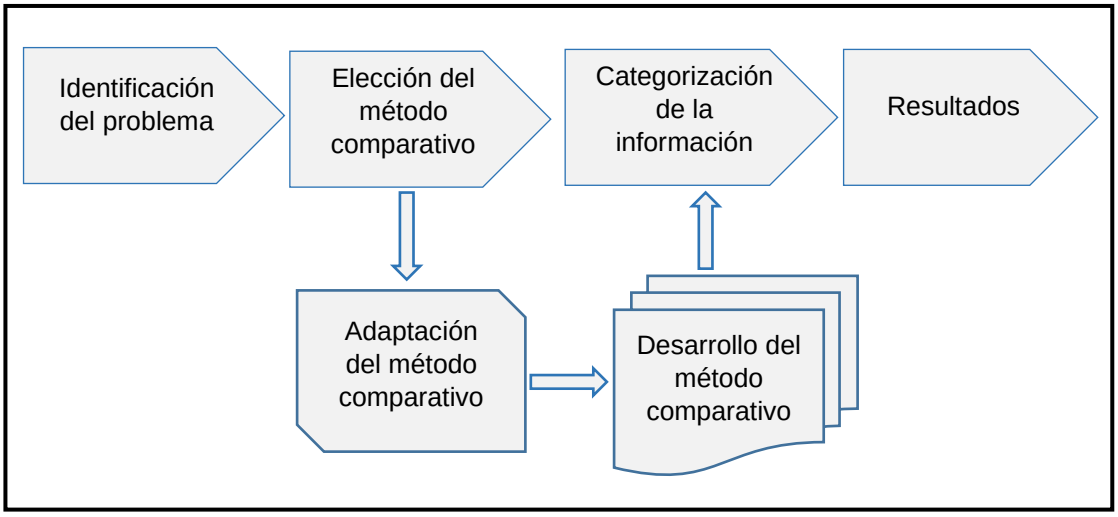
- **Discusión de resultados.**

Los resultados obtenidos se presentarán en tablas estructuradas, de tal forma, que se evidencien las características de las metodologías que más se relacionan con la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, así mismo, las carencias de cada una de ellas, para finalmente presentar la metodología que mejor se adapte a la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

En tal sentido, la investigación plantea un conjunto de procedimientos metodológicamente estructurados, conforme se puede observar en la figura n.° 7.

Figura n.° 7

Diseño metodológico de la investigación.



Fuente: Elaboración del autor.

2.2 Técnicas, Equipos y Materiales de recolección de datos

2.2.1 Técnicas

Esta investigación se basa en el análisis de fuentes tipo documental, que consisten en explorar, revisar y analizar estándares, métodos y metodologías registradas en libros, revistas científicas, publicaciones y demás textos escritos y digitales.

En ese contexto, se emplearán estrategias orientadas a establecer una revisión sistemática de las diversas fuentes de la investigación documental valiéndose de métodos establecidos en investigaciones científicas.

2.2.2 Equipos y materiales de recolección de datos

Se requerirán los siguientes equipos y materiales:

- Laptop
- Impresora
- Internet

Capitulo III: Desarrollo de la investigación

3.1 Análisis de la Norma Técnica Peruana NTP-ISO 27001/IEC:2014 y factores de riesgos.

En este apartado se analizaron los factores internos y externos que tienen vinculación directa con los riesgos a los cuales se encuentran expuestas las tecnologías de información y como la Norma Técnica Peruana NTP-ISO 27001/IEC:2014 los ha conceptualizado con el fin de generar mecanismos de control más apropiados.

3.1.1.1 Factor Humano en los riesgos de tecnologías de la información.

Se considera al personal como el eslabón más difícil en la seguridad de la información; y principal fuente de riesgo, al ser susceptible de ser engañado, manipulado, presionado, chantajeado o por propia iniciativa, para omitir, vulnerar y/o sabotear las políticas de seguridad de la organización.

El uso de las mejores herramientas de hardware, software, metodologías, políticas de seguridad de la información; no garantizan el control y gestión de riesgos de TI, porque estas por sí solas no funcionan; ya que, es necesario el compromiso y colaboración del personal de la organización; así mismo, diversas investigaciones han evidenciado que muchos de los incidentes informáticos tienen su origen en el factor humano, ocasionado generalmente por falta de conocimientos vinculados a riesgos de tecnologías de información, asimismo, por la ausencia del monitoreo de las medidas de seguridad de la información.

Proteger los activos de la organización mediante la seguridad de la información y una adecuada gestión de riesgos de TI, es responsabilidad de todo el personal de la institución pública, independiente de los niveles de responsabilidad y cargos que ejerzan en la organización; así podemos mencionar a:

- Empleados.
- Directivos.
- Administradores.
- Consultores.
- Técnicos.
- Programadores.
- Personal auxiliar.
- Usuarios de sistemas.
- Personal externo.

La gestión de riesgos de tecnologías de información implica considerar al factor humano como uno de los elementos clave, por lo que es necesario contemplar aspectos vinculados a la formación y concientización de los empleados públicos de todos los niveles, que incluya a directivos y/o gerentes.

3.1.1.2 Factor económico en los riesgos de tecnologías de la información.

Los recursos económicos en el estado siempre son escasos, por lo que implementar políticas para minimizar los riesgos de tecnologías de la información y aumentar el nivel de seguridad, se necesitará destinar una

partida económica de los pocos recursos económicos de los que disponen las instituciones públicas, por lo que, es necesario realizar un balance entre el costo de la implementación de controles contra los beneficios de las mismas; teniendo en cuenta que, en las instituciones públicas los principales afectados de la mala gestión de riesgos de TI serían los servicios destinados a los ciudadanos.

Por lo que, la metodología de gestión de riesgos de tecnologías de información debe considerar valorar las dimensiones (de seguridad) que interesan de un activo, incluyendo la cuantificación de la afectación al ciudadano. La valoración es la determinación del costo que supondría salir de una incidencia que afecta y/o destroza el activo.

Existen muchos factores vinculados a la afectación de los activos:

- Costo de reposición, adquisición e instalación.
- Costo de recuperación del valor del activo.
- Pérdida de ingresos vinculado al servicio o bien afectado.
- Disminución de la confianza de los usuarios y ciudadanos que se traduce en desprestigio institucional.
- Sanciones por incumplimiento de la ley u obligaciones contractuales.
- Daño a otros activos, propios o ajenos.
- Daño a personas y/o empresas.
- Perjuicio a la reputación institucional.
- Daños medioambientales.

3.1.1.3 Cultura organizacional en los riesgos de tecnologías de información.

La cultura organizacional en las instituciones públicas está conformada por las formas en que las personas desarrollan sus actividades, los mecanismos de comunicación que utilizan para relacionarse entre ellos, las normas formales e informales que rigen en la organización y el comportamiento en la atención al ciudadano, llegando a modelar las creencias y valores compartidos, que identifican a cada institución.

Adicionalmente, no todas las instituciones públicas poseen las mismas herramientas tecnológicas, sin embargo, no existe entidad pública que no tenga al menos una herramienta de tecnología de información para el cumplimiento de sus objetivos, misión y visión; lo que vuelve aún más compleja la cultura organizacional.

No obstante, el contexto actual ha incrementado el uso de tecnologías de información en las instituciones públicas, siendo así que se han implementado mecanismos para el trabajo remoto, educación virtual, telemedicina, notificación electrónica, mesa de parte virtual, entre otras; con la finalidad de que los servicios públicos se encuentren disponibles para los servicios a la ciudadanía, sin las limitantes de tiempo y espacio geográfico, que de alguna u otra manera se verán reflejados en la cultura organizacional.

En ese sentido, independientemente del tipo de tecnología de información que utilicen las instituciones públicas, los riesgos vinculadas a ellas se han incrementado exponencialmente, debido a que los empleados han salido del espacio geográfico de la institución, las redes de comunicaciones se han expandido, se comparten recursos e información entre diferentes

dispositivos, se crean datos en dispositivos que no pertenecen a la institución; con la consecuente que muchos empleados los utilizan sin el mínimo conocimiento y/o capacitación necesaria.

Por lo que, entender la cultura organizacional en el marco del uso de tecnologías de la información, es compleja, más aún en el contexto actual, donde se requiere brindar la accesibilidad de los servicios a través de plataformas digitales, sin embargo, ¿cuál es nivel de seguridad que ofrecen? y ¿cuál es el umbral de lo permitido?

En este contexto, se hace evidente, que las instituciones públicas deben gestionar los riesgos de tecnologías de información teniendo en cuenta la cultura organizacional.

3.2 Elección del método comparativo

La existencia de diversas metodologías vinculadas a la gestión de riesgos de tecnologías de la información, dificulta la elección de una estas, por lo que, para su selección se aplicará una comparación utilizando mecanismos y métodos formales y validados en otras investigaciones; no obstante, al ser las investigaciones únicas, se realizará una adaptación del Método de Estudio de Similitud entre Modelos y Estándares (MSSS), método que permitirá establecer los procedimientos para seleccionar la metodología de acuerdo a la investigación planteada.

3.2.1 Adaptación del Método de Estudio de Similitudes entre modelos y Estándares (MSSS)

En este apartado se realizará la adaptación del método MSSS, que permitirá realizar un estudio comparativo estructurado, en función de los siete (7) pasos

generales propuestos por el grupo de investigación MPSEI de la Universidad Politécnica de Madrid; sin embargo, para esta investigación se adicionaron mecanismos de análisis en algunos de los pasos, que permitirán precisar la comparación en el ámbito de las metodologías relacionadas con riesgos de tecnologías de información, tal como se muestra en la tabla n.º 1

Tabla n.º 1

Comparación entre el método MSSS original y la adaptación del mismo.

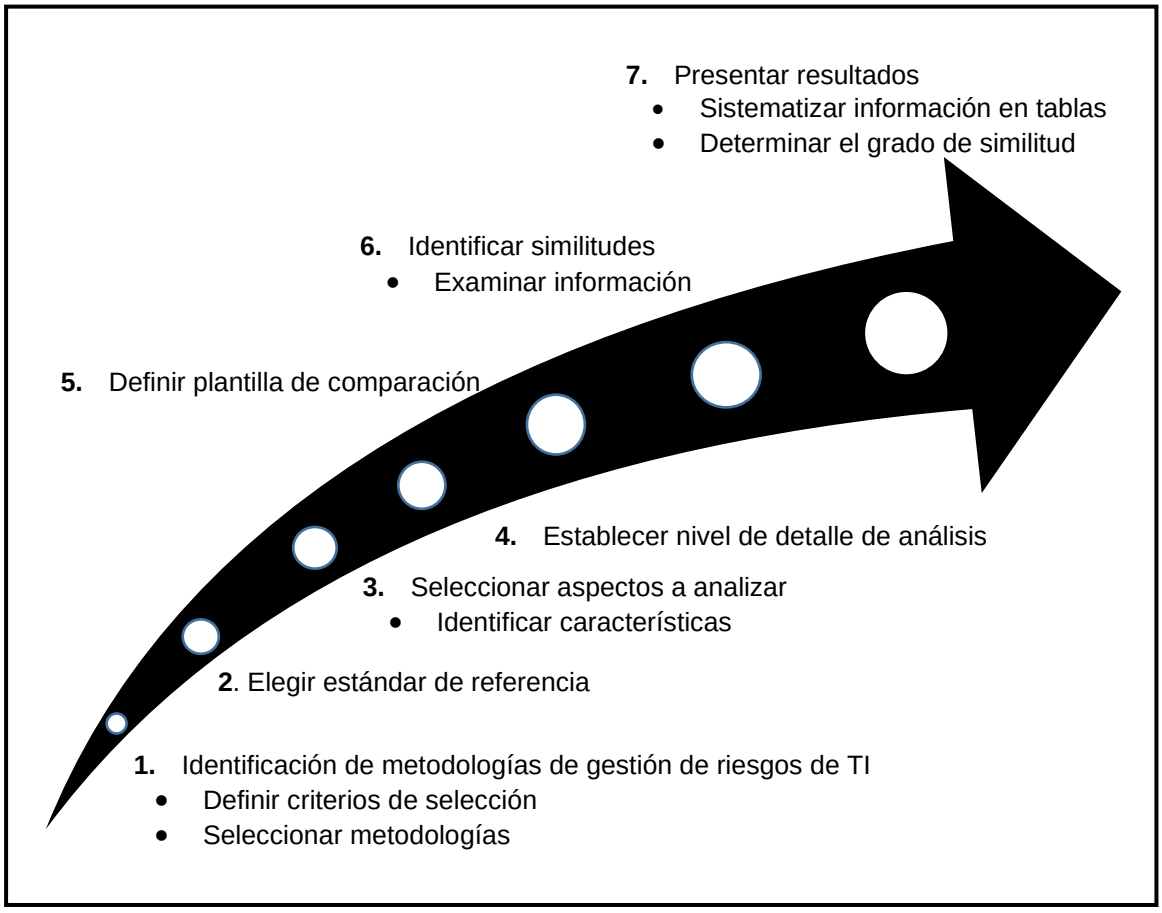
Método MSSS Original	Adaptación del Método MSSS
1. Seleccionar estándares y modelos.	**1.** Identificación de metodologías. • Definir criterios de selección. • Seleccionar metodologías.
2. Elegir modelo de referencia.	**2.** Elegir estándar de referencia.
3. Seleccionar los procesos a analizar.	**3.** Seleccionar aspectos a analizar. • Identificar características.
4. Establecer el nivel de detalle del análisis.	**4.** Establecer el nivel de detalle del análisis.
5. Definir una plantilla de comparación.	**5.** Definir una plantilla de comparación.
6. Identificar similitudes.	**6.** Identificar similitudes. • Examinar información.
7. Recoger resultados.	**7.** Presentar resultados. • Sistematizar información en tablas.

- Determinar el grado de similitud.

Fuente: Adaptación del Método MSSS propuesto por el grupo de investigación MPSEI de la Universidad Politécnica de Madrid.

Figura 8

Fases de la adaptación del Método MSSS.



Fuente: Elaboración del autor.

3.3 Categorización de la información

Se seleccionarán y analizarán los aspectos comunes de las metodologías de gestión de riesgos de tecnologías de la información respecto a la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, aplicando métodos formales de comparación.

Esta sección desarrollara los sietes (7) pasos obtenidos de la adaptación del Método MSSS, los cuales se listan a continuación:

1- Identificación de metodologías de gestión de riesgos de TI.
2- Elegir el estándar de referencia.
3- Seleccionar aspectos a analizar.
4- Establecer nivel de detalle del análisis.
5- Definir plantilla de comparación.
6- Identificar similitudes.
7- Presentar resultados.

3.3.1 Identificación de metodologías de gestión de riesgos de TI

Actualmente existen diversas metodologías de gestión riesgos de tecnologías de información disponibles para el análisis e implementación para el sector público o privado, que han sido diseñadas por organismos gubernamentales, sectores privados y/o en colaboración de ambos; con muchos años de vigencia en el mercado y que han sido implementadas en una gran variedad de empresas de distintos sectores con resultados positivos, lo que les ha valido un reconocimiento internacional en la administración de riesgos de activos de información.

En ese sentido, al ser la NTP - ISO/IEC 27001:2014, una norma principalmente para entidades estatales peruanas; las metodologías de gestión riesgos de tecnologías de información seleccionadas deben tener un enfoque relacionado a entidades gubernamentales, con documentación oficial disponible, vigente y suficiente, que permita a los gestores de riesgos una correcta implementación y administración.

Por otro lado, las entidades públicas generalmente carecen de presupuestos; un factor muy limitante en el aparato estatal, que indefectiblemente será un indicador para identificar metodologías de gestión de riesgos de tecnologías de información vinculados a los derechos de autor en el uso de las metodologías y/o documentación de las mismas.

Adicionalmente, para que una metodología de gestión de riesgos de tecnologías de información sea seleccionada, esta investigación ha establecido un conjunto de criterios, relacionados a documentación oficial, accesibilidad a la documentación, herramientas de análisis de riesgos, vigencia en el mercado, aplicable al sector estatal y tener reconocimiento internacional. Los criterios anteriormente indicados, permitirán sentar las bases y condiciones para las búsqueda e identificación de metodologías en la presente investigación.

Tabla n.º 2

Criterios para la selección de metodologías.

Ítems	Criterios de Selección
1	Documentación oficial.
2	Accesibilidad a documentación.
3	Herramientas de análisis de riesgos.
4	Vigencia.
5	Aplicable al sector estatal.
6	Nivel de reconocimiento.

Fuente: Elaboración del autor.

Las características para cada uno de los criterios de selección, se describen a continuación:

Documentación oficial: se refiere a información digital o impresa sobre manuales, guías, libros, investigaciones y otros documentos publicados por las entidades, organizaciones y sectores creadores de la metodología, donde se especifican las características, fases, métodos, herramientas, mecanismos u otros aspectos propios de cada metodología.

Accesibilidad a documentación: se refiere a que tan asequible y disponible se encuentra la documentación oficial de la metodología de gestión de riesgos de tecnología de información, identificando las restricciones y limitaciones de uso.

Herramientas de análisis de riesgos: se refiere a que la metodología de gestión de riesgos de tecnología de información posea herramientas para el análisis y evaluación de riesgos de tecnologías de información, para facilitar las tareas y la toma de decisiones del personal de TI.

Es necesario que las herramientas de análisis de riesgos sean de libre uso, en caso de ser herramientas empaquetadas (software privativo), por lo menos deben permitir el uso en una versión básica o de prueba.

Vigencia: se refiere a la validez de la metodología de gestión de riesgos de tecnología de información, en función al tiempo de la última actualización.

Aplicable al sector estatal: se analizarán las metodologías de gestión de riesgos de tecnología de información para determinar si poseen un enfoque gubernamental.

Nivel de reconocimiento: se refiere al nivel de expansión, prestigio y uso que ha alcanzado la metodología durante su vigencia en el mercado.

En tal sentido, en el periodo del 10 de junio al 20 de octubre del 2020, se realizó una búsqueda e identificación de metodologías vinculadas a la gestión de riesgos de tecnologías de información, en internet y materiales bibliográficos, identificándose a siete (7) metodologías, las cuales se detallan a continuación:

- Metodología Magerit v3.
- Estándar Australiano AS/NZS 4360.
- Metodología CORAS.
- Metodología CRAMM.
- Metodología MEHARI.
- Metodología NIST 800-300.
- Metodología Octave Allegro.

Las metodologías anteriormente indicadas, fueron analizadas de acuerdo a los criterios propuestos en esta investigación; conforme al siguiente detalle:

1) **Metodología Magerit V3:**

   a) **Documentación oficial:** metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Ministerio de Hacienda y Administraciones públicas del Gobierno Español, actualmente se encuentra en la versión 3, y ofrece una metodología sistemática para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones.

      Presenta 3 libros oficiales, en idiomas español, inglés e italiano; que han sido creados y editados por el Ministerio de hacienda y

Administraciones públicas del Gobierno Español, y publicados en el portal de administración electrónica del gobierno español.

- Libro I: Método
- Libro II: Catálogos de elementos
- Libro III: Guía de técnicas

b) **Accesibilidad de información:** la documentación oficial puede ser descargada libremente a través del portal de administración electrónica del gobierno español, en el siguiente enlace web: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

c) **Herramienta de análisis de riesgos:** la metodología Magerit V3 presenta las herramientas EAR (Entornos de Análisis de Riesgos) que facilitan el análisis y la gestión de riesgos de un sistema de información. Estas herramientas han sido creadas por el Centro Criptográfico Nacional (CCN-CERT).

Asimismo, se actualizan periódicamente y existen diversas variantes:

Pilar: Versión íntegra de la herramienta.

Pilar Basic: Versión sencilla para Pymes y administración local.

Upilar: Versión de Pilar reducida, destinada a la realización de análisis de riesgos muy rápidos.

RMAT (Risk Management Additional Tools):

Personalización de herramientas. (CCN - CERT, 2020)

Estas herramientas están disponibles para libre descarga desde la página web oficial CCN-CERT, con un periodo de evaluación por 30 días.

d) **Vigencia:** la metodología se utiliza actualmente en muchas organizaciones públicas y privadas, principalmente de Europa y Latinoamérica.

e) **Aplicable al sector estatal:** la metodología ha sido elaborada bajo un contexto gubernamental, no obstante, también es aplicable para Pymes.

f) **Nivel de reconocimiento:** internacional.

2) **Estándar Australiano AS/NZS 4360**

a) **Documentación oficial:** metodología de gestión de riesgos de tecnologías de información que proporciona una "guía genérica para el establecimiento e implementación el proceso de administración de riesgos involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos" (EDESA, 2020).

Presenta la guía AS/NZS 4360:1999 Risk Management, publicada por la Standards Association of Australia (Standards New Zealand, 2020).

b) **Accesibilidad de información:** no es de libre uso. Para acceder a la guía AS/NZS 4360:1999 Risk Management, se tiene que comprar licencia de uso a la Standards New Zealand.

c) **Herramienta de Análisis de riesgos:** no presenta herramienta asociada.

d) **Vigencia:** no se encuentra vigente, ha sido reemplazada por AS/NZS 31000:2018, que gestiona todo tipo de riesgos a nivel de organización. Es una metodología de gestión de riesgos basada en ISO 31000, para evaluar riesgos a nivel organizacional.

e) **Aplicable al sector estatal:** aplicable a cualquier tipo de organización.

f) **Nivel de reconocimiento:** internacional.

3) **Metodología CORAS**

a) **Documentación oficial:** metodología de análisis de riesgo de seguridad, que "proporciona un lenguaje personalizado para el modelado de amenazas y riesgos, y viene con pautas detalladas que explican cómo se debe usar el lenguaje para capturar y modelar información relevante durante las diversas etapas del análisis de seguridad" (CORAS, 2020).

Presenta la Guía oficial del método CORAS, descargable de forma gratuita a través de portal web CORAS http://coras.sourceforge.net/index.html.

b) **Accesibilidad de información:** la descarga de la documentación oficial es libre.

c) **Herramienta de Análisis de riesgos:** presenta la herramienta CORAS V1.1, de uso libre y gratuito, descargable desde el portal web CORAS.

La herramienta está diseñada para admitir el modelado sobre la marcha utilizando todo tipo de diagramas CORAS.

d) **Vigencia:** Hasta la fecha se mantiene vigente.

e) **Aplicable al sector estatal:** Aplicable a cualquier tipo de organización.

f) **Nivel de reconocimiento:** Internacional.

4) CRAMM (CCTA Risk Analysis and Management Method)

a) **Documentación oficial:** metodología de gestión de riesgos, desarrollado por la organización gubernamental británica CCTA (Agencia Central de Comunicaciones y Telecomunicaciones) del gobierno del Reino Unido. Es una metodología estructurada y completa, que cubre los riesgos desde el análisis, contramedidas, resultados, documentación de seguridad, costo y planificación de emergencia y continuidad de negocio.

Presenta la guía de administración CRAMM **(**Management Guide for CRAMM).

b) **Accesibilidad de información:** la documentación oficial no es de libre descarga y uso. Actualmente se puede adquirir desde el portal web de la Agencia de la Unión Europea para la Seguridad Cibernética (ENISA).

En la actualidad el sitio web oficial: http://www.cramm.com, ya no se encuentra disponible.

c) **Herramienta de análisis de riesgos:** CRAMM incluye una amplia gama de herramientas de evaluación de riesgos, y que son totalmente compatibles con la ISO 27001, las cuales se ocupan de tareas como:

- Activos de modelado de dependencia.
- Evaluación de impacto empresarial.
- Identificación y evaluación de amenazas y vulnerabilidades.
- Evaluar los niveles de riesgo.
- La identificación de los controles necesarios y justificados sobre la base de la evaluación del riesgo.
- Un enfoque flexible para la evaluación de riesgos.

En ese sentido, presenta la herramienta de software CRAMM. Esta herramienta permite la recopilación de datos, análisis, calculo y presentación de informes de gestión de riesgos, siendo así, que a nivel de informes permite presentar tres (3) tipos: Análisis Experto CRAMM, análisis Expresss CRAMM y Análisis BS7799.

Todas las herramientas son de uso comercial.

d) **Vigencia:** la metodología es utilizada actualmente en muchas organizaciones públicas y privadas, principalmente de Europa.

e) **Aplicable al sector estatal:** aplicable al sector gubernamental y a grandes corporaciones.

f) **Nivel de reconocimiento:** internacional.

5) **MEHARI (CCTA Risk Analysis and Management Method)**

a) **Documentación oficial:** metodología de gestión de riesgos desarrollada por CLUSIQ y CLUSIF (Club de seguridad de información francesa).

La metodología Mehari integra documentación, herramientas y bases de datos de conocimientos, para analizar de manera cuantitativa y cualitativa los factores de riesgos, amenazas y vulnerabilidades.

Presenta la siguiente documentación:

- Estándar MEHARI - Guía para la gestión de proyectos de seguridad.
- Mehari – Principios y especificaciones.
- Mehari – presentación general.
- Mehari - Guía para el análisis de problemas y la clasificación de activos.
- Mehari - Guía de diagnóstico de servicios de seguridad.
- Mehari - Análisis de riesgos y guía de tratamiento.

b) **Accesibilidad de información:** Mehari es una metodología de código abierto y gratuita que permite evaluar y gestionar los riesgos asociados con la información y su procesamiento (MEHARIPEDIA, 2017).

La documentación oficial puede ser descargada desde la web de Mehari:
http://meharipedia.x10host.com/wp/telechargements/document2/

c) **Herramienta de análisis de Riesgos:** Mehari integra herramientas y bases de datos de conocimiento utilizando Excel y Open Office;

asimismo, presenta el software RISICARE2 que permite realizar simulaciones y visualizaciones de casos.

d) **Vigencia:** la metodología se utiliza en todos los sectores, lo que incluye a organizaciones gubernamentales. Su uso se dio inicialmente en Europa, pero al día de hoy se ha extendido a más de 175 países a nivel mundial, incluido América del Sur.

e) **Aplicable al sector estatal:** aplicable al sector gubernamental y a todo tipo de sector.

f) **Nivel de reconocimiento:** internacional.

6) **Metodología NIST 800-300**

a) **Documentación oficial:** metodología de gestión de riesgos de los sistemas de tecnología de la información, elaborada por la National Institute of Standard Technology (Instituto Nacional de Estándares y Tecnología) de los Estados Unidos de Norteamérica. La metodología ha sido revisada y actualizada a NIST 800-300 REV 1, y tiene como propósito optimizar la administración del riesgo de los sistemas de información mediante evaluaciones de riesgos, llevadas a cabo en los tres (3) niveles en la jerarquía de gestión de riesgos, incluyendo un proceso general de gestión de riesgos, proporcionando a los líderes y/o ejecutivos de alto nivel, la información necesaria para determinar los cursos de acción adecuados en respuesta a los riesgos identificados (NIST, 2012).

Presenta la guía para realizar evaluaciones de riesgo (Guide for Conducting Risk Assessments) publicado por National Institute of

Standards and Tecnology del Departamento de comercio de los Estados Unidos.

b) **Accesibilidad de información:** la documentación oficial es de libre descarga desde el portal web https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

c) **Herramienta de SW:** la metodología no presenta herramienta de software asociada.

d) **Vigencia:** utilizada actualmente en muchas organizaciones federales de los Estados Unidos.

e) **Aplicable al sector estatal:** aplicable al sector gubernamental y otros sectores.

f) **Nivel de reconocimiento:** internacional.

7) **Octave Allegro**

a) **Documentación oficial:** metodología de gestión de riesgos de tecnologías de información que permite "racionalizar y optimizar el proceso de evaluación de riesgos de seguridad de la información para que una organización pueda obtener resultados suficientes con una pequeña inversión en tiempo, personas y otros recursos limitados" (Carnegie Mellon University, 2007).

Octave Allegro fue desarrollada por el Equipo de Respuesta a Emergencias Informáticas (CERT), dentro del programa de SEI (Software Engineering Institute).

Presenta el informe técnico Octave Allegro, que contiene la mejora del proceso de evaluación de riesgos de seguridad de la información.

b) **Accesibilidad de información:** la documentación oficial es de descarga gratuita a través de la página web: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419.

c) **Herramienta de análisis de riesgos:** presenta hojas de trabajo, para cada fase de los procesos que se analizan y que son utilizadas como entradas para el siguiente paso en el proceso.

d) **Vigencia:** metodología muy utilizada en Europa, principalmente en Reino Unido. Según un estudio realizado en el 2017 por Wisagate sobre uso de metodologías de seguridad, Octave Allegro y Nist 800-30, obtuvieron los primeros lugares.

e) **Aplicable al sector estatal:** aplicable a todo tipo de sector.

f) **Nivel de reconocimiento:** internacional.

Del análisis de las metodologías identificadas, se observa que todas presentan documentación oficial, generalmente mediante portales web oficiales; pero, solo algunas permiten el acceso a dicha documentación; sin embargo, todas poseen reconocimiento internacional y son aplicable a los sectores del estado. Cabe destacar que, de las metodologías analizadas, no todas poseen herramientas para el análisis, evaluación y/o monitoreo de riesgos; asimismo, algunas ya no están vigentes al momento de la presente investigación; tal como se puede observar en la

tabla n.º 3, donde se presentan las metodologías analizadas conforme a los criterios establecidos.

Tabla n.º 3

Metodologías de Gestión de riesgos de TI vs Criterios de selección.

	MAGERIT V3	**AS/NZS 4360**	**CORAS**	**CRAMM**	**MEHARI**	**NIST 800-30**	**OCTAVE ALLEGRO**
Documentación Oficial	SI	SI	SI	SI	SI	SI	SI
Accesibilidad de Documentación	SI	NO	SI	NO	SI	SI	SI
Herramienta de Análisis de riesgo	SI	NO	SI	SI	SI	NO	SI
Vigencia	SI	NO	SI	SI	SI	SI	SI
Aplicable al sector Estatal	SI	SI	SI	SI	SI	SI	SI
nivel de Reconocimiento	INTER	INTER	INTER	INTER	INTER	INTER	INTER

Nota: INTER, significa reconocimiento de la metodología a nivel internacional.

Fuente: Elaboración del autor.

El resultado del análisis permitió determinar las metodologías que finalmente se incorporaran al estudio de similitudes; siendo así, que solamente cuatro metodologías cumplen todos los criterios, tal como se visualiza en la tabla n.º 4, en tal sentido, serán estas las que posteriormente se compararán con Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

Tabla n.º 4

Selección de Metodologías para el estudio de similitudes.

	MAGERIT V3	CORAS	MEHARI	OCTAVE ALLEGRO
Documentación Oficial	SI	SI	SI	SI
Accesibilidad de Documentación	SI	SI	SI	SI
Herramienta de Análisis de riesgo	SI	SI	SI	SI
Vigencia	SI	SI	SI	SI
Aplicable al sector Estatal	SI	SI	SI	SI
nivel de Reconocimiento	INTER	INTER	INTER	INTER

Fuente: Elaboración del autor.

INTER significa internacional.

3.3.2 Elegir estándar de referencia

Para la investigación, el estándar de referencia es la Norma Técnica Peruana NTP-ISO/IEC 27001:2014. En función del estándar de referencia se comparan las metodologías de gestión de riesgos de tecnologías de información seleccionadas en el paso 1.

3.3.3 Seleccionar aspectos y características a analizar

La filosofía de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 está en asegurar a las organizaciones sobre incidentes relacionados a la seguridad de la información, entendiéndose que por naturaleza los activos de información de las entidades públicas se encuentran expuesta a errores, amenazas, vulnerabilidades, ataques, destrucción y otros mecanismos propios del uso. Es en ese sentido, la gestión de riesgos se vuelve un aspecto crucial para los activos de información.

La gestión de riesgos de tecnologías de información con relación a la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, implica determinar los aspectos principales, que permitan establecer las bases para una adecuada comparación con las metodologías de gestión de riesgos de tecnologías de información.

Analizada la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, se han determinado principalmente 10 aspectos fundamentales y 25 características esenciales, la cuales se encuentran explícitamente e implícitamente en la norma antes indicada.

A continuación, se presentan los 10 aspectos y 25 características seleccionadas:

1) Determinar el compromiso de la alta dirección.
    - Liderazgo y compromiso de la alta dirección.
    - Asignación de roles y responsabilidades.
    - Asignación de recursos.
    - Alineación de los objetivos con la estrategia de la organización.
2) Definir el alcance.

- Alcance.

3) Comprender el contexto de la organización.
   - Aspectos internos y externos.
   - Comprender las necesidades y expectativas de las partes interesadas.
4) Activos de información.
   - Identificar Activos de información.
   - Valoración de activos.
5) identificación de riesgos.
   - Establecer criterios de riesgos.
   - Identificación de propietarios de los riesgos.
   - Identificar amenazas y vulnerabilidades.
   - Identificar riesgos.
6) Evaluar el riesgo.
   - Valoración de consecuencias potenciales.
   - Valoración de probabilidad de ocurrencia.
   - Valoración del impacto.
7) Tratamiento del riesgo.
   - Opciones de tratamiento.
   - Determinación de controles.
8) Aplicabilidad de los controles.
   - Declaración de aplicabilidad.
9) monitoreo y mejora continua.
   - Monitoreo y evaluación.

- Auditorias.
- Mejora continua.

10) Concientización y comunicación.

- Concientización.
- Comunicación.
- Documentación.

En ese sentido, los criterios establecidos anteriormente se constituyen en las reglas para la comparación entre las metodologías de gestión de riesgos de tecnologías de información.

3.3.4 Establecer el nivel de detalle del análisis.

El nivel de detalle es un factor importante para determinar el nivel de profundidad del estudio, y para esta investigación, estará en función de las características establecidas por cada aspecto definido en el paso 3 de la adaptación del método MSSS.

Sobre la base del nivel de detalle, se procederá a identificar los aspectos y características presentes en cada metodología de gestión de riesgos de tecnologías de información, en correspondencia con la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

3.3.5 Definir plantillas de comparación.

Para esta investigación, una plantilla es un patrón estructurado y prediseñado, que proporcionara elementos para el análisis y comparación de contenidos.

En ese contexto, se han elaborado tres (3) plantillas, las cuales permitirán realizar el análisis, evaluación y comparación de cada uno de los aspectos y características de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, relacionadas con cada una de las metodologías seleccionadas previamente; con la finalidad de secuenciar los pasos para una correcta identificación de la metodología que presente una mayor similitud con la referida norma técnica.

A continuación, se describirán las plantillas elaboradas para esta investigación:

Plantilla n.º 01 - "Estudio de características y criterios": esta plantilla permitirá realizar un análisis descriptivo de cada uno de los 10 aspectos fundamentales y 21 características esenciales establecidos por la NTP-ISO/IEC 27001:2014, entre las metodologías participantes. La plantilla se ubica en el anexo n.º 01.

Plantilla n.º 02 - "Verificador de cumplimiento de características y criterios": esta plantilla presentara los resultados del análisis descriptivo registrados en la plantilla anterior, en el sentido, que registrará con un "Si", en caso la metodología cumpla con el aspecto o característica esencial de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, caso contrario, se registrará un "No". La plantilla se ubica en el anexo n.º 02.

Plantilla n.º 03 - "Comparador de características y criterios": esta plantilla recogerá y presentará los resultados globales de cada una de los aspectos y características de la Técnica Peruana NTP-ISO/IEC 27001:2014 presentes en cada una de las metodologías de gestión de riesgos de tecnologías de información comparadas. La plantilla se ubica en el anexo n.º 03.

3.3.6 Identificar similitudes entre metodologías.

En esta sección, se realizará la comparación propiamente dicha, para lo cual, se utilizará el resultado del paso uno (identificación de metodologías de gestión de riesgos de TI), conforme al estándar seleccionado, considerando los aspectos, características, y el nivel de detalle establecido, y en atención a ello, se tomarán como base, las plantillas de comparación diseñadas en esta investigación; con la finalidad de identificar la existencia o no de similitudes.

En esa misma línea, se estableció que el estándar de referencia, será la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, y conforme a su análisis y estudio, se identificó que esta presenta 10 aspectos fundamentales, que se encuentran relacionadas a 25 características, las cuales precisan la vinculación que existe con la gestión de riesgos de tecnologías de información.

En ese sentido, se realizó la comparación de las metodologías de gestión de riesgos con los aspectos y las características señaladas en párrafos anteriores; es decir, se analizó las características de cada uno de los aspectos, con cada una de las metodologías seleccionadas; que, en habidas cuentas, son las metodologías Magerit V3, Coras, Mehari y Octave Allegro.

Dentro de este marco de ideas, a continuación, se presenta el análisis realizado.

1) Metodología Magerit v3.

Aspecto 01: Determinar el compromiso de la alta dirección.

Tabla n.º 5

Identificación de características correspondientes al compromiso de la alta dirección en Magerit V3.

Características	Argumentación
Liderazgo y compromiso de la alta dirección	Esta metodología plantea que, para la realización de un proyecto de análisis de riesgos, es necesario realizar un estudio de oportunidad, con el objetivo de "identificar o suscitar el interés de la dirección de la organización en la realización de un proyecto de análisis de riesgos" (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, 2012, pág. 64). Cabe señalar, que los productos que se obtienen en esta etapa son: la sensibilización y apoyo de la dirección a la realización del proyecto, creación del comité de seguimiento, entre otros.
Asignación de roles y responsabilidades	En el proceso de gestión de riesgos se establecen varios actores, a nivel de órganos de gobierno, dirección ejecutiva, y dirección operacional; especificando funciones y responsabilidades; donde se involucran a los altos cargos de la organización, el comité de seguridad de la

	información, responsables de unidades de negocio, responsables de operaciones. Adicionalmente se identifican roles involucrados en el proceso de gestión de riesgos, así tenemos al responsable de la información, responsable del servicio, responsable de la seguridad, responsable del sistema y administradores y operadores. Se utiliza la matriz RACI para la asignación de responsabilidades. “De esta manera se logra asegurar que cada una de las tareas este asignada a un individuo o a un órgano colegiado” (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, 2012, pág. 56).
Asignación de recursos	Se plantea que el comité de seguimiento asegure la disponibilidad de recursos humanos necesarios para llevar a cabo el proyecto de la gestión de riesgos, así mismo, en la planificación del proyecto se deben garantizar los recursos humanos, financieros y temporales necesarios.
Alineación de los objetivos con la estrategia de la organización.	“En coordinación con los objetivos, estrategias y políticas de la organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado,

	satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección" (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, 2012, pág. 10).

Fuente: Elaboración del autor.

Aspecto 02: Definir el alcance

Tabla n.º 6

Identificación de características sobre el alcance en Magerit V3.

Características	**Argumentación**
Alcance	Esta tarea se centra a un dominio limitado, y en concordancia con los objetivos de proyecto, siendo estos de corto o largo alcance, con plena estimación de los participantes. Para ello propone el uso de técnicas de entrevistas, reuniones, brainstorming, Delphi; así también precisa determinar la evaluación de restricciones políticas, gerenciales, estratégicas, geográficas, temporales, estructurales, funcionales, legales, metodológicas, culturales, presupuestarias. Para que el alcance quede determinado, se debe concretar las siguientes características: "Los **activos esenciales:** información que se maneja y servicios que se prestan; **los puntos de**

	intercambio de interconexión con otros sistemas, aclarando qué información se intercambia y qué servicios se prestan mutuamente y **los proveedores externos**" (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, 2012, pág. 68).

Fuente: Elaboración del autor.

Aspecto 03: Comprender el contexto de la organización.

Tabla n.º 7

Identificación de características sobre el contexto de la organización en Magerit V3.

Características	Argumentación
Aspectos internos y externos.	Propone documentar el contexto externo en que se desarrolla la organización, considerando el ambiente cultural, social y político; identificando las obligaciones legales, reglamentarias y contractuales; así como la competencia y su posicionamiento. En cuanto al entorno interno propone identificar la política interna, compromisos con los accionistas y con los trabajadores.
Comprender las necesidades y expectativas de las partes interesadas.	Según la NTP-ISO/IEC 27001:2014, como parte de comprender las necesidades y expectativas de las partes interesadas incluyen requisitos, que pueden ser legales, regulatorios y obligaciones

	contractuales; y de acuerdo al ítem anterior sobre aspectos internos y externos; esta metodología los aborda en la gestión de riesgos.

Fuente: Elaboración del autor.

Aspecto 4: Activos de información.

Tabla n.º 8

Identificación de características sobre los activos de información en Magerit V3.

Características	**Argumentación**
Identificar Activos de Información	Mediante el método de análisis de riesgos MAR. 11 – Identificación de activos, se presenta un catálogo de tipos de activos de información, a través de una clasificación jerárquica, asignándoles para cada activo un código, nombre y descripción. De hecho, presenta un listado de activos, clasificados en: activos esenciales, arquitectura del sistema, datos / información, claves criptográficas, servicios, aplicaciones informáticas, equipamiento informático, redes de comunicaciones, soporte de información, equipamiento auxiliar, personal, XML; adicionalmente se presentan sub clasificaciones para poder identificar mejor los activos de información de las organizaciones.

Valoración de activos	Se realiza mediante la MAR 13. Valoración de activos; y se hace a través del análisis de dimensiones de valoración, con la finalidad de determinar los atributos que hagan valioso a un activo. “Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión” (MAGERIT – versión 3.0 Metodologia de Analisis y Gestión de Riesgos de los Sistemas de Informacion - Libro II - Catalogo de Elementos, 2012, pág. 7). Se utilizan las dimensiones de disponibilidad, integridad, confidencialidad, autenticidad, trazabilidad. Asimismo, ha establecido criterios de valoración en una escala de 0 a 10.

Fuente: Elaboración del autor.

Aspecto 5: Identificación de riesgos.

Tabla n.º 9

Identificación de características de los riesgos en Magerit v3

Características	**Argumentación**
Establecer criterios de riesgos	Estable un conjunto de criterios relacionados con escalas de valoraciones de riesgos, generando

	escalas de valoración respecto a requisitos de seguridad de información, requisitos de disponibilidad de los servicios, estimar las consecuencias de incidentes de seguridad; así mismo se establecen criterios respecto a la toma de decisiones del tratamiento, con la finalidad de establecer umbrales de tratamiento, umbrales de riesgo, entre otros criterios.
Identificación de propietarios de los riesgos.	La metodología no es precisa en la identificación de propietarios de los riesgos.
Identificar amenazas y Vulnerabilidades.	Se realiza a través de la MAR.2 Caracterización de las amenazas. La metodología facilita un catálogo de posibles amenazas relacionadas al peligro a los que se encuentran expuestos los activos de información; para lo cual genera una conexión entre amenaza, tipo de activo y dimensión. Del listado de amenazas tenemos: desastres naturales (fuego, agua, sismos, contaminación, etc.), origen industrial (contaminación electromecánica, corte de suministro eléctrico, etc.), errores y fallos no intencionados (errores de usuarios, errores de configuración, etc.), ataques intencionados (manipulación de log, abusos

	de privilegios de acceso, difusión de software dañino, etc.).
Identificar riesgos	Se realiza a través de la caracterización de las amenazas y vulnerabilidades.

Fuente: Elaboración del autor.

Aspecto 6: Evaluar el riesgo.

Tabla n.º 10

Identificación de características para la evaluación de riesgos en Magerit V3.

Características	**Argumentación**
Valoración de consecuencias potenciales	Plantea valorar el perjuicio que puede causar una amenaza sobre los activos de información; por lo que "hay que valorar su influencia en el valor del activo, en dos sentidos: Degradación: cuán perjudicado resultaría el [valor del] activo y probabilidad: cuán probable o improbable es que se materialice la amenaza" (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, 2012, pág. 28). En ese sentido proporciona una escala nominal (estimación cualitativa) para estimar la degradación del valor; así mismo brinda una escala de medición para estimar la tasa anual de ocurrencia.

Valoración de probabilidad de ocurrencia	La metodología propone la determinación del riesgo potencial, para ello determina que, conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia, en ese sentido, establece una serie de zonas para el tratamiento de los riesgos: zona 1 - riesgos muy probables y de muy alto impacto zona 2 - franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables, pero de impacto bajo o muy bajo. zona 3 - riesgos improbables y de bajo impacto zona 4 - riesgos improbables, pero de muy alto impacto" (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, 2012, pág. 29).
Valoración del impacto	Se realiza a través de la MAR. 41 - estimación del impacto y se aborda mediante la determinación del impacto potencial, en donde se valora a través del análisis de impacto acumulado e impacto repercutido. El impacto acumulado valora cada activo por cada amenaza en cada dimensión de valoración; mientras

	que el impacto repercutido, calcula el valor propio de cada activo por cada amenaza a la que se encuentra expuesto.

Fuente: Elaboración del autor.

Aspecto 7: Tratamiento del riesgo.

Tabla n.º 11

Identificación de características en el tratamiento del riesgo en Magerit V3

Características	Argumentación
Opciones de tratamiento	Plantea dos opciones para el tratamiento de riesgos: "reducir el riesgo residual (aceptar un menor riesgo) y ampliar el riesgo residual (aceptar un mayor riesgo)" (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, 2012, pág. 49), tomando en cuenta el contexto de la organización. Cabe destacar, que las opciones para el tratamiento de riesgos están en función de las zonas de riesgos, expuestos en la valoración conforme a la probabilidad de ocurrencia.
Determinación de controles	Se realiza a través de MAR. 3 - Caracterización de las salvaguardas; donde se establece un catálogo de salvaguardas a través de un conjunto de tareas, en función de indicadores de impacto y riesgo.

	Identifican salvaguardas para riesgos materiales, tecnológicos, organizativos, procedimentales, etc.

Fuente: Elaboración del autor.

Aspecto 8: Aplicabilidad de los controles.

Tabla n.º 12

Identificación de características de la declaración de aplicabilidad en Magerit V3.

Características	Argumentación
Declaración de aplicabilidad	A través de la selección de salvaguardas, se estudian la justificación y aplicabilidad cada una de las salvaguardas, con la finalidad de obtener un informe de declaración de aplicabilidad; en donde se realiza una calificación de cada salvaguarda en función de la eficacia frente a las amenazas que pretenden mitigar (Caracterización de salvaguardas).

Fuente: Elaboración del autor.

Aspecto 9: Monitoreo y mejora continua.

Tabla n.º 13

Identificación de características para el monitoreo y mejora continua en Magerit V3.

Características	Argumentación
Monitoreo y Evaluación.	Propone que los sistemas estén bajo monitorización permanente, considerando riesgos potenciales e indicadores de impacto. Asimismo, plantea que los responsables de la seguridad informática formulen

	indicadores claves de riesgos, algoritmos de cálculo, periodicidad de evaluación, umbrales de aviso y alarmas.
Auditorias	Plantea el uso de auditorías para determinar la evolución de los riesgos. “El informe de auditoría deberá dictaminar sobre la adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias…” (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, 2012, pág. 16).
Mejora continua	La metodología contempla que el análisis y el tratamiento de riesgos constituyen un análisis repetitivo, puesto que los sistemas de información evolucionan, por lo que es necesario una evaluación continua.

Fuente: Elaboración del autor.

Aspecto 10: Concientización y Comunicación

Tabla n.º 14

Identificación de características para la concientización y comunicación en Magerit V3.

Características	Argumentación
Concientización	La gestión de riesgos está estrechamente ligada a la seguridad de la información; en ese sentido, la metodología plantea concienciación y formación mediante la creación de una cultura de seguridad, basado en tres (3) pilares fundamentales: • Una política seguridad corporativa que se entienda, que se difunda y mantenga al día. • Una normativa de seguridad que, entrando en áreas específicas de actividad, aclare la postura de la Organización. • Una formación continua a todos los niveles, recordando las cautelas rutinarias y las actividades especializadas, según la responsabilidad adscrita a cada puesto de trabajo (MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método, 2012, pág. 11).

Comunicación	Mediante la sección de comunicación y consulta, la metodología plantea la colaboración de interlocutores, que involucre a los usuarios para canalizar sus necesidades y colaboren en gestión de la seguridad, a los proveedores externos y a los órganos de gobierno.
Documentación	La metodología plantea la creación de documentos en sus diferentes fases; así tenemos: • Documentación intermedia: constituida por los resultados de entrevistas, estadísticas, diagramas de flujos de información, procesos, etc. • Documentación final: constituida por modelos de valor, mapas de riesgos, declaración de aplicabilidad, evaluación de salvaguardas, informe de vulnerabilidades, etc.

Fuente: Elaboración del autor.

2) Metodología CORAS

Aspecto 01: Determinar el compromiso de la alta dirección

Tabla n.º 15

Identificación de características correspondientes al compromiso de la alta dirección en la Metodología Coras.

Características	Argumentación
Liderazgo y compromiso de la alta dirección.	Comprende el primer paso de los ocho que propone esta metodología; se inicia con las preparaciones para el análisis, con la finalidad de informar al responsable de la organización (cliente) de las responsabilidades que tiene respecto a la gestión de los riesgos. Este primer acercamiento se da mediante reuniones entre el cliente y el líder del análisis; con el propósito de involucrar a los tomadores de decisiones y a los expertos técnicos.
Asignación de roles y responsabilidades.	No presenta mecanismos para la asignación de roles y responsabilidades.
Asignación de recursos	No se ha determinado en la metodología la especificación de los recursos.
Alineación de los objetivos con la estrategia de la organización.	En el segundo paso, presentación de objetivos del cliente, se basa en identificar y “lograr que los representantes del cliente presenten sus objetivos generales del análisis y el objetivo que desean

	analizar. Por lo tanto, durante el segundo paso, los analistas recopilarán información basada en las presentaciones y discusiones del cliente" (Guia para el metodo Coras, 2011, pág. 25). En ese sentido, al ser los objetivos presentados por los representantes del cliente (de la organización); se presume que están alineados con la estrategia de la organización.

Fuente: Elaboración del autor.

Aspecto 02: Definir el alcance

Tabla n.º 16

Identificación de características sobre el alcance en la Metodología Coras.

Características	Argumentación
Alcance	En el segundo paso de la metodología, Presentación de objetivos del cliente, se aborda preliminarmente el establecimiento del alcance y el enfoque de la gestión de riesgos. En el paso cuatro, aprobación de la descripción del objetivo, el cliente aprueba la descripción final del objetivo del proyecto, el alcance, el enfoque y todos los supuestos de los riesgos.

Fuente: Elaboración del autor.

Aspecto 03: Comprender el contexto de la organización

Tabla n.º 17

Identificación de características sobre el contexto de la organización en la Metodología Coras.

Características	Argumentación
Aspectos internos y externos.	No ofrece información sobre esta característica.
Comprender las necesidades y expectativas de las partes interesadas.	En el paso 3: Refinar la descripción del objetivo utilizando diagramas de activos, establece la comprensión de forma concreta y refinada los objetivos por parte del cliente. Mediante una reunión entre el analista de gestión de riesgos y el representante del cliente; "La reunión se divide en tres partes: (1) presentación del objetivo tal como lo entienden los analistas; (2) identificación de activos; (3) análisis de riesgo de alto nivel" (Guia para el metodo Coras, 2011, pág. 26). Generalmente se incluye al cliente, pero también se involucran otras partes interesadas, que tengan que ver con el logro de los objetivos.

Fuente: Elaboración del autor.

Aspecto 4: Activos de información

Tabla n.º 18

Identificación de características sobre los activos de información en la Metodología Coras.

Características	Argumentación
Identificar Activos de Información.	En el paso 3 de la metodología, además de conocer las expectativas de las partes interesadas, también se identifican a los activos; dichos activos se documentan a través de los diagramas de activos; el cual presenta un conjunto de símbolos vinculados al lenguaje de modelado Coras.
Valoración de activos	La valoración de activos se realiza por niveles de importancia, en una escala del uno al cinco.

Fuente: Elaboración del autor.

Aspecto 5: Identificación de riesgos

Tabla n.º 19

Identificación de características de los riesgos en la Metodología Coras.

Características	Argumentación
Establecer criterios de riesgos	En el paso 3 de la metodología, también se identifican los riesgos a través de tablas de riesgos de alto nivel, donde se establecen criterios mediante preguntas ¿Quién / que lo causa?, ¿Cómo?, ¿cuál es

	el incidente?, ¿Qué le hace daño?, ¿Qué lo hace posible?
Identificación de propietarios de los riesgos	Indirectamente mediante la tabla de riesgos de alto nivel se identifican a los propietarios de los riesgos.
Identificar amenazas y Vulnerabilidades	El paso 5: identificación de riesgos, se ejecuta mediante el análisis y creación de diagramas de amenazas. Se realiza a través de talleres utilizando la técnica de lluvia de ideas estructuradas, con el fin identificar incidentes no deseados, amenazas y vulnerabilidades. El resultado de este paso es un documento donde se plasman los diagramas de amenazas Coras. Los diagramas de amenazas Coras son actualizados desde la perspectiva de los participantes y de los expertos en gestión de riesgos.
Identificar riesgos	El paso 5: Identificación de riesgos, se realiza mediante lluvia de ideas estructuradas, con el propósito de que los participantes expresen sus intereses, perspectivas y competencias en la gestión de riesgos.

Fuente: Elaboración del autor.

Aspecto 6: Evaluar el riesgo

Tabla n.º 20

Identificación de características para la evaluación de riesgos en la Metodología Coras.

Características	Argumentación
Valoración de consecuencias potenciales. Valoración de probabilidad de ocurrencia. Valoración de impacto.	La valoración de consecuencias, probabilidad de ocurrencias y la valoración de impacto, la metodología lo establece en el paso 6: estimación de riesgos mediante diagramas de amenazas; en donde se calculan los valores de riesgos, que permitan determinar riesgos aceptable o tratamiento de riesgos. "Las consecuencias se estiman para cada relación de un incidente no deseado a un activo. Los valores de consecuencia y los valores de probabilidad se toman de la escala de consecuencias del activo y la escala de probabilidad, respectivamente (Guia para el metodo Coras, 2011, pág. 37). Asimismo, en el paso 7: Evaluación de riesgos mediante diagramas de riesgos, se plantea la valoración del riesgo a través de la matriz de riesgos, donde se ponderan según el nivel de frecuencias vs consecuencias.

Fuente: Elaboración del autor.

Aspecto 7: Tratamiento del riesgo.

Tabla n.º 21

Identificación de características del tratamiento del riesgo en la Metodología Coras.

Características	Argumentación
Opciones de tratamiento.	En el paso 8: Tratamiento de riesgo utilizando diagramas de tratamiento, plantea el uso de diagramas de tratamiento Coras. La selección del tratamiento del riesgo estará en función de un análisis previo sobre costo / beneficio.
Determinación de controles.	La metodología plantea determinar los controles a través del análisis costo / beneficio.

Fuente: Elaboración del autor.

Aspecto 8: Aplicabilidad de los controles.

Tabla n.º 22

Identificación de características de la declaración de aplicabilidad en la Metodología Coras.

Características	Argumentación
Declaración de aplicabilidad.	Se establece la declaración de aplicabilidad, mediante un documento, donde se establecen los controles especificados para el tratamiento de los riesgos.

Fuente: Elaboración del autor.

Aspecto 9: Monitoreo y mejora continua.

Tabla n.º 23

Identificación de características para el monitoreo y mejora continua en la Metodología Coras.

Características	Argumentación
Monitoreo y medición.	La metodología no implementa mecanismos de mejora y medición.
Auditorias.	La metodología no presenta recomendaciones para el análisis mediante auditorias.
Mejora continua.	La metodología no presenta mecanismos para la evaluación y la mejora continua.

Fuente: Elaboración del autor.

Aspecto 10: Concientización y Comunicación.

Tabla n.º 24

Identificación de características para la concientización y comunicación en la Metodología Coras.

Características	Argumentación
Concientización.	La metodología no plantea criterios para establecer concientización vinculados a los elementos de la cultura organizacional.

Comunicación.	La metodología no establece mecanismos para comunicar los riesgos entre los actores que participan en la seguridad de la información.
Documentación.	La metodología posibilita la documentación del análisis de riesgos de cada uno de los 8 pasos, utilizando el lenguaje de modelado Coras.

Fuente: Elaboración del autor.

3) Metodología MEHARI

Aspecto 01: Determinar el compromiso de la alta dirección.

Tabla n.º 25

Identificación de características correspondientes al compromiso de la alta dirección en la Metodología Mehari.

Características	Argumentación
Liderazgo y compromiso de la alta dirección.	No establece mecanismos de gestión de riesgos relacionados al compromiso de la alta dirección y liderazgo.
Asignación de roles y responsabilidades.	No especifica la asignación de roles y responsabilidades en la gestión de riesgos.
Asignación de recursos	No especifica la asignación de recursos.
Alineación de los objetivos con la estrategia de la organización.	No se ha determinado que la metodología tenga en cuenta la gestión de riesgos de tecnologías de

	información como parte de la estrategia organizacional.

Fuente: Elaboración del autor.

Aspecto 02: Definir el alcance

Tabla n.º 26

Identificación de características sobre el alcance en la Metodología Mehari.

Características	**Argumentación**
Alcance	La metodología no proporciona elementos para definir el alcance de la gestión de riesgos.

Fuente: Elaboración del autor.

Aspecto 03: Comprender el contexto de la organización

Tabla n.º 27

Identificación de características sobre el contexto de la organización en la Metodología Mehari

Características	**Argumentación**
Aspectos internos y externos.	La metodología plantea tener en cuenta el contexto económico, social y geográfico; para determinar las medidas necesarias para la gestión de riesgos. Por lo tanto, debe examinarse la posible existencia de factores que podrían exponer a la organización a determinados tipos de riesgos.

Comprender las necesidades y expectativas de las partes interesadas.	La metodología plantea la identificación riesgos de activos de información, en función de las necesidades de la organización, tipos de necesidades, relación con proveedores e intereses de los usuarios.

Fuente: Elaboración del autor.

Aspecto 4: Activos de información.

Tabla n.º 28

Identificación de características sobre los activos de información en Metodología Mehari.

Características	Argumentación
Identificar Activos de Información.	La metodología plantea que "los activos son los principales objetos del riesgo. Son lo que se dañará; y el riesgo proviene del hecho de que cierta forma de activo es susceptible a algún daño particular" (MEHARI 2010 - Conceptos fundamentales y especificaciones funcionales, 2010, pág. 10). Por consiguiente, se clasifican en activos primarios y secundarios. A los activos primarios se organizan en tres categorías (servicios, datos necesarios para los servicios y procesos de gestión), correspondiéndose a necesidades funcionales; mientras que a los activos secundarios o de apoyo, se refieren a los medios para satisfacer las necesidades funcionales.

	Asimismo, proporciona un catálogo de activos de tecnologías de información.
Valoración de activos.	Plantea caracterizar a cada activo de acuerdo a su categoría y tipo (primario o secundario).

Fuente: Elaboración del autor.

Aspecto 5: Identificación de riesgos.

Tabla n.º 29

Identificación de características de los riesgos en la Metodología Mehari.

Características	**Argumentación**
Establecer criterios de riesgos.	La metodología propone analizarlos a través de 2 factores: la gravedad de los riesgos que las medidas prioritarias están diseñadas a reducir y el número de riesgos que se trataran.
Identificación de propietarios de los riesgos.	Mediante el listado de elementos característicos de riesgos, se plantea identificar los tipos de actores a los cuales se encuentran relacionados los riesgos y su relación con los tipos de activos, vulnerabilidades intrínsecas y eventos desencadenantes.
Identificar amenazas y vulnerabilidades.	La metodología propone determinar la vulnerabilidad intrínseca y la vulnerabilidad contextual de los activos de información.

	Además, proporciona una lista de vulnerabilidades intrínsecas. Esta lista relaciona principalmente los tipos de activos, tipos de daños y tipos vulnerabilidades.
Identificar riesgos.	La metodología plantea tres (3) pasos para establecer una correcta identificación de riesgos: • "Enumerar los elementos característicos de los riesgos. • Listar los riesgos que son teóricamente posibles, • Seleccionar todos los riesgos de esta lista que sean posibles dentro del contexto específico de gestión de riesgos ya existente" (MEHARI 2010 - Conceptos fundamentales y especificaciones funcionales, 2010, pág. 15). Mehari incorpora una base de conocimientos de riesgos típicos.

Fuente: Elaboración del autor.

Aspecto 6: Evaluar el riesgo

Tabla n.º 30

Identificación de características para la evaluación de riesgos en la Metodología Mehari.

Características	Argumentación
Valoración de consecuencias potenciales.	La metodología plantea analizarlo y medirlo a través del impacto intrínseco, con la finalidad de determinar el máximo nivel de consecuencia en que pueda incurrir la organización, en ausencia de medidas de seguridad.
Valoración de probabilidad de ocurrencia.	Propone una valoración a través del análisis de probabilidad intrínseca (probabilidad máxima que ocurra el riesgo). Adicionalmente formula un conjunto de medidas, con el propósito de contribuir a la reducción de la probabilidad de ocurrencia del riesgo; así tenemos: medidas disuasorias, medidas preventivas, medidas de confinamiento y medidas paliativas; cada una de ellas presenta principios y mecanismos de aplicación.
Valoración de impacto.	Se establecen escalas de valoración de impacto, escala de probabilidad y escalas de efectividad. Así mismo, propone el uso de la tabla de decisión, vinculada al impacto estimado y la probabilidad de

	ocurrencia; en donde se establece cuatro niveles de riesgo (intolerable, inadmisible y aceptables).

Fuente: Elaboración del autor.

Aspecto 7: Tratamiento del riesgo.

Tabla n.º 31

Identificación de características del tratamiento del riesgo en la Metodología Mehari.

Características	Argumentación
Opciones de tratamiento.	La metodología propone cuatro (4) opciones principales para el tratamiento de riesgos: retención del riesgo, reducir el riesgo, transferir el riesgo y evitar el riesgo.
Determinación de controles.	Planteada a través de la lista de servicios de seguridad, que es una base de conocimiento organizado por servicios y sub servicios.

Fuente: Elaboración del autor.

Aspecto 8: Aplicabilidad de controles.

Tabla n.º 32

Identificación de características de la declaración de aplicabilidad en la Metodología Mehari.

Características	Argumentación
Declaración de aplicabilidad	No se ha determinado documento en donde se establezcan los controles seleccionados.

Fuente: Elaboración del autor.

Aspecto 9: Monitoreo y mejora continua.

Tabla n.º 33

Identificación de características para el monitoreo y mejora continua en la Metodología Mehari.

Características	Argumentación
Monitoreo y evaluación.	La metodología propone la monitorización permanente de los riesgos, con la finalidad de garantizar que los riesgos en el tiempo, se corresponden con los niveles de calidad de los servicios deseados.
Auditorias.	Plantea la realización de pruebas posteriores a los controles, para ello recomienda el uso de la base de conocimientos de auditorías de servicios de seguridad.
Mejora continua.	La metodología contempla la mejora continua, dentro de la evaluación que se realiza a través de lista de servicios de seguridad.

Fuente: Elaboración del autor.

Aspecto 10: Concientización y Comunicación.

Tabla n.º 34

Identificación de características para la concientización y comunicación en la metodología Mehari.

Características	Argumentación
Concientización.	No se ha determinado mecanismos para la concientización de los involucrados en la gestión de riesgos; pero si lo considera dentro de la lista de servicios de seguridad para la evaluación de los recursos humanos.
Comunicación.	No se plantea mecanismos para comunicar riesgos en el contexto de la organización.
Documentación.	Se genera la documentación de la gestión de riesgos a través del uso de las bases de conocimiento.

Fuente: Elaboración del autor.

4) Metodología Octave Allegro

Aspecto 01: Determinar el compromiso de la alta dirección.

Tabla n.º 35

Identificación de características correspondientes al compromiso de la alta dirección en la Metodología Octave Allegro.

Características	Argumentación
Liderazgo y compromiso de la alta dirección.	La metodología define el patrocinio de la alta gerencia como factor crítico para el éxito de la

	implementación de la metodología en la gestión de riesgos; para ello “la gerencia debe comprometerse a brindar un apoyo activo al proceso y deben estar dispuestos a participar en el proceso cuando sea necesario, principalmente en el desarrollo y el patrocinio de criterios de medición de riesgos para toda la organización” (Carralli, Stevens, & William, 2007, pág. 35).
Asignación de roles y responsabilidades.	La metodología no define la asignación de roles y responsabilidades.
Asignación de recursos.	Para esta característica se plantean dos aspectos importantes: la composición y el tamaño del equipo. Se propone formar equipos multidisciplinarios, formados por personal operativo, personal del departamento de TI, alta dirección; así como el compromiso para disponer del tiempo necesario.
Alineación de los objetivos con la estrategia de la organización.	Plantea que para el proceso de evaluación de riesgos debería existir una conexión permanente entre los objetivos estratégicos, la seguridad de la información, el desarrollo de sistemas y la continuidad del negocio.

	Estas características se establecen en el paso 1 de la metodología: Establecer criterios de medición de riesgos.

Fuente: Elaboración del autor.

Aspecto 02: Definir el alcance.

Tabla n.º 36

Identificación de características sobre el alcance en la Metodología Octave Allegro.

Características	Argumentación
Alcance.	La metodología propone establecer el alcance en función de los activos de información y sus asociaciones con las personas, tecnologías e instalaciones.

Fuente: Elaboración del autor.

Aspecto 03: Comprender el contexto de la organización

Tabla n.º 37

Identificación de características sobre el contexto de la organización en la Metodología Octave Allegro.

Características	Argumentación
Aspectos internos y externos.	Para esta metodología, la evaluación del contexto de la organización está en función de los procesos y el contexto de la prestación de los servicios.

Comprender las necesidades y expectativas de las partes interesadas.	A través de los aspectos de composición y tamaño de equipo, la metodología indirectamente incorpora a las partes interesadas en la gestión de los riesgos.

Fuente: Elaboración del autor.

Aspecto 4: Activos de información

Tabla n.º 38

Identificación de características sobre los activos de información en la Metodología Octave Allegro.

Características	Argumentación
Identificar Activos de Información.	El paso 2 de la metodología plantea desarrollar un perfil de activo de información, donde se describen las características, cualidades y valores únicos de cada activo. El perfil de cada activo se registra en la hoja de trabajo, denominadas “Hojas de trabajo Allegro”.
Valoración de activos.	La valoración de activos, en esta metodología se establece mediante la identificación de los contenedores de los activos de información (paso 3), que permita identificar en donde se almacenan, transportan y procesan los activos de información; adicionalmente se identificación las áreas de preocupación (paso 4).

Fuente: Elaboración del autor.

Aspecto 5: Identificación de riesgos.

Tabla n.º 39

Identificación de características de los riesgos en la Metodología Octave Allegro.

Características	Argumentación
Establecer criterios de riesgos.	Propuesta en el paso 1: Establecer criterios de medición de riesgos. "Los criterios de medición de riesgos son un conjunto de medidas cualitativas contra las cuales se pueden evaluar los efectos de un riesgo realizado y constituyen la base de una evaluación de riesgos de activos de información" (Carralli, Stevens, & William, 2007, pág. 29).
Identificación de propietarios de los riesgos.	Como parte del paso 2: Desarrollar un perfil de activo de información, además de identificar los activos de información, también se determinan a los propietarios de activos de información, y custodios de activos de información; para los cuales se han establecido requisitos. Se utilizan hojas de trabajo Allegro.
Identificar amenazas y vulnerabilidades.	Se realiza a través del paso 5: Identificar escenarios de amenazas; en donde se plantea el uso de escenarios de amenazas y árboles de amenazas. Adicionalmente se propone los cuestionarios de amenazas, clasificados por tipo de contenedor

	(técnico, físico y personal). Se utilizan hojas de trabajo Allegro.
Identificar riesgos.	Se identifican los riesgos en el paso 6: Identificar riesgos. Se usan las hojas de trabajo allegro generadas en la sección de activos y amenazas.

Fuente: Elaboración del autor.

Aspecto 6: Evaluar el riesgo.

Tabla n.º 40

Identificación de características para la evaluación de riesgos en la Metodología Octave Allegro.

Características	**Argumentación**
Valoración de consecuencias potenciales.	En el paso 7: Analizar riesgos, se valoran las consecuencias a través de la asignación de puntajes relativos. "El puntaje de riesgo relativo se obtiene considerando la medida en que la consecuencia de un riesgo afecta a la organización en comparación con la importancia relativa de las diversas áreas de impacto" (Caralli, Stevens, Young, & Wilson, 2007, pág. 67).

Valoración de probabilidad de ocurrencia.	La probabilidad se establece cualitativamente como alta, media y baja; estrechamente relacionadas con vulnerabilidades y eventos de seguridad.
Valoración del impacto.	Se realiza mediante las hojas de trabajo Allegro relacionadas a los criterios de medición de riesgos y la declaración de consecuencia trabajadas en los pasos anteriores. Se establece la escala de medición de impacto (alto, medio y bajo). Se utilizan hojas de trabajo Allegro.

Fuente: Elaboración del autor.

Aspecto 7: Tratamiento del riesgo

Tabla n.º 41

Identificación de características del tratamiento del riesgo en la Metodología Octave Allegro.

Características	Argumentación
Opciones de tratamiento.	Mediante el paso 8: Seleccione el enfoque de mitigación, la metodología plantea 3 opciones: Aceptar, mitigar o diferir el riesgo.
Determinación de controles.	Para la determinación de los controles se deben tener en cuenta los contendores, el tipo de control (administrativo, técnico y físico) y la aceptación del riesgo residual después de aplicar el control.

Fuente: Elaboración del autor.

Aspecto 8: Aplicabilidad de los controles.

Tabla n.º 42

Identificación de características de la declaración de aplicabilidad en la Metodología Octave Allegro.

Características	Argumentación
Declaración de aplicabilidad.	La metodología administra la gestión de riesgos de TI a través de hojas de trabajo de perfil de activo de información, mapas de entorno de riesgo de activo de información y hojas de trabajo de riesgos de activos de información; lo que facilita el establecimiento de los criterios de medición de los riesgos de tecnologías de información, así como la priorización del impacto en los activos de la organización.

Fuente: Elaboración del autor.

Aspecto 9: Monitoreo y mejora continua.

Tabla n.º 43

Identificación de características para el monitoreo y mejora continua en la Metodología Octave Allegro.

Características	Argumentación
Monitoreo y evaluación.	La metodología plantea que la evaluación de riesgos es un proceso continuo, el cual permitirá determinar

	las posibles brechas de seguridad, así como el estado de los controles.
Auditorias.	No se ha determinado mecanismos para auditorias en esta metodología.
Mejora continua.	Se plantea a través de la repetibilidad de la gestión de la seguridad y la evaluación de los riesgos.

Fuente: Elaboración del autor.

Aspecto 10: Concientización y Comunicación.

Tabla n.º 44

Identificación de características para la concientización y comunicación en la Metodología Octave Allegro.

Características	Argumentación
Concientización.	La metodología plantea crear una cultura consciente del riesgo, y para ello propone que la metodología de gestión de riesgos debe ser accesible a todos los empleados de la organización y que la gestión de riesgos tenga el propósito de ayudar a los empleados.
Comunicación.	La metodología no plantea mecanismos de comunicación para la comunicación de riesgos.

Documentación.	La evaluación de riesgos se va documentando en cada una de los ocho pasos, a través de las hojas de trabajo Allegro.

Fuente: Elaboración del autor.

Capitulo IV: Resultados

De la revisión metódica y analítica de las metodologías de gestión de riesgos de tecnologías de información, seleccionadas previamente según la adaptación del método de Estudio de Similitudes entre Modelos y Estándares (MSSS), se han obtenido resultados, que permitirán realizar un análisis descriptivo; así mismo, determinar el grado de similitud que presentan cada una de las metodologías, respecto a la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, en función de la determinación de aspectos y características que esta plantea.

4.1 Resultados descriptivos de similitud entre la Metodología Magerit V3 y la Norma Técnica Peruana NTP-ISO/IEC 27001:2014

Tabla n.º 45

Satisfacción de aspectos y características de la NTP-ISO/IEC 27001:2014 en la metodología *Magerit V3.*

Metodología Magerit V3	
Aspecto 1: Determinar el compromiso de la alta dirección.	
Liderazgo y compromiso de la alta dirección.	SI
Asignación de roles y responsabilidades.	SI
Asignación de recursos.	SI
Alineación de los objetivos con la estrategia de la organización.	SI
Aspecto 2: Definir el alcance.	
Alcance.	SI
Aspecto 3: Comprender el contexto de la organización.	
Aspectos internos y externos.	SI

Comprender las necesidades y expectativas de las partes interesadas.	SI
Aspecto 4: Activos de información.	
Identificar activos de información.	SI
Valoración de activos.	SI
Aspecto 5: Identificación de riesgos.	
Establecer criterios de riesgos.	SI
Identificación de propietarios de riesgos.	NO
Identificar amenazas y vulnerabilidades.	SI
Identificar riesgos.	SI
Aspecto 6: Evaluar el riesgo.	
Valoración de consecuencias potenciales.	SI
Valoración de probabilidad de ocurrencia.	SI
Valoración del impacto.	SI
Aspecto 7: Tratamiento del riesgo.	
opciones de tratamiento.	SI
Determinación de controles.	SI
Aspecto 8: Aplicabilidad de controles.	
Declaración de aplicabilidad.	SI
Aspecto 9: Monitoreo y mejora continua.	
Monitoreo y evaluación.	SI
Auditorias.	SI
Mejora continua.	SI
Aspecto 10: Concientización y comunicación.	
concientización.	SI
Comunicación.	SI

Documentación.	SI

Fuente: Elaboración del autor

En la tabla n.° 45, se observa que la Metodología Magerit V3, no ha establecido procedimientos, técnicas u otros mecanismos, que permitan identificar a los propietarios de los riesgos; aumentando el riesgo en la toma de decisiones y dificultando la gestión oportuna y eficiente de los riesgos de tecnologías de la información.

En tal sentido, la identificación de los propietarios de riesgos es de vital importancia, ya que permite tener mapeado a las personas que tienen la autoridad para actuar y resolver los riesgos oportunamente en el momento adecuado, de tal forma que posibilite minimizar su impacto en la organización.

Es necesario precisar, que existen diferencias entre los propietarios de los riesgos y los propietarios de activos de información; el primero se refiere a la o las personas que son responsables del uso del activo de información asignado para el cumplimiento de sus funciones; pero que no necesariamente pueden tomar decisiones sobre los riesgos que se presentan o cuando se presenten; por otro lado, los propietarios de riesgos de información son aquellas personas o entidades que tienen la responsabilidad y la autoridad para gestionar los riesgos; no obstante, pueden existir propietarios de riesgos que a la vez son propietarios de activos de información.

Sin bien es cierto, la metodología Magerit V3 identifica roles y responsabilidades; estas se realizan a nivel de proyecto, utilizando la matriz de asignación responsabilidades (RACI) que permite relacionar actividades con recursos, asegurando que cada tarea este asignado a un individuo; sin embargo, esto

es muy diferente a la asignación de responsabilidades vinculados a los propietarios de riesgos, ya que estos deben evaluar y actuar constantemente en función de los riesgos que presenten diariamente en la organización.

4.2 Resultados descriptivos de similitud entre la Metodología Coras y la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

Tabla n.º 46

Satisfacción de aspectos y características de la NTP-ISO/IEC 27001:2014 en la metodología *Coras.*

Metodología Coras	
Aspecto 1: Determinar el compromiso de la alta dirección	
Liderazgo y compromiso de la alta dirección.	SI
Asignación de roles y responsabilidades.	NO
Asignación de recursos.	NO
Alineación de los objetivos con la estrategia de la organización	SI
Aspecto 2: Definir el alcance.	
Alcance	SI
Aspecto 3: Comprender el contexto de la organización	
Aspectos internos y externos.	SI
Comprender las necesidades y expectativas de las partes interesadas.	SI
Aspecto 4: Activos de información	
Identificar activos de información	SI
Valoración de activos	SI
Aspecto 5: Identificación de riesgos	
Establecer criterios de riesgos.	SI

Identificación de propietarios de riesgos.	SI
Identificar amenazas y vulnerabilidades.	SI
Identificar riesgos.	SI
Aspecto 6: Evaluar el riesgo.	
Valoración de consecuencias potenciales.	SI
Valoración de probabilidad de ocurrencia.	SI
Valoración del impacto.	SI
Aspecto 7: Tratamiento del riesgo	
opciones de tratamiento.	SI
Determinación de controles.	SI
Aspecto 8: Aplicabilidad de controles.	
Declaración de aplicabilidad.	SI
Aspecto 9: Monitoreo y mejora continua	
Monitoreo y evaluación.	NO
Auditorias.	NO
Mejora continua.	NO
Aspecto 10: Concientización y comunicación	
concientización.	NO
Comunicación.	NO
Documentación.	SI

Fuente: Elaboración del autor.

En la tabla n.° 46, se evidencia que la metodología Coras, no ha establecido acciones que permitan a la alta dirección establecer mecanismos de asignación de roles y responsabilidades en el proceso de gestión de riesgos de tecnologías de la información; lo que podría generar desorganización y descoordinación en las

necesidades operativas, tácticas y estratégicas, teniendo en cuenta que la asignación de roles y responsabilidades permitirá establecer los perfiles idóneos de los profesionales que estarán al frente de la organización, siendo este uno de los aspectos fundamentales en la era digital, y de esta forma permitir que la alta dirección pueda identificar y establecer las tareas que realizará cada uno de los responsables.

Respecto a la asignación de recursos para el tratamiento, implementación y mantenimiento de gestión de riesgos de tecnologías de información, no se ha determinado que la metodología vincule los recursos humanos, materiales y financieros como parte intrínseca de la gestión efectiva y dinámica de los riesgos de tecnologías de información y por tanto de la seguridad de la información.

En relación al monitoreo y evaluación, esta metodología no ha planteado mecanismos o formas que permitan a los gestores de riesgos de TI, evaluar y monitorear el dinamismo de los riesgos de tecnologías de información; así como tampoco propone formas para analizar, medir y documentar el desempeño y efectividad de los controles establecidos a lo largo del proceso de la gestión de riesgos; en igual forma, no se han establecido medidas, procedimientos o políticas para la implementación de auditorías internas o externas, que posibiliten obtener oportunidades para la mejora continua.

De igual forma, se evidencia que esta metodología no propone herramientas y canales de comunicación internos y externos, que puedan utilizar las organizaciones para mantener contacto con los clientes y usuarios, cuando se identifiquen o se activen riesgos de tecnologías de información; de tal forma que, se tenga establecido un protocolo para saber que comunicar, cuando comunicar y a quien comunicar; y de esta forma posibilitar la actuación oportuna y minimizar el impacto en la

organización; del mismo modo, no se han determinado formas o medios para la formación y concientización de los usuarios y propietarios de los activos de información, teniendo en cuenta que se trata de un aspecto fundamental en la estrategia para la implementación y mejora continua de los controles relacionados a los riesgos y su vínculo con la seguridad de la información.

4.3 Resultados descriptivos de similitud entre la Metodología Mehari y la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

Tabla n.º 47

Satisfacción de aspectos y características de la NTP-ISO/IEC 27001:2014 en la metodología *Mehari.*

Metodología Mehari	
Aspecto 1: Determinar el compromiso de la alta dirección	
Liderazgo y compromiso de la alta dirección.	NO
Asignación de roles y responsabilidades.	NO
Asignación de recursos.	NO
Alineación de los objetivos con la estrategia de la organización	NO
Aspecto 2: Definir el alcance.	
Alcance	NO
Aspecto 3: Comprender el contexto de la organización	
Aspectos internos y externos.	SI
Comprender las necesidades y expectativas de las partes interesadas.	SI
Aspecto 4: Activos de información	
Identificar activos de información	SI
Valoración de activos	SI

Aspecto 5: Identificación de riesgos	
Establecer criterios de riesgos.	SI
Identificación de propietarios de riesgos.	SI
Identificar amenazas y vulnerabilidades.	SI
Identificar riesgos.	SI
Aspecto 6: Evaluar el riesgo.	
Valoración de consecuencias potenciales.	SI
Valoración de probabilidad de ocurrencia.	SI
Valoración del impacto.	SI
Aspecto 7: Tratamiento del riesgo	
opciones de tratamiento.	SI
Determinación de controles.	SI
Aspecto 8: Aplicabilidad de controles.	
Declaración de aplicabilidad.	NO
Aspecto 9: Monitoreo y mejora continua	
Monitoreo y evaluación.	SI
Auditorias.	SI
Mejora continua.	SI
Aspecto 10: Concientización y comunicación	
concientización.	SI
Comunicación.	SI
Documentación.	SI

Fuente: Elaboración del autor.

Del análisis realizado a la metodología de Mehari, según lo especificado en la tabla n.º 47, se evidencia, que esta metodología no relaciona el liderazgo de la alta

dirección con el proceso de la gestión de riesgos de tecnologías de información, lo que pone en riesgo que los objetivos, políticas y procedimientos planteados para minimizar los riesgos de TI, pierdan estabilidad, lo que podría generar una tendencia al incumplimiento de los controles y políticas relacionados a estos, por lo que difícilmente se lograrían los resultados esperados.

En relación, a la asignación de roles y responsabilidades; así como, a la asignación de recursos; esta metodología no especifica los mecanismos para asegurar que los roles, funciones y responsabilidades relevantes a la gestión de riesgos de TI, estén asignadas y comunicadas; del mismo modo, se evidencia una falta de integración de la gestión de riesgos de tecnologías de información y la alineación de los objetivos con la estrategia de la organización; lo que imposibilita el cumplimiento de la misión, visión y objetivos estratégicos, así como, obtener el máximo rendimiento de los recursos humanos, materiales y financieros de la organización. En consecuencia, es preciso indicar, que la adopción de una metodología de gestión de riesgos de tecnologías de información es una decisión estratégica para la organización.

Del mismo modo, se evidencian deficiencias para delimitar sobre que procesos, departamentos, dependencias y actividades se establecerá el alcance de la gestión de riesgos de tecnologías de información, lo que no permite identificar sobre que activos de información se aplicará tratamiento de riesgos de TI, y su relación entre los recursos humanos, procesos y tecnologías susceptibles de ser aprovechadas por las vulnerabilidades y amenazas informáticas. De otro lado, se tiene que en la definición del alcance de un sistema de gestión de riesgos de TI se tendrá que conocer el contexto interno y externo de la organización.

Por otro lado, en relación a la Declaración de aplicabilidad, si bien es cierto, es un documento para aquellas empresas que deseen obtener la certificación ISO 2700, no deja de tener importancia, debido a que proporciona una guía para aplicar auditoría interna o externa, ya que en ella se tiene establecido las amenazas, vulnerabilidades y controles a los que se encuentran expuestos los activos de información; así también permite argumentar las decisiones de incluir o excluir determinados controles.

4.4 Resultados descriptivos de similitud entre la Metodología Octave Allegro y la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

Tabla n.º 48

Satisfacción de aspectos y características de la NTP-ISO/IEC 27001:2014 en la metodología *Octave Allegro.*

Metodología Octave Allegro	
Aspecto 1: Determinar el compromiso de la alta dirección	
Liderazgo y compromiso de la alta dirección.	SI
Asignación de roles y responsabilidades.	NO
Asignación de recursos.	SI
Alineación de los objetivos con la estrategia de la organización	SI
Aspecto 2: Definir el alcance.	
Alcance	SI
Aspecto 3: Comprender el contexto de la organización	
Aspectos internos y externos.	SI
Comprender las necesidades y expectativas de las partes interesadas.	SI
Aspecto 4: Activos de información	

Identificar activos de información	SI
Valoración de activos	SI
Aspecto 5: Identificación de riesgos	
Establecer criterios de riesgos.	SI
Identificación de propietarios de riesgos.	SI
Identificar amenazas y vulnerabilidades.	SI
Identificar riesgos.	SI
Aspecto 6: Evaluar el riesgo.	
Valoración de consecuencias potenciales.	SI
Valoración de probabilidad de ocurrencia.	SI
Valoración del impacto.	SI
Aspecto 7: Tratamiento del riesgo	
opciones de tratamiento.	SI
Determinación de controles.	SI
Aspecto 8: Aplicabilidad de controles.	
Declaración de aplicabilidad.	SI
Aspecto 9: Monitoreo y mejora continua	
Monitoreo y evaluación.	SI
Auditorias.	NO
Mejora continua.	SI
Aspecto 10: Concientización y comunicación	
concientización.	SI
Comunicación.	NO
Documentación.	SI

Fuente: Elaboración del autor.

Para la Metodología Octave Allegro, la alta gerencia es un factor crítico para realizar con éxito la evaluación de gestión de riesgos de tecnologías de información, por lo que esta debe patrocinar y comprometerse en brindar los recursos humanos y financieros con la finalidad de obtener los resultados esperados; sin embargo, no se ha establecido los medios y mecanismos que permitan asignar los roles y responsabilidades vinculados a la asignación, gestión, monitoreo y evaluación de los activos de información en el proceso de gestión de riesgos de tecnologías de información; tal como se observa en la tabla n.º 48.

En igual forma, se observa la ausencia de medidas, procedimientos o políticas para la implementación de auditorías internas o externas, que posibiliten a las entidades determinar el nivel de eficiencia de los controles y/o medidas implantadas en la organización, asimismo, que permitan decidir si los controles implementados son los adecuados para proteger los activos de información, asegurar la integridad de los datos, la verificación de los sistemas y el cumplimiento de las leyes y regulaciones. La planificación e implementación de auditorías permitirá mantener la mejora continua dentro de las entidades, permitiendo minimizar la interrupción de los procesos de negocio.

Por otro lado, se evidencia que esta metodología no propone herramientas y canales de comunicación internos y externos, que permitan a los usuarios y clientes internos y externos informar de los posibles riesgos de TI que presenta el uso activos de información en el marco del desarrollo de las funciones laborales dentro y fuera de la organización; de tal forma que, se tenga establecido un protocolo para saber que comunicar, cuando comunicar, a quien comunicar y quien debe comunicar; y de esta forma posibilitar la actuación oportuna, que permita en el menor tiempo posible implementar los controles para minimizar el impacto en la organización.

Tabla n.º 49

Resultados de las metodologías de gestión de riesgos con la NTP-ISO/IEC 27001:2014.

Aspectos y Características	Magerit V3	Coras	Mehari	Octave Allegro
Aspecto 1: Determinar el compromiso de la alta dirección.				
Liderazgo y compromiso de la alta dirección.	SI	SI	NO	SI
Asignación de roles y responsabilidades.	SI	NO	NO	NO
Asignación de recursos.	SI	NO	NO	SI
Alineación de los objetivos con la estrategia de la organización.	SI	SI	NO	SI
Aspecto 2: Definir el alcance.				
Alcance	SI	SI	NO	SI
Aspecto 3: Comprender el contexto de la organización.				
Aspectos internos y externos.	SI	SI	SI	SI
Comprender las necesidades y expectativas de las partes interesadas.	SI	SI	SI	SI
Aspecto 4: Activos de información.				
Identificar activos de información.	SI	SI	SI	SI
Valoración de activos.	SI	SI	SI	SI
Aspecto 5: Identificación de riesgos.				
Establecer criterios de riesgos.	SI	SI	SI	SI

Identificación de propietarios de riesgos.	NO	SI	SI	SI
Identificar amenazas y vulnerabilidades.	SI	SI	SI	SI
Identificar riesgos.	SI	SI	SI	SI
Aspecto 6: Evaluar el riesgo.				
Valoración de consecuencias potenciales.	SI	SI	SI	SI
Valoración de probabilidad de ocurrencia.	SI	SI	SI	SI
Valoración del impacto.	SI	SI	SI	SI
Aspecto 7: Tratamiento del riesgo.				
opciones de tratamiento.	SI	SI	SI	SI
Determinación de controles.	SI	SI	SI	SI
Aspecto 8: Aplicabilidad de controles.				
Declaración de aplicabilidad.	SI	SI	NO	SI
Aspecto 9: Monitoreo y mejora continua.				
Monitoreo y evaluación.	SI	NO	SI	SI
Auditorias.	SI	NO	SI	NO
Mejora continua.	SI	NO	SI	SI
Aspecto 10: Concientización y comunicación.				
concientización.	SI	NO	SI	SI
Comunicación.	SI	NO	SI	NO
Documentación.	SI	SI	SI	SI

Fuente: Elaboración del autor.

4.5 Determinación del Grado de similitud.

Para la investigación, el grado de similitud se define como la cantidad de requisitos establecidos por la Norma Técnica Peruana NTP-ISO/IEC 27001:2014,

que deben cumplir las metodologías de gestión de riesgos de tecnologías de información.

De esta manera, la investigación ha planteado 25 requisitos (características) relacionados a la gestión de riesgos que fueron extraídos de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014; los cuales deberán cumplir las metodologías de gestión de riesgos de TI, seleccionadas previamente; y conforme a la información mostradas en las tablas n.os 45, 46, 47 y 48 precedentes, se evidencia que la metodología Magerit v3, es la que presenta más criterios relacionados con esta norma, al cumplir 24 de un total de 25 criterios, así mismo, se determinó que, de las cuatro (4) metodologías comparadas, se tiene que la Metodología Coras es la que presenta una menor relación con los criterios previamente establecidos, al determinarse que solo cumple 18 de 25; tal como se observa en la tabla n.º 50.

Tabla n.º 50

Grado de similitud de las metodologías de gestión de riesgos con la NTP-ISO/IEC 27001:2014.

Cantidad de requisitos	Magerit V3	Coras	Mehari	Octave Allegro
Cumple	24	18	19	22
No cumple	1	7	6	3
Total	25	25	25	25

Fuente: Elaboración del autor.

Del análisis precedente, se tiene que la Metodología Magerit V3 presenta un 96 por ciento (96%) de similitud a los aspectos y características vinculados a la gestión de riesgos planteados en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014; en

contraste con las demás metodologías de gestión de riesgos de tecnologías de información estudiadas; tal como se describe en la tabla n.º 51.

Tabla n.º 51

Porcentaje de cumplimiento de requisitos de las metodologías de gestión de riesgos con la NTP-ISO/IEC 27001:2014.

Metodologías	**Magerit V3**	**Coras**	**Mehari**	**Octave Allegro**
Porcentaje	0.96	0.72	0.76	0.88

Fuente: Elaboración del autor.

Capitulo V: DISCUSIÓN

En este apartado, se analizarán y se discutirán los resultados obtenidos en la sección anterior.

En primer lugar, se eligieron los mecanismos de comparación de estándares basados en un aspecto formal, en ese sentido, se discuten los resultados obtenidos con la tesis de Gasca (2011) sobre *"Estudio de similitud del proceso de gestión de riesgos en proyectos de outsourcing de software: utilización de un método"*, utilizó un método de mapeo de estándares y modelos basado en el Método de estudio de similitud entre modelos y estándares (MSSS), y obtuvo como resultado al modelo CMMI-ACQ, el cual presentó más características relacionadas con la gestión de riesgos dentro del outsourcing de software; situación similar se obtuvo en la presente investigación, toda vez que usando la adaptación del Método MSSS se pudo evidenciar que la Metodología de gestión de riesgos Magerit V3 presenta una mayor de similitud con la gestión de riesgos planteados en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

Del mismo modo, Prieto, Meneses, & Vega, (2015) en su investigación "Análisis comparativo de modelos de madurez en inteligencia de negocios" aplicó el método MESME para identificación y comparación de similitudes en modelos de gestión de inteligencia de negocios (BI), el cual ayudó a ponderar los elementos del modelo de madurez e identificó al modelo Enterprise Intelligence como modelo de referencia; no obstante, se identificó que el método MESME presenta similares pasos de comparación al método MSSS; en ese marco, la presente investigación usó la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 como modelo de referencia.

Así mismo, se revisaron y analizaron las metodologías de gestión de riesgos de tecnologías de información más importantes y vigentes en el mercado; en esa perspectiva,

se discuten los resultados obtenidos con la tesis de Crespo (2016) denominada *"Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES"* vinculada al sector ecuatoriano, donde analizó las metodologías de gestión de riesgos CRAMM, OCTAVE-S, Microsoft Risk Guide, COBIT 5 y COSO III con la finalidad de crear una metodología propia, y obtuvo como resultado la metodología ECU@Risk; asimismo, indicó que la Metodología Magerit es la más completa, al proporcionar un marco de trabajo para la toma de decisiones en gestión de riesgos; la cual guarda relación con los resultados obtenidos en la presente investigación, toda vez que se establecieron criterios de selección para la elección de metodologías y se obtuvo que la Metodología Magerit V3 presenta un 96 por ciento (96%) de similitud en los aspectos y características vinculados a la gestión de riesgos planteados en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

CONCLUSIONES

1. El objetivo de esta investigación abordó el problema relacionado a encontrar una metodología de gestión de riesgos de tecnología de información que mejor se relacione con la Norma Técnica Peruana NTP - ISO/IEC 27001:2014; en ese sentido, se realizó un análisis de las metodologías de gestión de riesgos de tecnologías de información más importantes en el mercado, conforme a seis criterios de selección (documentación oficial, accesibilidad a documentación, herramientas de análisis de riesgos, vigencia, aplicable al sector estatal y reconocimiento internacional) diseñados para este trabajo investigativo, y se obtuvo como resultado que, de un total de siete (7) metodologías analizadas, solo cuatro (4) de ellas (Magerit V3, Coras, Mehari y Octave Allegro) cumplieron el 100% los criterios de selección; metodologías que finalmente fueron comparadas con la Norma Técnica Peruana NTP - ISO/IEC 27001:2014.
2. Se determinó que la metodología Magerit V3, es la metodología de gestión de riesgos de tecnologías de información que más se relaciona con la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, al presentar un 96% de similitud; en ese sentido, se evidenció que esta metodología presenta un alto grado de semejanza con los aspectos y características definidas en la NTP-ISO/IEC 27001:2014 vinculados a la gestión de riesgos, de tal forma, que se ha disminuido la incertidumbre en la selección de la metodología a usar en la implementación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, para las instituciones del estado peruano.
3. Se estableció que la metodología Magerit V3 se constituye en una metodología madura en la gestión de riesgos de tecnologías de información

para instituciones estatales, toda vez que, cumplió con criterios diseñados para esta investigación, la misma que para su identificación, se adaptó el Método de Estudio de Similitud entre Modelos y Estándares (MSSS), el cual es un método estructurado y formal de comparación establecido en investigaciones internacionales.

RECOMENDACIONES

- Se sugiere realizar estudios complementarios en campo, que permitan determinar la factibilidad técnica y económica de la metodología de gestión de riesgo Magerit V3 de acuerdo a la Norma Técnica Peruana NTP - ISO/IEC 27001:2014 en las entidades del estado peruano.

- Se recomienda determinar la adopción, formalización e implementación de políticas agiles vinculadas a la gestión de riesgos de tecnologías de información.

BIBLIOGRAFIA

(2012). En *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro I Método* (pág. 56). Madrid: Ministerio de Hacienda y Administraciones Públicas.

(05 de 04 de 2020). Obtenido de CCN - CERT: https://www.ccn-cert.cni.es/soluciones-seguridad/ear-pilar.html

Alberts, C., Behrens, S., Pethia, R., & Wilson, W. (1999). *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) Framework, Version 1.0.* Pittsburgh: Carnegie Mellon University.

Bribiesca, G., Carrillo, V., Corona, A., Cruz, E., Ramirez, Y., Ramirez, M., . . . Torres, R. (2016). *Tecnologías de información y comunicación en las organizaciones.* Mexico: Publicaciones Empresariales UNAM. FCA Publishing.

Calvo-Manzano, J. A., Cuevas Augustin, G., San Feliu Gilabert, T., & Muñoz, M. (2008). Process similarity study: Case study on project planning practices based on CMMI-DEV v1. 2. *EuroSPI 2008 Industrial Proceedings* (págs. 11.13 - 11.23). ISCN y Dublin City University.

Caralli, R., Stevens, J., Young, L., & Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* USA: Carnegie Mellon University.

Carnegie Mellon University. (2007). Obtenido de https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419

Carralli, R. A., Stevens, J. F., & William, Y. (2007). *OCTAVE Allegro: mejora del proceso de evaluaciòn de riesgos de seguridad de información.* Carnegie Mellon University.

CORAS. (05 de 04 de 2020). Obtenido de http://coras.sourceforge.net/index.html

Crespo Martinez, P. E. (2016). *Metodologia de seguridad de la información para la gestión del riesgo informático aplicables a MPYMES.* Cuenca, Ecuador.

Del Carpio Wong, M. (2016). *http://peru.gob.pe.* Obtenido de http://peru.gob.pe/pm/portales/portal_ongei/docs/ONGEI.pdf

Dirección General de Modernización Administrativa, P. e. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

EDESA. (05 de 04 de 2020). Obtenido de https://www.edesaesp.com.co/wp-content/uploads/2013/05/ASNZ-4360-de-1999.pdf

Gasca Hurtado, G. P. (2010). Estudio de similitud del proceso de gestion de riesgos en proyectos de outsourcing de software: utilización de un metodo. *Revista ingenierias Universidad de medellin*, 119-130.

Gil-Garcia, R., Criado, I., & Tellez, J. (2017). *Tecnologías de información y comunicacíon en la administración pública: Conceptos, enfoques, aplicaciones y resultados.* México: INFOTEC.

Guia para el metodo Coras. (2011). Berlin: Springer-Verlag.

Javier Santiago, E., & Sanchez Allende, J. (2017). Riesgos de ciberseguridad en las empresas. *Tecnologi@ y desarrollo*.

Jouas, J.-P., Cobija, J.-R., Duperrin, G., Gouin, G., Jolivet, C., Libertad, B., . . . Rollos, J. (2017). *Mehari: Guía de análisis y tratamiento de riesgo.* CLUSIF.

Laudon, K., & Laudon, J. (2012). *Sistemas de Información Gerencial.* México: Pearson Education.

MAGERIT – versión 3.0 Metodologia de Analisis y Gestión de Riesgos de los Sistemas de Informacion - Libro II - Catalogo de Elementos. (2012). Madrid: Ministerio de Hacienda y Administraciones Públicas.

MEHARI 2010 - Conceptos fundamentales y especificaciones funcionales. (2010). Paris: Club de Seguridad de la Información de Francia.

MEHARIPEDIA. (2017). Obtenido de http://meharipedia.x10host.com/wp/

NIST. (09 de 2012). Obtenido de https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Noraini Che, P., & Bokolo, A. (2015). A Model of Mitigating Risk For IT. *4th International Conference on Software Engineering and Computer Systems (ICSECS),*, (págs. 49-54). Malaysia.

Pareek, M. (2011). Medicion y elaboracion de informes de riesgos tecnologicos. *ISACA Journal*.

Prieto Morales, R., Meneses Villegas, C., & Vega Zepeda, V. (2015). Analisis comparativo de modelos de madurez en inteligencia de negocios. *Revista Chilena de Ingeniería*, 361-371.

Ramirez castro, A., & Ortiz Bayona, Z. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad del negocio. *Ingenieria*, 56-66.

Seclén Arana, J. A. (2016). *Factores que afectan la implementación del sistema de gestion de la seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001*. Lima.

Standards New Zealand. (05 de 04 de 2020). Obtenido de https://shop.standards.govt.nz/search/ed

Valencia, F., Marulanda, C., & López, M. (2016). Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional. . *Gerencia tecnológica informática*, 65-77.

Wikipedia. (14 de 09 de 2018). Obtenido de https://en.wikipedia.org/wiki/Simple_matching_coefficient

Anexo n. 01

Plantilla n.º 01 - “Estudio de características y criterios”

Aspectos n	Argumentación
Característica 1	
Característica 2	
Característica 3	
Característica 4	
.	
.	
.	
Característica n	

Fuente: Elaboración del autor.

Anexo n. 02

Plantilla n.º 02 – "Verificador de cumplimiento de características y criterios"

Metodología …	Cumple (SI / NO)
Aspecto 1	
Característica 1	
Característica 2	
.	
.	
.	
Característica n	
Aspecto 2	
Característica 1	
Característica 2	
.	
.	
Característica n	

Fuente: Elaboración del autor.

Anexo n. 03

Plantilla n.º 03 - "Comparador de características y criterios"

Aspectos y Características	Metodología 1 cumple (SI / NO)	Metodología 3 cumple (SI / NO)	Metodología 3 cumple (SI / NO)	Metodología n cumple (SI / NO)
Aspecto 1				
Característica 1				
Característica 2				
Característica 3				
.				
.				
.				
Característica n				
Aspecto 2				
Característica 1				
Característica 2				
Característica 3				
.				
.				
.				
Característica n				

Fuente: Elaboración del autor.

ANEXO 01

CONSTANCIA DE APROBACIÓN DE ORIGINALIDAD DE TESIS

Yo, Regis Jorge Alberto Diaz Plaza, Docente Revisor del trabajo de investigación[1], del estudiante, Luciano Llauce Valdera

Titulada:
Análisis comparativo de metodologías de gestión de riesgos de tecnologías de la información en el marco de la NTP - ISO/IEC 27001:2014,

luego de la revisión exhaustiva del documento constato que la misma tiene un índice de similitud de 18% verificable en el reporte de similitud del programa Turnitin.

El suscrito analizó dicho reporte y concluyó que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad Nacional Pedro Ruiz Gallo.

Lambayeque, 14 de marzo del 2022

……
DR. REGIS JORGE ALBERTO DIAZ PLAZA
DNI: 16620941
ASESOR

Se adjunta:

Resumen del Reporte (Con porcentaje y parámetros de configuración)

Recibo digital.

UNPRG
UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Tesis

INFORME DE ORIGINALIDAD

18%	18%	4%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repository.unimilitar.edu.co Fuente de Internet	1%
2	bibdigital.epn.edu.ec Fuente de Internet	1%
3	ruidera.uclm.es Fuente de Internet	1%
4	dspace.ucuenca.edu.ec Fuente de Internet	1%
5	dspace.udla.edu.ec Fuente de Internet	1%
6	polux.unipiloto.edu.co:8080 Fuente de Internet	1%
7	repository.unad.edu.co Fuente de Internet	1%
8	bdigital.unal.edu.co Fuente de Internet	1%
9	repository.ucatolica.edu.co Fuente de Internet	<1%

.....
DR. REGIS JORGE ALBERTO DIAZ PLAZA
DNI: 16620941
ASESOR

10	tesis.usat.edu.pe Fuente de Internet	<1 %
11	hdl.handle.net Fuente de Internet	<1 %
12	qdoc.tips Fuente de Internet	<1 %
13	1library.co Fuente de Internet	<1 %
14	segredip.blogspot.com Fuente de Internet	<1 %
15	repositorio.upn.edu.pe Fuente de Internet	<1 %
16	www.dspace.espol.edu.ec Fuente de Internet	<1 %
17	Submitted to Escuela Politecnica Nacional Trabajo del estudiante	<1 %
18	revistas.udistrital.edu.co Fuente de Internet	<1 %
19	repositorio.ugm.cl Fuente de Internet	<1 %
20	fcqi.tij.uabc.mx Fuente de Internet	<1 %
21	repositorioacademico.upc.edu.pe Fuente de Internet	<1 %

22	Submitted to Universidad Tecnológica Israel Trabajo del estudiante	<1 %
23	www.ongei.gob.pe Fuente de Internet	<1 %
24	www.iso27000.es Fuente de Internet	<1 %
25	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	<1 %
26	Submitted to Universidad Nacional Abierta y a Distancia, UNAD,UNAD Trabajo del estudiante	<1 %
27	asistencia-acreditacion.blogspot.com Fuente de Internet	<1 %
28	openaccess.uoc.edu Fuente de Internet	<1 %
29	documents.mx Fuente de Internet	<1 %
30	www.coursehero.com Fuente de Internet	<1 %
31	www.pcm.gob.pe Fuente de Internet	<1 %
32	creativecommons.org Fuente de Internet	<1 %
33	www.ccn-cert.cni.es Fuente de Internet	

Recibo digital

Este recibo confirma quesu trabajo ha sido recibido por Turnitin. A continuación podrá ver la información del recibo con respecto a su entrega.

La primera página de tus entregas se muestra abajo.

Autor de la entrega:	Luciano LLAUCE VALDERA
Título del ejercicio:	tesis1
Título de la entrega:	Tesis
Nombre del archivo:	LUCIANO_LLAUCE_VALDERA.docx
Tamaño del archivo:	872.97K
Total páginas:	112
Total de palabras:	24,965
Total de caracteres:	144,572
Fecha de entrega:	06-mar.-2022 04:14p. m. (UTC-0500)
Identificador de la entre...	1777772449

UNIVERSIDAD NACIONAL
"PEDRO RUÍZ GALLO"
ESCUELA DE POSGRADO

MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN GERENCIA DE TECNOLOGÍAS DE INFORMACIÓN Y GESTIÓN DE SOFTWARE

"Análisis Comparativo de Metodologías de Gestión de Riesgos de Tecnologías de la Información en el Marco de la NTP - ISO/IEC 27001:2014"

TESIS

Presentada para optar el Grado Académico de Maestro en Ingeniería de Sistemas con mención en Gerencia de Tecnologías de la Información y Gestión del Software

AUTOR:
Bach. Luciano Llauce Valdera

ASESOR:
Regis Jorge Alberto Díaz Plaza

Lambayeque, Perú
2021