UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

IMPLEMENTACIÓN DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN ESTÁNDARES INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:

Bach. Guevara Chambergo Jhon Dennis
https://orcid.org/0000-0003-3453-4433

Asesor:

Mg. Cachay Maco Junior Eugenio

https://orcid.org/0000-0003-4056-3142

Línea de Investigación:
Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú 2021

APROBACIÓN DEL JURADO

IMPLEMENTACIÓN DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN ESTÁNDARES INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA

_____

Bach. Guevara Chambergo Jhon Dennis

_____

Mg. Ing. Cachay Maco Junior Eugenio

Asesor

_____ _____

Mg. Sialer Rivera María Noelia

Presidente de Jurado

Mg. Chirinos Mundaca Carlos Alberto

Secretario de Jurado

_____

Mg. Ing. Cachay Maco Junior Eugenio

Vocal de Jurado

Dedicatorias

Mi tesis la dedico con todo mi amor y cariño a mis padres y familia en general, por ser mi fuente de motivación e inspiración para poder superarme cada día, por sus palabras de aliento que me motivaban a seguir adelante y siempre ser perseverante en mis metas y objetivos y por su apoyo incondicional que me brindan cada día. Les agradezco, y hago presente mi gran afecto hacia ustedes.

Guevara Chambergo Jhon Dennis

Agradecimientos

Al concluir esta etapa maravillosa de mi vida quiero agradecer profundamente a Dios por permitirme vivir y disfrutar de mi familia en estos momentos difíciles, gracias a mi familia por apoyarme en cada decisión y proyecto de mi vida, gracias a la vida porque cada día me demuestra lo hermosa y justa que puede llegar a ser, gracias a mi familia por creer en mí y motivarme a cumplir con el desarrollo de esta tesis.

Guevara Chambergo Jhon Dennis

Resumen

Las tecnologías de la cuarta revolución industrial motivan el crecimiento económico mundial de forma eficiente, sin embargo, este mismo crecimiento, obliga a las organizaciones a evaluar los riesgos que amenazan su estabilidad económica. Estudios relacionados con la seguridad de la información consideran que es importante conocer, analizar, evaluar y tratar eficientemente los riesgos de una organización, evitando un exceso de confianza en la gestión, permitiendo probabilidades relativas de ocurrencia entre los diferentes tipos de incidentes de seguridad incluida la seguridad cibernética. Estándares como la norma ISO/IEC 27005 proporcionan directrices para gestionar estos riesgos que apoyados en metodologías brindan un uso e implementación efectiva en la organización; pero existen estimaciones no alineadas a la realidad, sobre los ataques cibernéticos, afectando el rendimiento de los procesos y la complejidad de los mismos. El trabajo buscó establecer confianza en sus resultados, por ende se desarrolló una metodología de gestión de riesgos de seguridad basado en la metodología TARA y MAGERIT, apoyado en un marco de trabajo como RISK IT, basado en el estándar internacional ISO/IEC 27005, que ayudó a la organización a identificar activos, vulnerabilidades, contramedidas y estrategias de selección de riesgos, con el fin de elaborar un plan de tratamiento de riesgos que apoye la gestión de riesgos empresarial, manifestando un nivel de integración adecuado. Con ello las PYMEs podrán guiarse del producto de este trabajo para dar su primer paso en la seguridad de la información, así el personal no cuente con mucha experiencia en el manejo de los conceptos relacionados, debido a que posee una complejidad media en sus 4 procesos. Estos procesos se integraron en un 50% con el estándar ISO/ IEC 27005 y en un 33% en con MAGERIT, TARA y RISK IT obteniendo un rendimiento de 1.10 días hábiles en su implementación.

Palabras Clave:

ISO 27005, Gestión de Riesgos, MAGERIT, Metodologías, RISK IT, Seguridad de Información, TARA.

Abstract

The technologies of the fourth industrial revolution are driving global economic growth in an efficient manner, however, this same growth forces organizations to evaluate the risks that threaten their economic stability. Studies related to information security consider that it is important to know, analyze, evaluate and efficiently treat the risks of an organization, avoiding overconfidence in management, allowing relative probabilities of occurrence among the different types of security incidents including cyber security. Standards such as ISO/IEC 27005 provide guidelines for managing these risks that, supported by methodologies, provide an effective use and implementation in the organization; but there are estimates that are not aligned with reality, about cyber-attacks, affecting the performance of processes and their complexity. The work sought to establish confidence in its results, therefore a security risk management methodology was developed based on the TARA and MAGERIT methodology, supported by a framework such as RISK IT, based on the international standard ISO/IEC 27005, which helped the organization to identify assets, vulnerabilities, countermeasures and risk selection strategies, in order to develop a risk treatment plan that supports enterprise risk management, showing an adequate level of integration. With this, the SMEs can be guided by the product of this work to take their first step in information security, even if the personal does not have much experience in the handling of the related concepts, due to the fact that it has a medium complexity in its 4 processes. These processes were integrated 50% with the ISO/IEC 27005 standard and 33% with MAGERIT, TARA and RISK IT, obtaining a performance of 1.10 working days in its implementation.

Keywords:

ISO 27005, Risk Management, MAGERIT, Methodologies, RISK IT, Information Security, TARA.

Índice

I. INTRODUCCIÓN

1.1. Realidad Problemática.

Las tecnologías de la cuarta revolución industrial, tales como, la inteligencia artificial, redes 5G, dispositivos de internet de las cosas, tecnologías en la nube y blockchain, motivan el crecimiento económico mundial de forma eficiente, sin embargo, este mismo crecimiento, obliga a las organizaciones a evaluar los riesgos que amenazan su estabilidad económica debido a la alta dependencia digital.

Según el informe *The Global Risks Report 2021* de World Economic Forum, (2021), en el Perú, el 60% de la población son usuarios activos de internet, evidenciando de esta manera, que la capacidad diferencial para acceder a datos y tecnologías digitales, es un indicador de crecimiento económico para el país, tal es el caso que en el mismo informe, los países Qatar y los Emiratos Árabes Unidos, presentan un 99.7% y 99.1% respectivamente, como porcentaje de su población activa con acceso a datos y tecnologías digitales. Es importante resaltar estos datos, debido a que, en el mismo informe, se realizó una encuesta a nivel mundial respecto a la percepción de materialización de un riesgo crítico a corto plazo para la empresa que dirige, colocando en cuarto lugar a las fallas de ciberseguridad, y en primer lugar a las enfermedades infecciosas, esto último, debido al panorama mundial de la pandemia del virus COVID-19. (Ver Figura 1).

Por ende, al estar los fallos de ciberseguridad en una posición relevante de riesgos para las empresas, muchas empresas aseguradoras han considerado soluciones de ciber resiliencia, con el objetivo de tratar los ciber riesgos como otros riesgos que pueden transferirse a una aseguradora. Estas aseguradoras, por lo tanto, están invirtiendo tiempo y presupuesto en investigaciones de identificación de ciber riesgos.

Figura 1. Percepción de riesgos críticos a corto plazo (0 – 2 años). Fuente: *World Economic Forum* (2021).

Según el informe *Hiscox Cyber Readiness Report* de Hiscox, (2021), empresa proveedora de seguros para empresas desde 1901, las empresas se encuentran centrando el gasto de tecnologías de la información en la resiliencia cibernética para gestionar los crecientes ataques. Evidenciando que 38% a 43% de las empresas aseguradas han sufrido por lo menos un ataque, en algunos casos, ataques múltiples, y uno de cada seis empresas atacadas mencionaron que su supervivencia se encontraba amenazada. El mismo informe, detalla el nivel de madurez en ciberseguridad de las empresas aseguradas, según el framework de medición de COBIT y la arquitectura de seguridad SABSA, donde se obtuvo en promedio general el valor de nivel 3.03 de 5, demostrando que las empresas mantienen un nivel adecuado de gestión de riesgos de seguridad de la información.

La norma internacional ISO 31000 de International Organization for Standardization, (2009), establece la estructura de procesos que los modelos de gestión de riesgos empresariales deben presentar en las organizaciones. Por ello, varias metodologías, tales como RISK IT, OCTAVE, MAGERIT, entre otras, toman como base esta norma, estableciendo las fases regulares de identificación de riesgos, análisis de riesgos y tratamiento de riesgos.

Según Eling, McShane y Nguyen, (2021), una de las causas de que la eficiencia de la gestión de riesgos obtiene una percepción negativa es debido a que los equipos de alta dirección durante la identificación de riesgos, no se encuentran preparados para prevenir o manejar las consecuencias causadas por la nueva generación de ciberataques, tales como deepfakes, envenenamiento por aprendizaje automático y contratos inteligentes de hacking. Además, durante la fase de análisis de riesgos, existe un exceso de confianza en la gestión permitiendo probabilidades relativas de ocurrencia entre los diferentes tipos de incidentes de seguridad cibernética, esto habilita una estimación no alineada a la realidad, sobre los ataques cibernéticos, afectando las opciones de selección de tratamientos de riesgos. Muchos de los analistas de riesgos cibernéticos, no consideran indicadores de otras regiones geográficas, o cómo las diferencias culturales afectan en el enfrentamiento legal al cibercrimen. Sin embargo, el factor más relevante respecto al análisis de ciber riesgos, es la falta de consideración de métodos cuantitativos para la valoración de riesgos, ya sea con uso de probabilidades bayesianas o redes neuronales artificiales. Para la fase de tratamiento de riesgos, se ha evidenciado en el informe, que las empresas no cuentan con una base de datos de pérdidas financieras sufridas por motivo de fallas de ciberseguridad, ni tampoco realizan una investigación posterior de los incentivos de los atacantes y las víctimas de eventos de pérdida cibernética.

Para Falco, et al., (2019), uno de los retos más complejos para los responsables de ciberseguridad en las empresas, es la proyección integral que debe tener la gestión de ciber riesgos con la gestión de riesgos empresarial, sobre todo si las organizaciones presentan accionistas o grupos de interés preocupados en el valor bursátil. La norma internacional ISO 31000 de International Organization for Standardization, (2009), es una de las primeras normas enfocadas en la gestión de riesgos integral de una empresa, y en conjunto con COSO, se ha convertido en el mercado como una de las opciones más utilizadas para el enfoque integral.

La presente investigación buscó aportar mediante un análisis de bases de datos científicas y casos de estudios de aplicación de metodologías o modelos ad hoc de gestión de riesgos de seguridad de la información, e identificó los resultados obtenidos según el problema particular detectado en la gestión de ciber riesgos, diseñar una metodología ad hoc para una pequeña empresa manufacturera de la ciudad, considerando las características relevantes para su implementación. El trabajo buscó establecer confianza en sus resultados, por ende, la metodología ad hoc de gestión de riesgos de seguridad de la información, fue validada por expertos relacionados al tema y se analizaron los resultados esperados.

1.2. Trabajos previos.

Sayyed G, (2020), realizó la investigación, UAE Cyber Security Perception and Risk Assessments Compared to Other Developed Nations, en Emiratos Árabes Unidos (UAE). La implementación de metodologías de gestión de ciber riesgos involucra tener un claro entendimiento de las diversas definiciones respecto a los conceptos relacionados, sin embargo, la falta de información según el rubro de la organización a implementar la metodología, repercute en los resultados de gestión. Para ello los investigadores estudiaron las características representativas para la percepción y comportamiento de riesgo de ciberseguridad, y aplicaron encuestas y análisis de datos estadísticos, con el fin de elaborar un instrumento de medición de riesgo relativo en la ciudadanía. Por esta razón, diseñaron un cuestionario con preguntas relacionadas a la percepción y comportamiento en ciberseguridad, el cual aplicaron a 350 participantes de diferentes regiones de UAE. Este cuestionario obtiene el RR o Riesgo Relativo del país, que es un valor cuantitativo calculado en base a las respuestas. Los resultados obtenidos mostraron dos gráficos comparativos: a. Un gráfico comparativo entre el Riesgo Relativo y el índice de ciberseguridad global de los 9 países estudiados (US, UK, Canada, Australia, Suecia, Japón, Alemania, Francia, Brasil y UAE). En todos los casos, el RR era mayor al ICG o Indicador Global de Ciberseguridad. b. Un gráfico que muestra la relación entre pérdidas millonarias por cibercrimen contra su ICG, en los nueve países evaluados. Se evidenció que 2 de 9 países (US y Brasil) no mostraban relación

entre estos dos indicadores. El instrumento elaborado ayudará a los países a calcular su riesgo relativo y compararlo con indicadores globales como ICG y permitir reforzar esfuerzos en ciberseguridad a nivel de estratégicas nacionales. El reforzamiento de conciencia de los ciudadanos en ciberseguridad permitirá incrementar otros niveles económicos como consecuencia y repercusión de lucha contra el cibercrimen. Los Emiratos Árabes Unidos se encuentran en un nivel estándar de ciberseguridad a la par con otras potencias mundiales.

Carnero, Carbajal, Armas, & Madrid, (2020), realizaron la investigación, Information security risk management model for mitigating the impact on SMEs, en Perú. Con la finalidad de identificar las amenazas a las que las PYMEs del Perú se encuentran expuestas, los autores propusieron un modelo divido en 3 fases. Para la primera fase del modelo relaconada con la identificación del activo crítico de riesgo, utilizaron MAGERIT; para la segunda fase que estuvo relacionada con el tratamiento se basaron en las pautas que la norma ISO 31000 brinda para este proceso y para la tercera fase establecieron objetivos relacionados con el rendimiento y los criterios de éxito apoyados de la norma ISO /IEC 27004. En la implementación del método identificaron 21 activos que fueron analizados utilizando ficha de captura establecidas en MAGERIT, de estos activos 17 se identificaron como críticos. Además, se identificaron 46 amenazas de las cuales el 30% fueron identificadas como amenazas críticas, las salvaguardas fueron identificadas con la herramienta PILAR y 15 controles de procedimiento y prevención. Estos controles seleccionados permitieron que se redujera de un 71% a un 67.6% el impacto acumulado.

Tran, Thiriet, Marchand, El Mrabti y Luculli, (2019), realizaron la investigación, Methodology for risk management related to cyber-security of Unmanned Aircraft Systems, en Francia. Los sistemas aéreos no tripulados presentan tecnologías complejas los cuales necesitan de una gestión de riesgos de ciberseguridad ante posibles ataques terroristas. Por esta razón los investigadores diseñaron una metodología ad hoc analizando el estándar ISO 27005 y las herramientas FMVEA, árbol de ataques, EVITA, MEHARI, ED202A/DO326 y SORA. Posteriormente aplicaron la metodología propuesta

en la empresa Sogilis Company, plasmando los resultados en un caso de estudio. La metodología construida, consideró las fases de: a. Establecimiento de contexto utilizando JARUS-SORA, b. Identificación de riesgos utilizando árbol de ataques, c. Análisis y evaluación de riesgos utilizando la guía ED202A/DO326, d. Tratamiento de riesgos utilizando la guía ED202A/DO326. Los resultados obtenidos mostraron que en el caso de estudio se construyeron 6 árboles de ataques, y se obtuvieron 24 requerimientos de ciberseguridad, que nacieron tras analizar 3 escenarios de funcionamientos defectuosos donde se afectaba la disponibilidad, la integridad o la confidencialidad de la información. Se construyó una metodología adaptable al proceso de desarrollo de una aeronave no tripulada de la empresa Sogilis Company en Francia. Los límites de esta metodología propuesta se centran en que las aplicaciones software de las naves no tripuladas ya deben estar definidas.

Svilicic, Kamahara, Rooks y Yano, (2019), realizaron la investigación, Maritime Cyber Risk Management: An Experimental Ship Assessment, en Croacia y Japón. Los sistemas de una embarcación transnacional presentan sistemas informáticos complejos, exigiendo una metodología ad hoc de gestión de ciber riesgos que proteja la información de las navegaciones. Los investigadores propusieron un método el cual consta de actividades de preparación de evaluaciones, realización de evaluaciones y comunicación de resultados, las actividades involucradas fueron, actividades: 1. Caracterización de ciber sistemas, 2. Identificación de sistemas y activos críticos, 3. Consideraciones tecnológicas y de arquitectura, 4. Encuesta sobre ciberseguridad a bordo del barco, 5. Escaneo de ciber vulnerabilidades, 6. Determinación de ciber riesgos (impacto y frecuencia), 7. Informe de evaluación, 8. Recomendaciones para la mitigación de riesgos, 9. Presentación de resultados (gerentes y operadores de la embarcación). El escaneo computacional de vulnerabilidades del sistema de información y visualización de cartas electrónicas (ECDIS) del barco se presenta como una parte específica de esta evaluación de seguridad cibernética. La conducta de evaluación se basa en una encuesta desarrollada y realizada al entrevistar a la tripulación de un barco. Los resultados obtenidos mostraron que, con la propuesta, se detectaron 7 ciber vulnerabilidades, 2 de nivel alto, 4 de

nivel medio y 1 de nivel bajo. Además, se detectaron 9 ciber amenazas, 3 con probabilidad del 50%, 4 con probabilidad del 20% y 2 con probabilidad del 10%. De esas 9 ciberamenazas, 2 tuvieron un impacto de 100, 1 de impacto 90, 2 de impacto 80, 1 de impacto 15 y 3 de impacto 10. La aplicación de la propuesta se realizó en el buque escuela Fukae-maru de la Universidad de Kobe. Se logró realizar un análisis de riesgo cibernético cuantitativo para evaluar los riesgos cibernéticos del buque. El proceso de evaluación presentado es integral y aplicable a todos los barcos, y ofrece pautas para mitigar los riesgos cibernéticos y mejorar el nivel de seguridad cibernética de los sistemas y activos cibernéticos críticos del barco.

Shettya, et al., (2018), realizaron la investigación Reducing Informational Disadvantages to Improve Cyber Risk Management, en Estados Unidos. Las organizaciones que gestionan ciber riesgos y eligen como opción de tratamiento de riesgos la transferencia de responsabilidad a una empresa aseguradora, necesitan contar con una herramienta que permita medir de manera eficaz los riesgos y sus pérdidas relacionadas. La propuesta fue desarrollada por los autores de NIST, y considera: a. Descubrimiento automático de vulnerabilidades, b. Análisis de propagación lateral, c. Métricas de seguridad, d. Plan de mitigación priorizada y e. Cumplimiento con un marco de ciberseguridad. El método propuesto manifiesta una evaluación cuantitativa de la explotación y el impacto de los ciberataques. La herramienta construida consiste en 5 fases: 1. Mapear sistemas y redes para establecer las dependencias entre activos, 2. Descubrimiento de vulnerabilidades, 3. Generar gráfico de ataques, 4. Generar gráfico bayesiano de ataques, 5. Puntuar los ciber riesgos. Al aplicar la herramienta a dos redes de una misma organización, se obtuvo que la red 1 tuvo un puntaje de 3.5 de 10, y la red 2 un puntaje de 4 de 10. Dentro de la red 1, se identificaron 4 activos, de los cuales obtuvieron los siguientes puntajes de riesgo: 4.3, 3.2, 3.2 y 3.2. Dentro de la red 2, se identificaron 5 activos, de los cuales se obtuvieron los siguientes puntajes: 4.9, 3.8, 3.8, 3.8 y 3.2. La propuesta de nombre CRISM es una herramienta de monitoreo directo que investiga las redes organizacionales con información de vulnerabilidad continuamente actualizada integrada con efectos potenciales

sobre los valores de los activos corporativos relacionados. CRISM produce puntajes de riesgo que pueden ser utilizados por los suscriptores de seguros y también por los gerentes de riesgo empresarial y los oficiales de seguridad de la información para priorizar la mitigación del riesgo cibernético. Si bien CRISM puede ser una herramienta útil tanto para las aseguradoras como para los asegurados, las organizaciones naturalmente dudan en permitir el acceso externo a las redes corporativas.

Rea Guaman, Calvo Manzano y San Feliu, (2018), realizaron el estudio A Prototype to Manage Cybersecurity in Small Companies, en España. Las pequeñas empresas cuentan con poco presupuesto para invertir en seguridad de la información, y por tal motivo, necesitan contar con una metodología ad hoc de gestión de riesgos de ciberseguridad, que evite la complejidad y demora en la implementación. El método para la construcción siguió lo siguiente: a. Estudiar las normas relacionadas y herramientas existentes para la gestión de ciberseguridad. b. Análisis de características y particularidades de herramientas seleccionadas, c. Descripción de los conceptos utilizados, d. Definición de los procesos de la propuesta. La herramienta construida, estudió las normas BS 7799, las normas de la familia ISO 27000 y la NIST 800-53, además de las herramientas RISICARE, MSAT, PILAR y SE Risk. Los conceptos que manejó fueron: activos, categorías de activos, vulnerabilidades y amenazas, dimensión de valoración, vulnerabilidad, amenaza y riesgo. Dentro del prototipo se utilizaron escalas de cuantificación y una matriz de calor para la ubicación de los riesgos identificados. Los resultados mostraron que el prototipo construido se automatizó en Microsoft Excel, y utilizaron datos simulados para la demostración de ejemplo. La validación y la implementación del prototipo se realizará en Ecuador con mejoras en la interfaz para optimizar la experiencia del usuario. Como conclusión final, los autores indicaron la deficiencia de sistemas informáticos orientados a la gestión de las vulnerabilidades en ciberseguridad, puesto que la mayoría de investigaciones se enfocan en las amenazas de ciberseguridad.

Krumay, Bernroider y Walser, (2018), realizaron la investigación Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework, en Austria. Como parte de las metodologías de gestión de riesgos, es necesario contar con controles de seguridad de la información y métricas definidas. La mayoría de empresas acude a aplicar NIST, sin embargo, se necesita saber si NIST tiene un alineamiento efectivo con las normas internacionales respecto a gestión de riesgos de seguridad de la información. El método aplicado analiza la norma NIST, específicamente la aplicación relacionada a los controles de ciberseguridad con las métricas que esta establece para las organizaciones que lo aplican. Y determina si la NIST manifiesta un alto grado de alineamiento con lo que las teorías necesitan para los controles y métricas de ciberseguridad. El método aplicado consistió en los siguientes pasos: 1. Revisión de literatura con apoyo de seis expertos, utilizando palabras claves relacionadas con el motor Google Scholar, 2. Elaboración de una tabla de principio de codificación basado en las categorías de NIST, con el objetivo de que todos los investigadores, hablen un mismo lenguaje, 3. Elaboración de un mapeo de controles NIST con interpretación directa o indirectamente a través de las 5 funciones de ciberseguridad (identificar, proteger, detectar, responder y recuperar), 4. Finalmente se estableció una tabla con áreas temáticas descubiertas especificando sus números de controles y métricas establecidas. Se encontraron 56 artículos científicos, de los cuales se extrajeron 1378 controles y métricas de seguridad de ciberseguridad. Se establecieron 7 principios de codificación simple basado en las 26 categorías de NIST, la confianza calculada por dos de los investigadores, obtuvieron como valor 96% y 97%. Se estableció una tabla con las 26 categorías de NIST, y en cada una de ellas, el porcentaje de alineamiento de manera directa e indirecta con el fundamento teórico. Respecto a los 1378 controles, se puede decir que tienen asignaciones indirectas con mayor frecuencia, mientras que el 66% de todas las métricas se asignaron dentro de una sola función de la guía NIST, el 40% incluso se asignaron directamente a una categoría sin ningún mapeo indirecto adicional a otras categorías. Las organizaciones de los sectores de energía, transporte, banca, salud, agua y las infraestructuras del mercado digital y financiero deben

considerar el marco de ciberseguridad para asegurar un nivel razonable de ciberseguridad. Esto incluye explícitamente la evaluación de controles y la aplicación de métricas para informar su estado de seguridad y madurez. Además, muestra la cobertura del marco NIST mediante la investigación en términos de métricas y controles, y sugieren áreas que merecen más atención en investigaciones futuras. Además, también sugieren una serie de áreas temáticas que parecen faltar o estar subrepresentadas en el marco del NIST.

Ganin et al., (2017), realizaron la investigación, Multicriteria Decisión Framework for Cyber Security Risk Assessment and Management, en Estados Unidos. Los investigadores necesitaban investigar un mecanismo que ayude tanto a la gestión como a la evaluación de riesgos de ciberseguridad, debido al a que los sistemas cibernéticos cambian con los avances técnicos así mismo cambia la distribución en sus dominios: físico, de información y sociocognitivo, y las estructuras de red que contienen muchos nodos. Por esta razón, realizaron un análisis de decisiones que cuantifica la amenaza, la vulnerabilidad y las consecuencias a través de un conjunto de criterios diseñados para evaluar la utilidad general de las alternativas de gestión de la ciberseguridad. El mecanismo propone considerar un modelo TVC (amenaza, vulnerabilidad y consecuencia). En 1. Amenazas, se analizó 1.1 Facilidad de ataques, 1.2 Beneficios de un ataque exitoso, en 2. Vulnerabilidades, se analizó 2.1 Dominios físico, 2.2 Dominio de información, 2.3 Dominio social, 3. Consecuencias en el aspecto de confidencialidad, integridad y disponibilidad. Los resultados obtenidos mostraron que mediante el mecanismo elaborado y simulación de datos lo más realista posible, los porcentajes de contribución con los riesgos fueron: para 1.1 Facilidades de ataques se obtuvo 11.73%, para 1.2 Beneficios de un ataque exitoso se obtuvo 12.57%, para 2.1 Dominio físico se obtuvo 5.03%, para 2.2 Dominio de información se obtuvo 23.56%, para 2.3 Dominio social se obtuvo 6.28%, para 3 Consecuencia de confidencialidad se obtuvo 25.13%, para consecuencia integridad se obtuvo 7.85% y para consecuencia de disponibilidad 7.85%. Si bien la técnica desarrollada en este estudio es un paso hacia una estimación de riesgos más basada en sistemas en un sistema cibernético, hay mejoras que deben abordarse en el trabajo futuro. Un modelo

ideal calcularía el riesgo como pérdida esperada y el valor como pérdida esperada evitada, pero estos cálculos precisos simplemente no son posibles cuando se desconocen las amenazas. Por lo tanto, MCDA proporciona un medio alternativo para el análisis de riesgos. En particular, el objetivo de este trabajo no era desarrollar un conjunto rígido de métricas y criterios para la ciberseguridad, sino proporcionar un marco general que se pueda adaptar a los sistemas individuales.

Papastergiou y Polemi, (2017), realizaron la investigación, MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology. El rubro de cadena de suministros es un rubro delicado debido a la alta dependencia de información entre empresas, y un ciberataque puede ocasionar una catástrofe de efecto dominó, para ello se necesita una metodología que permita evaluar los riesgos dentro de este tipo de negocio. Por esta razón, los investigadores propusieron una metodología de evaluación de riesgos de la cadena de suministro impulsada por la evidencia que se basa en pruebas y hallazgos científicos y experimentales de alta calidad (incluidos resultados e indicadores de simulación) para optimizar la evaluación y mitigación de la cadena de suministro relacionada a riesgos y amenazas cibernéticas. La metodología está compuesta por seis bloques: 1. Establecimiento de límites (1.1 Metas y objetivos de la cadena de suministros, 1.2 Identificación de partes interesadas, 1.3 Modelado), 2. Análisis de amenazas (2.1 Identificación de ciber amenazas, 2.2 Evaluación de amenazas), 3. Análisis de vulnerabilidades (3.1 Identificación de vulnerabilidades confirmadas, 3.2 Identificación de vulnerabilidades potenciales, 3.3 Evaluación de vulnerabilidades individuales, 3.4 Evaluación de vulnerabilidades acumulativas, 3.5 Evaluación de vulnerabilidades propagadas), 4. Análisis de impacto (4.1 Evaluación de impactos de activos individuales, 4.2 Evaluación de impactos acumulativos, 4.3 Evaluación de impactos propagados), 5. Estimación de riesgos (5.1 Evaluación de riesgos de activos individuales, 5.2 Evaluación de riesgos acumulativos, 5.3 Evaluación de riesgo propagado) y 6. Estrategia de mitigación. Los resultados mostraron la composición de la metodología, el cual consta de 17 actividades, alineadas a los estándares ISO 28000, ISO 28001 e ISO 27005. La metodología propuesta manifiesta: visión

holística, colaborativa, centrado en el negocio, cumple con estándares, es implementable, independiente al sector de negocio, auditable y consciente de la privacidad. La metodología MITIGATE se implementará en una herramienta colaborativa durante el proyecto MITIGATE, lo que permitirá a todos los socios comerciales dentro de una cadena de suministros realizar su evaluación de riesgos. Se localiza en el sector marítimo para que los interesados puedan probar su funcionalidad y rendimiento.

Mukhopadhyay, Chatterjee, Bagchi, Kirs, y Shukla, (2017), realizaron la investigación, Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. Dentro de la gestión de riesgos de seguridad de la información, existen modelos aplicables para la mitigación de la misma, por lo que, es necesario contar con resultados de aplicación de esos modelos para determinar cuál es el más eficiente para nuestra organización y construir un marco de evaluación y mitigación de ciber riesgos con el fin de optimizar costos, evitar pérdidas de capitalización de mercado y evitar una pérdida de valor de marca en las organizaciones. Por esta razón, se revisó (1) Literatura relacionada con métodos tradicionales, métodos cualitativos y modelos conductuales, métodos cuantitativos, modelos híbridos y modelos de aseguramiento de ciber riesgos. (2) Ciberataques maliciosos, como ataques de virus, ataques DoS, fraudes financieros, sistemas de penetración, robo de información de titulares. El modelo se validó con datos de CSI-FBI de los años 1997 a 2010, utilizando el 80% de los datos para entrenamiento y 20% para pruebas. El marco se divide en dos fases. En la fase 1 denominada evaluación de ciber riesgos, manifiesta como actividades involucradas a 1.1 Estimación de la probabilidad de ciberataques en el tiempo, 1.2 Estimación de inversión en tecnologías de seguridad vs probabilidades futuras de tendencias en ciberataques, 1.3 Estimación de distribución de pérdidas vs ciberataques, 1.4 Cuantificación de severidad esperada de un ciberataque usando el modelo de riesgo colectivo. La fase 2 denominada aseguramiento a través de la mitigación de ciber riesgos, manifiesta como actividades a 2.1 Computación premium para productos de seguros cibernéticos, 2.2 Estrategias de mitigación de ciber riesgos por cada uno de los ataques. Los resultados mostraron que la

representación de los principales sectores es financiera (20%), consultoría (11%), educación (11%), tecnología de la información (10%) y manufactura (8%). Más del 40% de los encuestados eran personas responsables de la seguridad empresarial. En esta investigación, presentaron el marco CRAM para cuantificar la probabilidad de que un ataque malicioso comprometa los sistemas de TI de una organización y afecte negativamente a sus ingresos y ganancias utilizando modelos GLM (es decir, Logit y Probit). También utilizaron el concepto de modelado de riesgo colectivo para calcular la pérdida derivada de ataques maliciosos. El estudio propone además algunas estrategias para mitigar el ciber riesgo mediante el uso de instrumentos financieros.

Nagaraju, Fiondella y Wandji, (2017), realizaron la investigación, A Survey of Fault and Attack Tree Modeling and Analysis for Cyber Risk Management, en Estados Unidos. Los diversos modelos existentes para análisis de ciber riesgos, pueden aplicarse según las necesidades de la organización, sin embargo, dos de ellos, el modelado de árbol de ataque y el árbol de fallas, suelen confundirse por su similitud. Por esta razón, esta investigación proporciona una revisión de los dos enfoques de modelado más populares, incluidos los árboles de fallas y ataques, y analiza sus beneficios y posibles limitaciones. Los enfoques de modelado de confiabilidad y riesgo discutidos en la literatura incluyen árboles de fallas (FT), árboles de eventos (ET), diagramas de decisión binaria (BDD), redes de Petri (PN), modelado de Markov (MM) y árboles de ataque (AT) para caracterizar sistemáticamente los riesgos latentes en los sistemas ciber físicos. La encuesta elaborada para el estudio, debería ser beneficiosa para los profesionales de la seguridad que deseen aplicar técnicas de modelado de confiabilidad y riesgo para garantizar la seguridad cibernética de sus sistemas, así como para los investigadores que buscan identificar nuevas oportunidades de modelado. Los resultados mostraron que se detallaron las fases de ambos enfoques. El árbol de fallas, presenta eventos importantes, eventos básicos, eventos conectores, eventos de condiciones y eventos de transferencia. Mientras que el árbol de ataques considera nodo raíz, nodos hoja y nodos intermedios. El trabajo proporcionó una encuesta sobre el modelado y análisis de árboles de fallas y ataques para la gestión del riesgo cibernético. Se

revisaron los elementos básicos de estos enfoques de modelado. Se proporcionó una variedad de modelos y aplicaciones, así como una discusión de las limitaciones de los enfoques. Las investigaciones futuras revisarán paradigmas adicionales de modelado de riesgo cibernético, como árboles de eventos, diagramas de decisión binarios, redes de Petri y modelos de Markov para identificar las limitaciones de su expresividad y capacidad para cuantificar y mitigar el riesgo. Luego, desarrollaremos generalizaciones teóricas a estas técnicas de modelado matemático con el fin de superar estas limitaciones y aplicarlas a los sistemas para demostrar estas mejoras.

1.3. Teorías relacionadas al tema.

Metodologías de gestión de riesgos.

RISK IT

El RISK IT es un framework que está basado en principios orientados a la gestión de riesgo de TI. El framework complementa COBIT, un framework integral para el gobierno y control de soluciones y servicios basados en TI impulsados por negocios. Mientras que COBIT proporciona un conjunto de controles para mitigar el riesgo de TI, RISK IT proporciona un marco para que las empresas identifiquen, gobiernen y administren el riesgo de TI. En pocas palabras, COBIT proporciona los medios de gestión de riesgos; RISK IT proporciona los fines. Empresas que se han adecuado a COBIT como marco de gobierno de TI pueden usar RISK IT para potenciar su gestión. (ISACA, 2009)

El framework RISK IT, trata sobre el riesgo de TI, es decir, el riesgo empresarial relacionado con “el uso de tecnología de la información, la gobernanza empresarial eficaz y la gestión de riesgos de TI” (ISACA, 2009); es decir:

a. Siempre se conecta con los objetivos comerciales.
b. Alinea la gestión del riesgo empresarial relacionado con TI con la gestión de riesgo empresarial general (ERM), siempre y cuando se aplique, es decir, si el ERM se implementa en la empresa.
c. Equilibra los costos y beneficios cuando se administra el riesgo de TI.
d. Promueve una correcta comunicación de los riesgos de TI.

e. Establece el orden correcto desde arriba al tiempo que define y aplica.
f. Responsabilidad de operar con tolerancia.
g. Es parte de las actividades diarias.

Para priorizar y gestionar el riesgo de TI, los altos ejecutivos necesitan un marco de referencia y una comprensión clara de la función de TI y el riesgo de TI. Sin embargo, las partes interesadas claves de la empresa, incluidos los miembros de la alta dirección ejecutiva y las mismas personas que deberían ser responsables de la gestión de riesgos dentro de la empresa, a menudo no tienen una comprensión completa (ISACA, 2009)

El riesgo de TI no es solo un problema técnico. Si bien los expertos en la materia de TI ayudan a comprender y gestionar los aspectos del riesgo de TI, la gestión empresarial es el actor más importante. Los gerentes comerciales monitorean lo que los recursos tecnológicos demandan para una alta capacidad de soporte a los objetivos del negocio y gestionan los parámetros en los cuales ellos se limitarán para una óptima generación de valor (ISACA, 2009)

El marco RISK IT, permite a la empresa tomar decisiones adecuadas y conscientes del riesgo, además permitirá a los usuarios lo siguiente (ISACA, 2009):

a. Integrar la gestión de riesgos de TI en la gestión general de riesgos empresariales (ERM) de la organización.
b. Tomar decisiones sobre el alcance del riesgo, el apetito de riesgo y la tolerancia al riesgo por parte de la empresa.
c. Comprender cómo se responderá al riesgo.

En resumen, las empresas pueden comprender y gestionar todos los tipos de riesgos de TI importantes con el marco de RISK IT ya que proporciona una visión de extremo a extremo de los riesgos relacionados con el uso de TI, así como una visión similar de la gestión de riesgos. (ISACA, 2009).

Pero el año 2020 ISACA nos presenta RISK IT Framework, 2nd Edition cubriendo ciertos puntos relacionados con el internet de las cosas (IOT), riesgos en la ciberseguridad y los riesgos de la información de los datos electrónicos relacionado con medios digitales. En este contexto RISK IT Framework 2nd Edition y su volumen complementario RISK IT Practitioner Guide 2nd Edition, ayudan a los profesionales de TI a identificar y calificar al riesgo no solo involucrando al área de TI sino también a nivel empresarial cumpliendo con:

a. Integrar la gestión del riesgo de TI tradicional, la seguridad de la información y el riesgo cibernético en los procesos generales de ERM. (ISACA, 2020).
b. Facilitar la toma de decisiones integral, holística y consciente de los riesgos a nivel empresarial. (ISACA, 2020).
c. Guiar la respuesta al riesgo empresarial siempre que el riesgo relacionado con TI supere la tolerancia (ISACA, 2020).

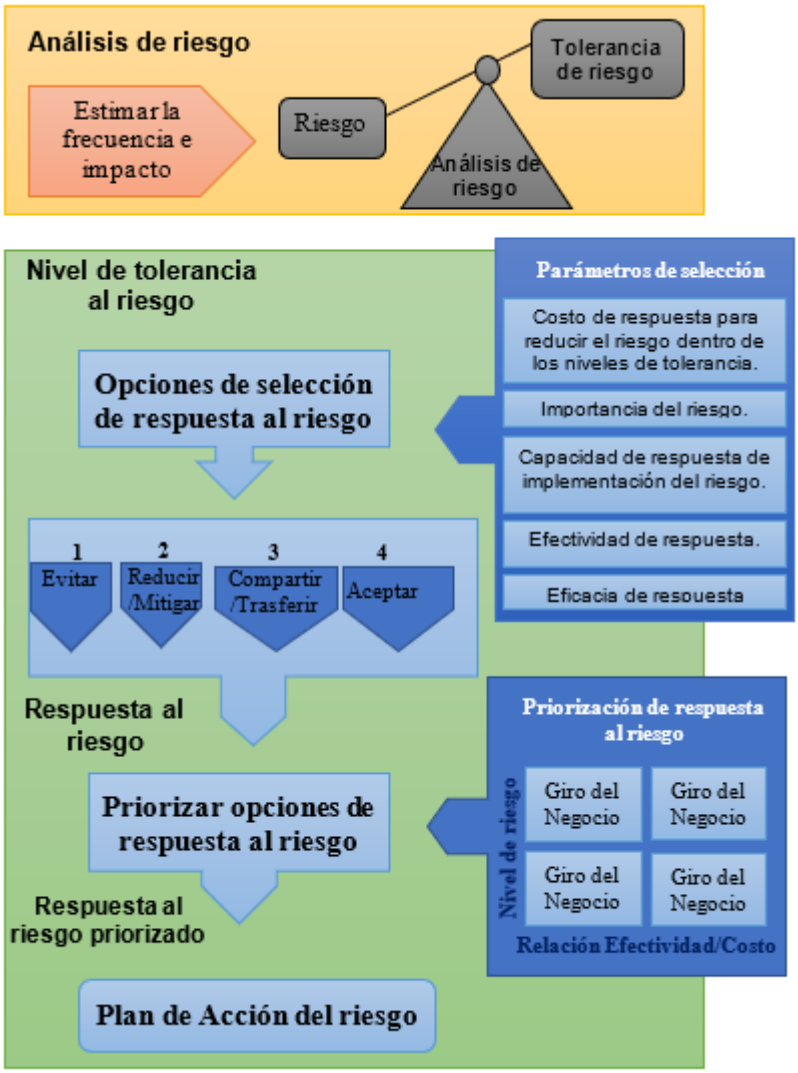


Figura 2. Análisis de riesgo del Framework RISK IT. Fuente*:* (ISACA, 2020)

TARA

Threat Assessment and Remediation Analysis (TARA) es una metodología de ingeniería utilizada mayormente para activos cibernéticos, es decir cualquier activo de TI que se relaciona con la persona, software, internet o intranet en el ciberespacio. Esta metodología es utilizada en inteligencia militar para ciberseguridad y ciberdefensa en algunos países de Norteamérica.

TARA es parte de la cartera de prácticas de Seguridad de Sistemas (SSE) de MITRE desde su desarrollo 2010 se ha utilizado en más de 30 evaluaciones de riesgo cibernético, para el 2017 el catálogo de TARA se renovó y colaboró con el Organismo Internacional de Energía Atómica (OIEA) sobre análisis y

planificación de incidentes cibernéticos para instalaciones nucleares. (Wynn, 2014).

Los objetivos de TARA son:

a. Identificar y priorizar Tácticas, Técnicas y Procedimientos (TTP) de alto riesgo a los que un activo cibernético está expuesto. (Wynn, y otros, 2011).
b. Identificar y priorizar contramedidas (CM) contra esos TTP. (Wynn, y otros, 2011).
c. Finalmente, recomendar CM para reducir la probabilidad de un ataque de un activo cibernético. (Wynn, y otros, 2011).

La metodología TARA define un alcance y un análisis. Para el Alcance se considera el objetivo de la evaluación al igual que la gama de amenazas a evaluar, también considera capacidades e intenciones del actor de amenazas y el resumen del alcance de evaluación. Para el análisis se considera dos pasos:

a. Evaluación de susceptibilidad a amenazas cibernéticas **(CTSA),** Donde se identifica y evalúa la susceptibilidad de un activo cibernético a un ataque en relación con un conjunto de TTP. De este paso resulta una Matriz de susceptibilidad que básicamente es: Modelar la superficie de ataque, realizar una búsqueda en el catálogo para identificar los Vectores de Ataque (AV) candidatos, eliminar los AV inverosímiles y definir un modelo de puntuación para clasificar los AV plausibles.

b. Análisis de corrección de riesgos cibernéticos **(CRRA),** etapa donde identifica un conjunto de contramedidas que reducen la susceptibilidad o atenúan los efectos de un ataque cibernético. De este paso resulta una Recomendación de mitigación en base a: Seleccionar AV para mitigar, utilizar mapeos de mitigación para identificar posibles contramedidas, eliminar CM inverosímiles, definir un modelo de puntuación para clasificar

a las CM, seleccionar el mejor conjunto de soluciones de CM y desarrollar recomendaciones bien formadas.

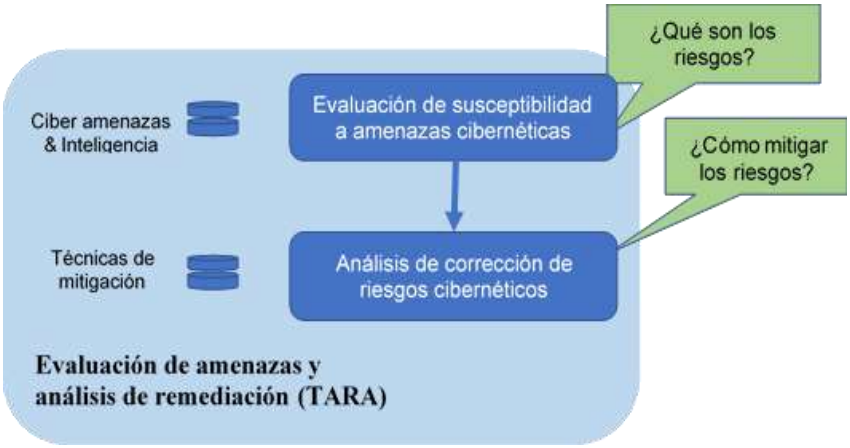


Figura 3. Esquema de metodología TARA. Fuente*:* (Wynn, y otros, 2011).

Uno de los objetivos de estas recomendaciones es establecer la trazabilidad de una CM a las TTP que mitiga, y al activo cibernético y la capacidad (o capacidades) de la misión que se han vuelto más resilientes mediante la aplicación de CM. Esta trazabilidad permite a los administradores de programas tomar decisiones informadas al seleccionar qué CM implementar en un programa determinado.

Contramedida (CM)			**Efectividad de mitigación (por ID de vector de ataque)**		
CM ID	**Nombre**	**Índice Costos**	**TTP#1**	**TTP#2**	**TTP#3**
			RS	**RS**	**RS**
TOTAL		SUMA	CANT1	CANT2	CANT3

Figura 4. Formato para Matriz de susceptibilidad en TARA. Fuente: Elaboración propia.

MAGERIT.

Una metodología formal de Análisis de Amenazas y Riesgos (AAR) es una metodología sistemática que permite a las organizaciones conocer el riesgo al que están exhibidos sus sistemas de información y, como resultado, gestionarlos, reduciendo dichos riesgos a niveles aceptables. Mediante un AAR completo se identifican las amenazas aplicables y, en consecuencia, se pueden diseñar e implementar las contramedidas adecuadas (Hernandez Ardieta, Blanco, & Vara, 2012).

MAGERIT es una AAR reconocida por el Gobierno de España como AAR estándar para la Administración Pública Española, y también ha sido seleccionada por la OTAN (Organización del Tratado del Atlántico Norte) e incluida en el catálogo de AARs formales de ENISA (Agencia Europea de Seguridad de la Información y Redes) y EAD (Agencia Europea de Defensa) (ENISA, 2007)

MAGERIT se basa en la descripción detallada de los activos de la organización, las amenazas sobre ellos y las salvaguardas existentes que protegen esos activos de las amenazas identificadas. A partir de esa información, MAGERIT deriva el nivel de riesgo (función de la probabilidad o frecuencia de la amenaza y el impacto causado) para cada dimensión de seguridad (disponibilidad, integridad y confidencialidad de los datos) de cada activo. De esta forma, MAGERIT permite observar cómo se reduce el riesgo actual con el incremento del número de salvaguardas y su nivel de madurez, alcanzando un nivel de riesgo denominado objetivo o residual. (ENISA, 2007)

Un análisis de amenazas y riesgos basado en MAGERIT sigue tres etapas: evaluación de riesgo potencial, evaluación de riesgo real y evaluación de riesgo residual u objetivo. Durante la etapa de evaluación de riesgos potenciales, se realizan los siguientes pasos (ENISA, 2007):

1. Caracterización de los activos (ver figura 4), incluyendo sus interrelaciones y su valor (qué costo-daño causaría su degradación). La valoración de activos puede seguir enfoques cualitativos o cuantitativos (ENISA, 2007).

2. Caracterización de las amenazas, identificando las aplicables a los activos seleccionados y considerando su frecuencia (número de ocurrencias de la amenaza durante un período específico, por ejemplo, anualmente) y la degradación causada en el activo en caso de que aparezca la amenaza (ENISA, 2007).

3. Estimación del impacto potencial, definido como el daño al activo derivado de la ocurrencia de la amenaza. Incluye el valor acumulado y el valor desviado (ENISA, 2007).

4. Estimación del riesgo potencial, definido como la tasa de exposición de una amenaza a aparecer, causando un impacto y considerando la ausencia de salvaguardas. Incluye el valor acumulado y el valor desviado (ENISA, 2007).

La etapa de evaluación de riesgos real implica la selección de las salvaguardas (y su nivel de madurez) ya incorporadas en el sistema de TI bajo análisis. Una salvaguarda puede reducir el riesgo del nivel potencial al nivel actual al reducir la frecuencia de amenazas, limitar el impacto causado en caso ocurra la amenaza, o ambos (ENISA, 2007)

Finalmente, durante la etapa de evaluación del riesgo residual, el analista puede incorporar nuevas salvaguardas o mejorar el nivel de madurez de las actuales, hasta que el nivel real de riesgo se reduzca a un nivel residual y aceptable (ENISA, 2007)

La Figura 4 muestra la relación entre las salvaguardas y los diferentes tipos de niveles de riesgo.

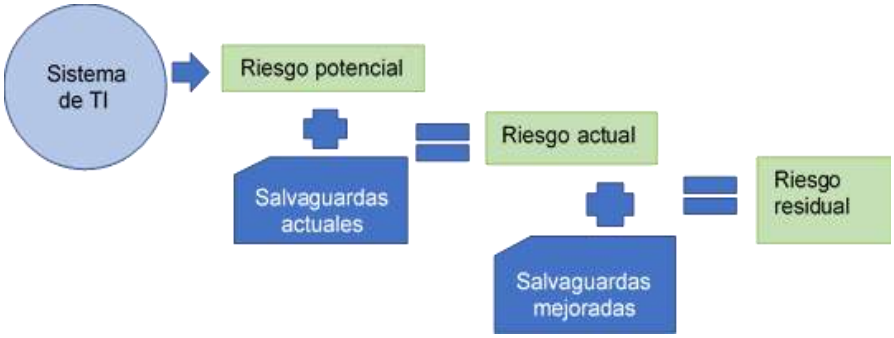


Figura 5. Relación entre salvaguardas y tipos de niveles de riesgo. Fuente: *MAGERIT* (ENISA, 2007)

Tipo de activo	Nombre de Activo	Dimensión			Valoración del activo (I+D+C)
		[I] Integridad	[D] Disponibilidad	[C] Confidencialidad	

Figura 6. Formato para caracterizar un activo. Fuente: *MAGERIT* (ENISA, 2007).

Es importante mencionar que la gestión de riesgos propuesta por esta metodología abarca tres procesos que se visualizan en la figura 7 y cada proceso establece ciertas tareas que se visualizan en la figura 8, por ejemplo, para el "Proyecto de Análisis de Riesgos (PAR)" se solicita realizar tres actividades que MAGERIT los denomina PAR.1, PAR.2 y PAR.3.

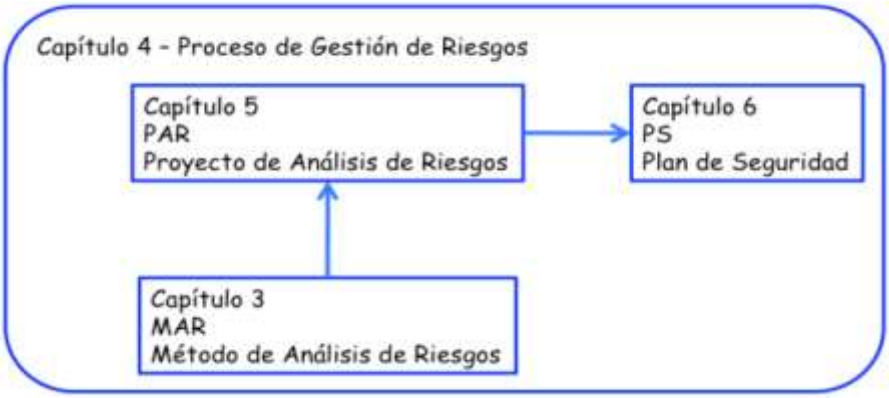


Figura 7. Actividades formalizadas. Fuente: *MAGERIT* (ENISA, 2007).

Gestión de riesgos.

En este punto es necesario tener claridad con la definición de la palabra riesgo. La definición en el diccionario de la Real Academia nos indica que etimológicamente proviene de la palabra “Riesgo” que significa risco (Real Academia Española, 2014) denotando así el peligro que supone. Pero en el contexto informático y tecnológico la palabra riesgo se definió por primera vez a través de un estándar internacional ISO 3100 indicando que es “Efecto de la incertidumbre sobre los objetivos”. (International Organization for Standardization, 2009)

Desde esa fecha hasta la actualidad todo estándar internacional certificado o no lo tomó como referencia para la optimización de la gestión orientada a los riesgos: cómo analizarlo, cómo estimarlos, cómo tratarlo y cómo comunicarlo. A manera de ejemplo, el estándar NIST SP 800-30 (2002), manifiesta que: “La gestión de riesgos es un proceso de identificación, estimación y toma de decisiones para reducir el riesgo a un nivel que se pueda admitir” (NIST SP 800-30, 2002).

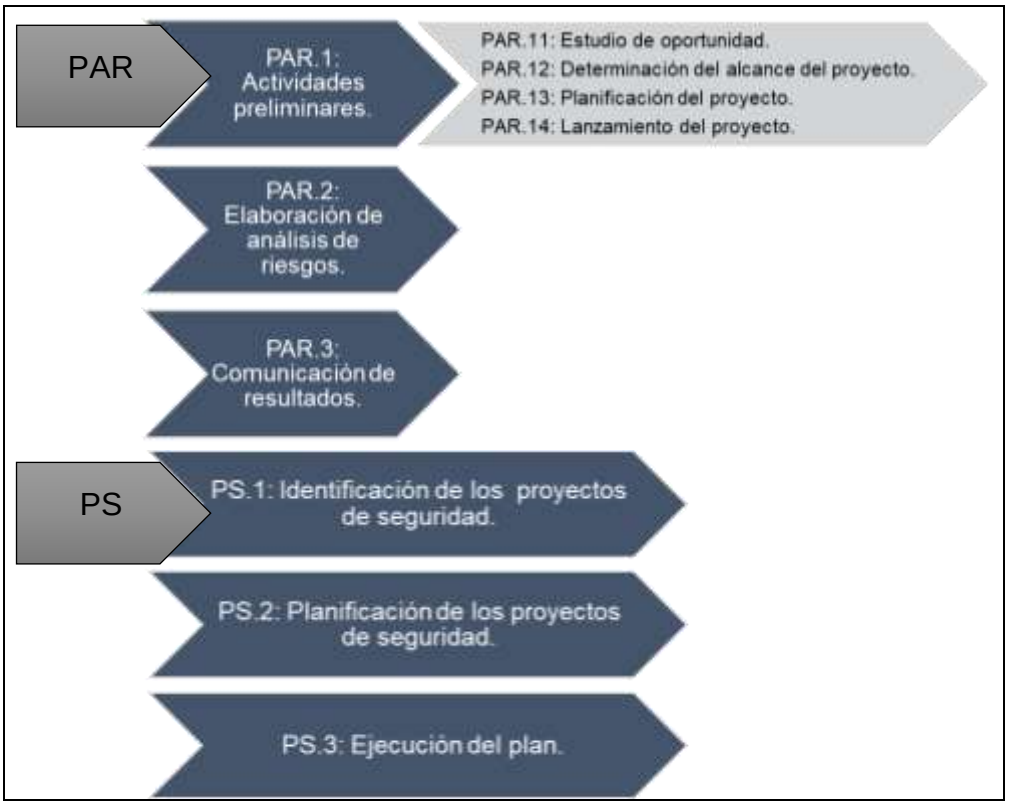


Figura 8. Tareas por actividades de la metodología MAGERIT. Fuente: *MAGERIT* (ENISA, 2007).

La gestión de riesgos, de acuerdo a las definiciones anteriores, es el proceso por el cual aprovechamos las oportunidades que nos brinda esta incertidumbre (desconocimiento total o parcial) y minimizamos las vulnerabilidades y pérdidas ocasionadas por el efecto (sea positivo o negativo) de este impacto en los objetivos trazados (forma en cómo opera la organización siguiendo metodologías o políticas internas). La práctica de este proceso es continuo y cíclico ya que la probabilidad de que algo suceda es incierta (puede ocurrir o no) y proviene de diferentes fuentes (personas, entorno, actividades, elementos) y por eso es conveniente la identificación de estas fuentes, reconocerlas para saber sus causas, sus efectos y consecuencias, este análisis y la priorización de riesgos y la búsqueda, evaluación y aplicación de contramedidas relevantes para un tratamiento así como el seguimiento de los resultados. Este proceso potencia la gobernanza y optimiza las políticas empresariales además de brindar seguridad, confianza y competitividad, generando una cultura de prevención.

En resumen, para hablar de gestión de riesgo referente al tema seleccionado debemos clarificar ciertos conceptos que a continuación se mencionan, dichas definiciones en su mayoría fueron extraídos del libro 1 de Magerit v3:

a. Activos: información relacionada con el negocio necesaria para que funcione correctamente
b. Amenaza: cualquier daño que afecte a los activos ocasionando una posible pérdida o paralización de la función principal de la empresa.
c. Vulnerabilidad: Debilidad en el diseño que posibilita que se ejecute o no una amenaza.
d. Probabilidad: Posibilidad de que un hecho se produzca.
e. Frecuencia: Tasa de ocurrencia de una amenaza.
f. Tratamiento: Proceso destinado a modificar el riesgo.

Gestión de riesgos de seguridad de la información.

La información es un recurso muy valioso en toda organización desde ahí el afán de protegerla por ello se eligen recursos (humano y técnico) para fomentar su seguridad. La seguridad de la información (sea física o digital) suelen ser medidos de acuerdo a un nivel (alto, medio, bajo), para luego evaluar el impacto en la organización. Por ello es importante que todas las empresas gestionen estos niveles de seguridad en sus sistemas de información enfocándose en la prevención de los riesgos de manera global o implementado por separado.

El estándar ISO 31000 en su revisión del año 2018 reafirma el ciclo de vida de un proceso de Gestión de Riesgo (International Organization for Standardization, 2018), al observar la figura 9 el concepto de seguridad va más allá de la implantación de medidas de seguridad técnicas. Todos los demás estándares certificados tomaron como guía este proceso.

La descripción al detalle de la figura 9, se definió en la sección denominada Procesos de gestión de riesgos en este documento donde se podrá rescatar el aporte de esta norma para la evaluación de riesgos

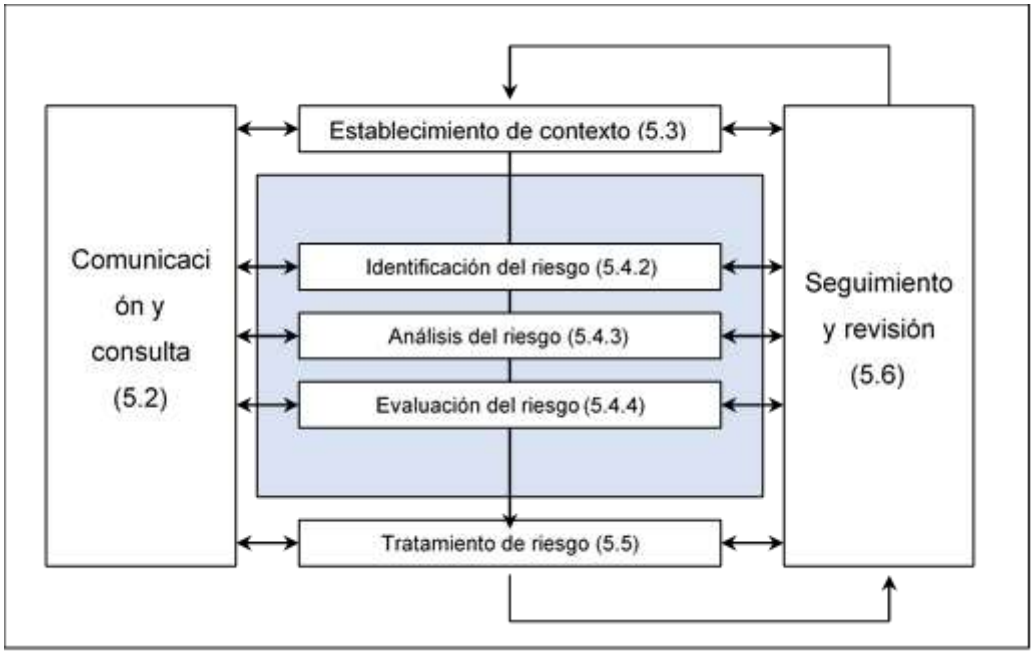


Figura 9. Proceso de gestión de riesgos según ISO 31000. Fuente: *ISO 31000:2018*

Proceso de gestión de riesgos.

Las evaluaciones de riesgo generalmente sirven para identificar y analizar posibles vulnerabilidades y amenazas a un sistema dado, así como el valor relativo de los activos y los posibles daños resultantes de su compromiso. Esto se hace con el fin de estimar los riesgos que puede enfrentar el propietario, operador o usuario del sistema. Como tal, su resultado es la base para todas las demás actividades de gestión de riesgos al generar nuevos requisitos de seguridad, ayudar en la elección y especificación de contramedidas, evaluar las políticas de seguridad actuales, respaldar las decisiones de gestión relevantes, evaluar los mecanismos de protección existentes, los controles, etc.

El resultado de una evaluación de riesgos suele ser una evaluación cualitativa o cuantitativa de los posibles riesgos a los que se expone una organización, teniendo en cuenta su contexto y las posibles amenazas. Cabe señalar que la mayoría de las evaluaciones de riesgos, así como la mayoría de los procesos de gestión de riesgos, no tienen como objetivo obtener un sistema completamente seguro, ya que esto a menudo es imposible. En

cambio, el objetivo final es alcanzar lo que se percibe como una seguridad aceptable a un costo aceptable (también llamado seguridad "suficientemente buena"). Los marcos difieren en su interpretación de esto y en la forma de lograrlo y mantenerlo.

En el sentido más general, una gestión de riesgos es una tarea multidisciplinaria que puede contener uno o más de los siguientes pasos (la figura 9 mapea los pasos a las fases de la gestión de riesgos):

a. **Establecimiento de contexto:** Identificar y definir el contexto digital, técnico social y empresarial en el que opera el sistema, así como construir algún tipo de modelo del propio sistema de información. Aunque el contexto del SI siempre es relevante, este paso a veces se omite si ya existe una especificación satisfactoria del SI. Esto suele ser parte de la etapa de "preparación" de la figura 9. Otras actividades relevantes para esta fase son la definición del alcance de la evaluación, los requisitos de seguridad, los objetivos de las partes interesadas, los criterios de riesgo, etc.

b. **Identificación de riesgos:** este es el núcleo de cualquier evaluación de riesgos y tiene que ver con el uso de los datos disponibles para identificar posibles vectores de ataque y vulnerabilidades del sistema. Este paso corresponde a la etapa de "identificación" en la figura 9.
c. **Análisis de Riesgos:** este paso tiene que ver con la comprensión de las probabilidades, impactos y otros parámetros asociados con los riesgos identificados para permitir una mejor comprensión de las vulnerabilidades del sistema. Este paso corresponde a la etapa de "análisis" de la figura 9.

d. **Evaluación de riesgos:** en este paso final, los riesgos se clasifican y priorizan para permitir que los tomadores de decisiones seleccionen contramedidas. Este paso corresponde a la etapa de "evaluación" de la figura 9.

e. **Seleccionar contramedidas:** aunque a menudo se considera que este paso está fuera del alcance de una evaluación de riesgos, es común que los resultados obtenidos de los pasos anteriores se utilicen para algunos, para seleccionar o priorizar contramedidas, estrategias de mitigación, controles de seguridad o políticas de seguridad. Esto corresponde a la etapa de “tratamiento” en la figura 9.

Estándares internacionales de seguridad de la información.

ISO 27001.

Es el cuidado otorgado a la información organizacional con el fin de evitar el uso desautorizado de la misma. El actual crecimiento de las tecnologías de la información conduce a que se considere generar conciencia sobre adquirir nuevos conocimientos en seguridad de la información y de los mecanismos existentes para la gestión correspondiente. Por ese motivo consideró los siguientes puntos relevantes para hacer análisis teórico relacionado al tema de mi investigación. (International Organization for Standardization, 2013)

a. Principios de seguridad de la información.

La información, es un tipo de activo compuesto por datos estructurados que representan una realidad en la organización cuyo objetivo es apoyar en la toma de decisiones. La información es el recurso principal de la empresa y de sus sistemas de información, es por ello que se considera muy importante tomar conciencia en la protección de los mismos. La información se almacena en medios físicos o electrónicos (International Organization for Standardization, 2013).

Dentro de la seguridad de la información se presentan ciertos principios para lo cual toda salvaguarda debe respetar, estos principios dictan que toda actividad en seguridad de la información debe tener el enfoque de preservar tres conceptos básicos sobre la información, los cuales son: confidencialidad, integridad y disponibilidad. La confidencialidad evita que las personas no

autorizadas vean los datos protegidos. La integridad evita que los datos protegidos sean modificados por cambios no deseados o no autorizados. La disponibilidad es la capacidad de mantener los datos accesibles por las partes interesadas cuando lo necesiten (International Organization for Standardization, 2013)

b. Sistema de gestión de seguridad de la información.

Es el conjunto de políticas, procesos y procedimientos que permiten gestionar de manera adecuada la seguridad de la información en las organizaciones. Tres son los documentos más importantes en una auditoría interna para un SGSI (International Organization for Standardization, 2013), estos son:

a. La política de seguridad de la información, el cual establece las directivas generales basado en la estructura organizacional de la empresa, procesos, infraestructuras, aplicaciones, entre otros.
b. El alcance del SGSI, el cual determina la limitación que tendrá el sistema, basado en los procesos y servicios organizacionales.
c. La declaración de aplicabilidad, el cual indica todos los controles de la norma ISO 27002 que han sido aplicados en la empresa.

Un SGSI está alineado al ciclo de Deming o ciclo PDCA (por sus términos en inglés Plan, Do, Check y Act), el cual permitirá la mejora continua de este sistema. Parte de un SGSI es contar con un método de gestión de riesgos que conlleva a obtener un plan de tratamiento de riesgos, y sus medidas correctivas aplicadas, que serán evidencia ante la auditoría de certificación. No es obligación aplicar la norma ISO 27005 a pesar de pertenecer a la familia ISO 27000, sin embargo, el método seleccionado debe basarse en los principios que dicta la norma. El SGSI deberá presentar actividades de auditoría que

garanticen una evaluación interna e independiente con el resto de áreas especificadas en el alcance, y también deberá presentar actividades de auditoría externa que garanticen una revisión con un punto de vista diferente a la perspectiva interna (International Organization for Standardization, 2013)

Métodos de gestión y evaluaciones de riesgos.

Debido a la gran cantidad de metodologías y marcos disponibles para evaluar el riesgo, un criterio de clasificación sería útil para comprender las diversas opciones disponibles. Las metodologías de evaluación de riesgos o gestión de riesgos se pueden agrupar en función de varios factores.

Según Houmb, (2007), las evaluaciones de riesgo se pueden clasificar en tres tipos principales: basadas en reglas, basadas en riesgos (probabilísticas) y basadas en juicios. Las evaluaciones basadas en reglas generalmente se basan en un conjunto de estándares o listas de verificación que se utilizan como reglas que el sistema debe cumplir. Las evaluaciones basadas en riesgos y basadas en juicios también toman en consideración amenazas desconocidas y se enfocan en evaluar probabilidades e impactos para cada evento no deseado. La diferencia radica en la interpretación de la probabilidad: para las evaluaciones basadas en riesgos, solo se utilizan datos empíricos de contextos similares para estimar la probabilidad, mientras que para las evaluaciones basadas en juicios se utiliza la interpretación subjetiva del experto como probabilidad (Zambon, Etalle, Wieringa, & Hartel, 2011). Introduce un marco para comparar métodos de evaluación de riesgos basado en los siguientes tres parámetros:

a. La escala utilizada para evaluar el riesgo (cualitativo frente a cuantitativo).
b. ¿Qué factores se utilizan para evaluar el impacto?

c. Los factores y operaciones utilizados para calcular el riesgo.

ISO 27005.

Es un estándar internacional que determina el armazón general de la gestión de riesgos de seguridad de la información. Es miembro de la familia ISO 27000, por lo tanto, brinda soporte al estándar internacional ISO 27001 en el proceso de gestión de riesgos, y define los principios que los métodos de valoración y tratamiento de riesgos de seguridad de la información desarrollarán en la organización. Su base se encuentra en el ciclo de Deming, por lo que este estándar determina actividades para planificar, hacer, evaluar y mejorar la gestión de riesgos de seguridad de la información, alimentando la cultura de mejora continua (International Organization for Standardization, 2018).

El estándar define los objetivos que las actividades de gestión de riesgos de seguridad de la información en la organización deben cumplir según el enfoque de autodeterminación, es decir, la misma organización evaluará y desarrollará los métodos necesarios para cumplir con los objetivos que dicta el estándar. Por lo tanto, la organización debe iniciar estableciendo políticas antes que la caracterización de sistemas de información (International Organization for Standardization, 2018).

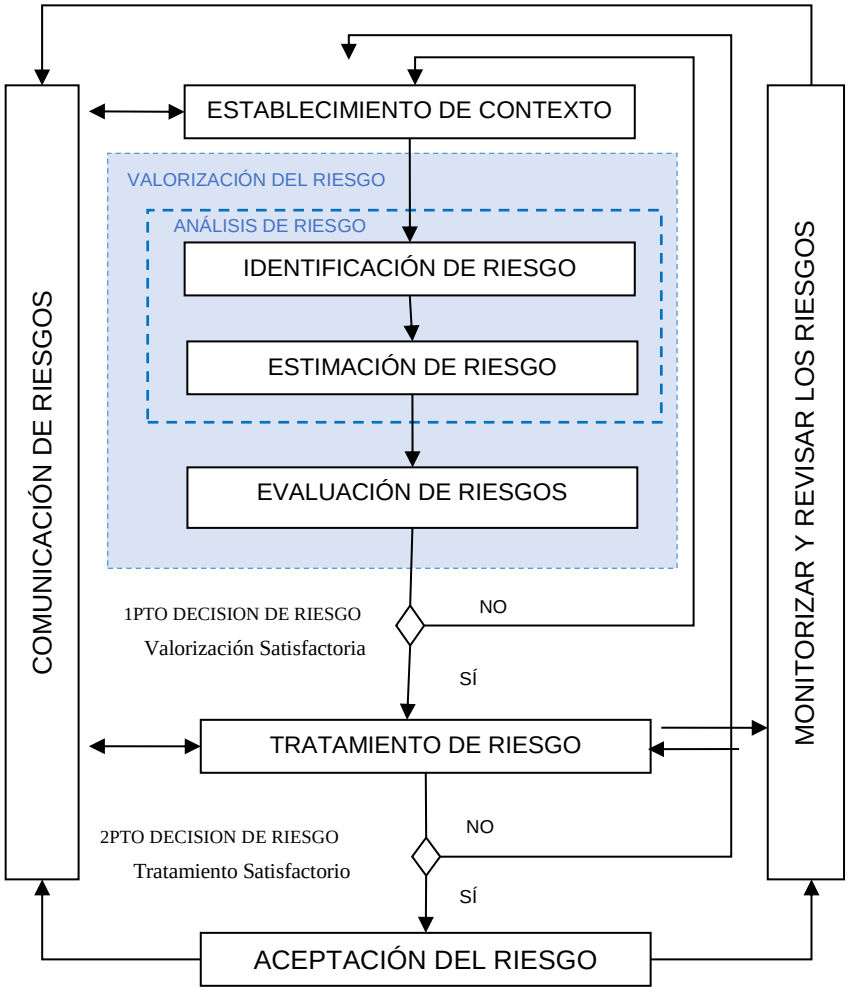


Figura 10. Proceso De Gestión de Riesgo de Seguridad de Información. Fuente: *ISO 27005* (2011).

a. **Establecimiento de contexto;** en esta parte todas las ISO y metodologías determinan el alcance a evaluar de la parte técnica o empresarial. Por ejemplo, se debería solicitar un reporte de información relevante de la organización para poder entregar como producto de esta fase un criterio de evaluación de riesgo, criterios de aceptación de riesgos, roles y responsabilidades en la organización respecto a estos riesgos.

b. **Identificación de riesgo;** este proceso se ubica dentro del contexto definido como análisis de riesgo. Es aquí donde se determina las vulnerabilidades y ataques al activo de información determinado por la

empresa. Por ejemplo, del proceso a (establecimiento de contexto) se tienen criterios de riesgo y responsabilidades en la organización que determinan diferentes listas: lista de activos, lista de amenazas, lista de controles y lista de vulnerabilidades.

c. **Estimación de riesgo;** parte del análisis de riesgo donde se calcula que amenazas podrían afectar el activo de información. Por ejemplo, del proceso anterior se tuvo diferentes listas que servirán para estimar el riesgo entregando como producto la lista de valoración de consecuencias y las probabilidades en escenarios de incidencias.

d. **Evaluación de riesgos;** en este proceso se valora el riesgo para poder pasar al siguiente proceso. Aquí se opta por determinar cómo se evaluará el riesgo dependiendo del análisis de riesgo efectuado en los procesos b y c, obteniendo como producto una lista de riesgos priorizados.

e. **Tratamiento de riesgo;** en este proceso se definen las estrategias de tratamiento, políticas internas o externas e incluso otros estándares a usar para controlar el riesgo. Por ejemplo, con el criterio de evaluación del riesgo en este proceso se determina si el riesgo se modifica, se retiene, se elimina o se comparte logrando como producto un plan de tratamiento de riesgo, un riesgo residual y políticas o acuerdos contractuales.

f. **Aceptación del riesgo;** en este proceso se definen criterios de riesgo en base al tratamiento antes realizado. Por ejemplo, con la ayuda de un plan de tratamiento se busca aceptar o no aceptar el riesgo y justificarlo por ello como producto de esta fase se considera la lista de riesgos aceptados y la lista de riesgo no aceptados.

g. **Comunicación de riesgos;** este proceso se refiere al compromiso de la organización para entablar comunicación con la parte interesada. Por ejemplo, para empezar este proceso se debe tener información del riesgo

obtenido en los procesos anteriores a este además de un plan de comunicación para lograr como producto una mejor distribución de información además de un informe de rendimiento.

h. **Monitorizar y revisar los riesgos;** este proceso se refiere al constante monitoreo de lo implementado. Esta parte de todo el estándar, así como las métricas a usar en el proceso f. Es aquí donde se dice que nada se gestiona sino se mide y nada se mide sino se gestiona. En este último proceso se necesita un portafolio de cambios porque la información del riesgo obtenido varía en las actividades de gestión del riesgo, por ello se monitorean y revisan los factores de riesgo para luego implementarlo. El resultado final es una lista actualizada de identificación de riesgos, Informe del estado del riesgo y algunos planes alternativos.

1.4. Formulación del Problema.

¿Cómo mejorar la gestión de ciber riesgos en una empresa manufacturera peruana?

1.5. Justificación e importancia del estudio.

El presente trabajo busca cerrar las brechas existentes dentro del diseño de una metodología de gestión de riesgos de ciberseguridad que las organizaciones manifiestan al momento de enfrentar un incidente ya sea por motivo de reacción o prevención. Con ello las pequeñas empresas manufactureras podrán guiarse del producto de este trabajo para dar su primer paso en la seguridad de la información, así el personal no cuente con mucha experiencia en el manejo de los conceptos relacionados.

La metodología busca apoyar a la gestión de riesgos empresarial, manifestando un nivel de integración adecuado, que permita colaborar con el cuidado del valor de negocio, ya sea o no con fines lucrativos. Además, pretende establecer un punto de partida para un nivel de madurez más avanzado dentro de la organización, como el gobierno corporativo de las tecnologías de la información y el gobierno de datos

1.6. Hipótesis.

Implementando una metodología de gestión de riesgos ad hoc se mejora la gestión de ciber riesgos en una empresa manufacturera peruana.

1.7. Objetivos.

1.7.1. Objetivo general.

Implementar una metodología de gestión de riesgos ad hoc basada en estándares internacionales y buenas prácticas para una empresa manufacturera peruana.

1.7.2. Objetivos específicos.

A. Seleccionar metodologías de gestión de riesgos de seguridad de la información.
B. Determinar las características de gestión de riesgos de seguridad de una empresa manufacturera peruana previamente seleccionada.
C. Diseñar la metodología de gestión de riesgos de seguridad de la información ad hoc en base a estándares internacionales y buenas prácticas.
D. Validar la metodología propuesta ante expertos relacionados en seguridad de la información.
E. Implementar la metodología con autorización de la empresa seleccionada para el estudio.

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

La investigación es de tipo cuantitativa – cuasi experimental porque a través de la recopilación y análisis de la información permitirá probar la hipótesis de la investigación.

2.2. Población y muestra.

Población.

Existen estándares internacionales y metodologías que ayudan a la empresa a direccionar sus políticas de gestión de riesgos, en diversos rubros. Para este estudio se seleccionaron aquellos estándares y/o metodologías que corresponden a la seguridad de la información y a la forma como dividen sus procesos en un total de 15, por lo tanto, esto corresponde a la población. La población estuvo estratificada por tipo de método como se detalla en el cuadro comparativo descrito en el Anexo 8. Los elementos de la población son listados de la siguiente manera:

a. **Estándares internacionales:**

1. ISO/IEC 27005.
2. AS/NZS 4360.
3. IT Grundschutz.
4. ISO/IEC 27004.

b. **Metodologías internacionales:**

5. MAGERIT
6. MEHARI
7. OCTAVE
8. SRA (Structured Risk Analysis)
9. CRAMM
10. CORAS
11. TARA.
12. EBIOS

c. **Marco de trabajo(framework) internacionales:**

13. FAIR
14. FRAP
15. Risk IT

Muestra.

Para la muestra se usó la técnica de muestreo no probabilístico de elección por conveniencia, porque existe mucha mayor información en casos de estudio a empresas con características similares, pero en países diferentes a Perú; donde ya han sido implantados los estándares y metodologías internacionales en gestión de riesgos, manifestados anteriormente en la población de esta investigación. Siendo lo siguiente estándares y/o metodologías los más utilizados en los artículos científicos consultados (Ver Anexo 8):

1. ISO 27005: Estándar internacional de gestión de riesgos de seguridad de la información considerado el esqueleto principal para la metodología a implementar.
2. RISK IT: Marco de referencia que nos ayuda a gestionar los riesgos en cuanto a conceptos de valor- beneficio para la empresa.
3. MAGERIT: metodología de gestión de riesgos basado en amenazas del activo apoyados en el estándar ISO 27005.
4. TARA: metodología enfocada al análisis de riesgo del activo del ciberespacio considerado ciber activo.

2.3. Variables, Operacionalización.

Tabla 1.

Operacionalización de las variables.

Variables	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos
Metodología de gestión de riesgos	Calidad de la implementación de la metodología.	Rendimiento	$R = \sum_{j=1}^{p} \left(\frac{\sum_{i=1}^{m} TR\ ij}{\sum_{i=1}^{n} TEij} \right) / p$	Técnica: Revisión Documental Instrumento: Ficha de registro de datos, Tabla SIPOC.
		Integridad	$I = \left(\sum_{j=1}^{p} \left(\frac{\sum_{i=1}^{m} C\ ij}{\sum_{i=1}^{n} Cij} \right) / p \right) * 100$	
		Complejidad	$C = \left({\sum_{i=1}^{n} Si}/{p} \right) * 100$	
Gestión de ciber riesgos.	Administración de la Gestión de ciber riesgos	Porcentaje de activos involucrados	$AI = \left(\frac{\sum_{i=1}^{m} A\ ij}{\sum_{i=1}^{n} Aij} \right) * 100$	
		Porcentaje de riesgos críticos	$RC = \left(\frac{\sum_{i=1}^{m} R\ ij}{\sum_{i=1}^{n} Rij} \right) * 100$	
		Porcentaje de controles seleccionados para el plan de tratamiento de riesgos.	$CPT = \left(\frac{\sum_{i=1}^{m} C\ ij}{\sum_{i=1}^{n} Cij} \right) * 100$	

Nota: Elaboración propia.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.

Las técnicas de recolección son de tipo cuantitativa porque todos los datos se recaban antes de analizarlo. Por ejemplo, para determinar la población y la muestra de nuestro estudio se tuvo que seleccionar de los artículos científicos los diferentes estándares y metodologías usadas para la gestión de riesgos de seguridad de la información.

Técnicas de recolección de datos.

Revisión documental (de organización y métodos).

Esta técnica tiene que ver con la organización de información registrada como, por ejemplo: artículos científicos y los procesos de la metodologías y estándares que se utilizaron en la construcción de la metodología. También MAGERIT nos proporciona lineamientos para desarrollar un plan de tratamiento, para realizar un plan de seguridad y un cuadro de roles (RACI)

Instrumentos de recolección de datos.

Ficha de registro de datos.

Instrumento relacionado con la técnica aplicada a la investigación documental. Es una forma de obtener un producto en base a fuentes investigadas; por ejemplo, fichas relacionadas al contexto de la organización donde se implementó la metodología, fichas para registro de datos de cada proceso que se implementó (Ver Anexo 8 y figura 5)

Tabla SIPOC.

Es una herramienta utilizada para caracterizar los procesos identificando elementos claves como proveedores (S), entradas (I), procesos (P), salidas(O) y clientes (C). En la investigación se utilizó en la caracterización de los procesos de la metodología propuesta. La tabla N°2 es el formato SIPOC propuesto para la investigación.

Tabla 2.

Formato SIPOC.

Responsable P	Entrada	Proceso			Salida	Responsable C
		Actividad	Formato	Duración		

Nota: Elaboración propia.

A continuación, se describió una pequeña leyenda de lo que debe ser registrado en el Formato SIPOC:

1. Responsable P, actor o actores responsables de proveer las entradas al proceso.
2. Entrada, documentos relevantes para iniciar el proceso.
3. Actividad, acción definida en verbo que ejecuta el proceso.
4. Formato, apoyo de registro sea lista, tabla, cuestionario, etc. que ayude con el recojo de información.
5. Duración, tiempo estimado en días que se contabiliza desde el inicio hasta el fin de la actividad.
6. Salida, producto de la actividad del proceso
7. Responsable C, actor o actores responsables de la recepción de las salidas.

2.5. Procedimiento de análisis de datos.

Para medir la calidad de la implementación en la metodología el análisis de datos empezó con las actividades aplicadas para gestión de riesgos a base de estándares y metodologías ya investigados en los artículos científicos de estudio alineados al contexto empresarial que en el caso de estudio fue de una empresa manufacturera.

Luego se ejecutó reuniones virtuales realizadas en las siguientes etapas:

a. A inicios del proyecto. Se realizó una ficha para en la reunión virtual con la parte interesada logrando plantear los objetivos del proyecto y lo que se necesita de la empresa para lograr la implementación.
b. En el transcurso del proyecto. Se realizó una reunión para cotejar datos procesados por el modelo.
c. Al término del proyecto. Se ejecutaron las dos últimas reuniones. Una con los expertos quienes analizaron el modelo y otra con el grupo de los interesados para presentar el informe final con los resultados.

Para el análisis estadístico se usó las operaciones de sumatoria y la media aritmética aplicados en las variables dependiente e independiente como sigue:

Análisis de datos variable independiente.

Tabla 3.

Análisis del indicador de Rendimiento.

Indicador	Rendimiento	
Fórmula	$R = \left(\sum_{j=1}^{p} \frac{TRj}{TEj} \right) / p$	
Variable	**Definición**	**¿Cómo se obtiene?**
R	Se refiere al tiempo promedio que se usará al aplicar los procesos de la metodología construida.	Se obtuvo al aplicar la fórmula.
TR	Es el tiempo real que se obtuvo al implementar cada proceso de la metodología.	Se obtiene del registro de la implementación de la metodología.
TE	Es el tiempo estimado para la implementación de cada proceso de la metodología.	Se obtiene del cronograma de ejecución de los procesos de la metodología
p	Cantidad de procesos de la metodología	

Nota: Elaboración propia.

Tabla 4.

Análisis del indicador de Integridad.

Indicador	Integridad	
Fórmula	$I = \left(\sum_{j=1}^{p} \left(\frac{\sum_{i=1}^{m} C\ ij}{\sum_{i=1}^{n} Cij} \right) / p \right) * 100$	
Variable	**Definición**	**¿Cómo se obtiene?**
I	Promedio de cumplimiento de la metodología de gestión con los estándares y/o metodologías de la muestra.	Se obtuvo aplicando la fórmula.
C	Características de los estándares y/o metodologías de la muestra	Se obtuvo de las definiciones de los procesos de los estándares y/o metodologías
m	Cantidad de características seleccionadas de los estándares y/o metodologías	Conteo de características seleccionadas de estándares y/o metodologías para la metodología de gestión.
n	Cantidad de características de los estándares y/o metodologías	Conteo de características totales de estándares y/o metodologías de la muestra
p	Cantidad de estándares y/o metodologías	Cantidad de estándares y/o metodologías de la muestra

Nota: Elaboración propia.

Tabla 5.

Análisis del indicador de Complejidad.

Indicador	Complejidad	
Fórmula	$C = \left(\sum_{i=1}^{n} Si / p\right) * 100$	
Variable	**Definición**	**¿Cómo se obtiene?**
C	Porcentaje de nivel de complejidad del cuadro SIPOC	Se obtuvo aplicando la fórmula.
S	Nivel de complejidad de los cuadros SIPOC por fase de la metodología	Definición de nivel de complejidad de cuadros SIPOC
n	Cantidad de nivel de complejidad de los cuadros SIPOC por fase	Conteo de cuadros SIPOC por fase de la metodología
p	Cantidad de fases de la metodología	Conteo de fases de la metodología

Nota: Elaboración propia.

Análisis de datos variable Dependiente.

Tabla 6.

Análisis del indicador de Porcentaje de activos involucrados.

Indicador	Porcentaje de activos involucrados	
Fórmula	$AI = \left(\frac{\sum_{i=1}^{m} A\,ij}{\sum_{i=1}^{n} Aij}\right) * 100$	
Variable	**Definición**	**¿Cómo se obtiene?**
AI	Porcentaje de activos involucrados en la gestión de riesgos.	Se obtiene al aplicar la fórmula
A	Son los activos en la gestión de riesgos.	Se obtiene de la fase 2 del modelo.
m	Cantidad de activos identificados en la empresa	Se obtiene de la realidad de la empresa
n	Cantidad de activos reales relacionados con la gestión de riesgos	Se obtiene de la fase 2 del modelo.

Nota: Elaboración propia.

Tabla 7.

Análisis del indicador de Porcentaje de riesgos críticos.

Indicador	Porcentaje de riesgos críticos	
Fórmula	$RC = \left(\frac{\sum_{i=1}^{m} R\ ij}{\sum_{i=1}^{n} Rij}\right) * 100$	
Variable	**Definición**	**¿Cómo se obtiene?**
RC	Es el porcentaje de criticidad de riesgo en la gestión de riesgos.	Se obtiene al aplicar la fórmula
R	Son los riesgos de la gestión.	Se obtiene de la fase 3 del modelo
m	Cantidad de riesgos con nivel de criticidad en la empresa	Se obtiene de la realidad de la empresa.
n	Cantidad de riesgos relacionados con la gestión de riesgos	Se obtiene de la fase 3 del modelo

Nota: Elaboración propia.

Tabla 8.

Análisis del indicador de Porcentaje de controles seleccionados para el plan de tratamiento de riesgos.

Indicador	Porcentaje de controles seleccionados para el plan de tratamiento de riesgos	
Fórmula	$CPT = \left(\frac{\sum_{i=1}^{m} C\ ij}{\sum_{i=1}^{n} Cij}\right) * 100$	
Variable	**Definición**	**¿Cómo se obtiene?**
CPT	Es el porcentaje de controles seleccionados para el plan de tratamiento de riesgos.	Se obtiene al aplicar la fórmula
C	Son los controles del plan de tratamiento de riesgos.	Se obtiene de la Fase 4 del modelo
m	Cantidad de controles alineados a la empresa.	Se obtiene de la realidad de la empresa.
n	Cantidad de controles propuestos para el tratamiento de riesgos.	Se obtiene de la MAGERIT

Nota: Elaboración propia.

2.6. Criterios éticos.

Los criterios éticos se relacionaron con el grado de confiabilidad que se demostrará en la metodología de gestión de riesgos y por ello se aplicó los siguientes criterios.

a. Criterio de confidencialidad.

La información que otorgó la empresa manufacturera requerida para esta investigación se obtuvo de manera legal respetando las políticas internas de seguridad de información y respetando la Ley 29733 “Ley de protección de datos personales”. El estado penaliza el mal uso de la información entregada, es por ello que se protegió la información ante cualquier comportamiento inadecuado.

b. Criterio de conformidad.

El estudio buscó estar alineado con las leyes que el colegio de ingenieros del Perú establece dentro de sus políticas internas respecto a la ética profesional que caracteriza a los profesionales de esta rama de la ciencia, por ello, se buscó que los expertos seleccionados manifiesten compromiso con el código deontológico del colegio profesional en mención, considerando las penalidades sujetas al incumplimiento de objetividad y transparencia.

2.7. Criterios de Rigor Científico.

La presente investigación se ejecutó bajo un enfoque cuantitativo, por lo que validó la aplicabilidad de la metodología, bajo criterios científicos que permitan su transferibilidad en contexto similares, midiendo los indicadores propuestos, generados a partir de la recolección de resultados y orden correspondiente, de manera exhaustiva, clara y concisa.

a. Criterio de claridad.

Bajo este criterio se buscó que lo manifestado en la metodología sea entendible en el lenguaje aplicado, sin llegar a cometer ambigüedad de

definición de términos o conflictos de elementos, alterando el entendimiento del responsable de la implementación en la organización.

b. Criterio de objetividad.

Los resultados fueron medibles y concretos dentro de la conducta que manifestaron, permitiendo datos concretos del contexto y de la realidad obtenida tras la implementación de la metodología propuesta.

c. Criterio de coherencia.

Las descripciones de actividades manifestaron correspondencia lógica entre la teoría y lo plasmado dentro de la metodología propuesta, con el fin de reforzar la premisa de que la curva de aprendizaje de la metodología debe ser corta y mantener así, el nivel de complejidad, en bajo grado.

d. Criterio de pertinencia.

El contenido de la metodología buscó respetar los principios de seguridad de la información y términos familiarizados a la gestión de riesgos de seguridad de la información. Se evitó confusión con términos de riesgos financieros, riesgos de salud, riesgos operacionales, entre otros similares.

e. Criterio de suficiencia.

La metodología buscó cubrir lo exigido por los principios de la gestión de riesgos, y manifestó suficiencia en sus actividades e instrumentos construidos.

f. Criterio de relevancia.

Los elementos de la metodología fueron importantes para lograr el entendimiento de la gestión de riesgos y determinar claramente los objetivos que busca enfrentar dentro de la organización.

III. RESULTADOS.

3.1. Resultados en Tablas y Figuras.

La investigación tuvo como objetivo diseñar la metodología de gestión de riesgos de seguridad de la información ad hoc en base a estándares internacionales y buenas prácticas.

Después de analizar los resultados obtenidos en la metodología a implementar se procedió a registrar los datos obtenidos en los indicadores de las variables, tal como sigue:

El primer indicador es Rendimiento y se calculó por la siguiente fórmula:

$$R = \left(\sum_{j=1}^{p} \frac{TRj}{TEj} \right) / p$$

Se manifestó que el tiempo real (*TR*) en comparación al tiempo estimado (*TE*) que se usó al aplicar los 4 procesos de la metodología (p) resultó en una media de 1.10 días hábiles para el indicador de rendimiento. Por ejemplo, el tiempo estimado para el Proceso 4 fue de 15 días hábiles pero el tiempo de implementación fue de 8 días hábiles resultando en una media de 0.53 días hábiles convirtiendo al Proceso 4 en uno de los procesos con mejor rendimiento. Ver figura 11.

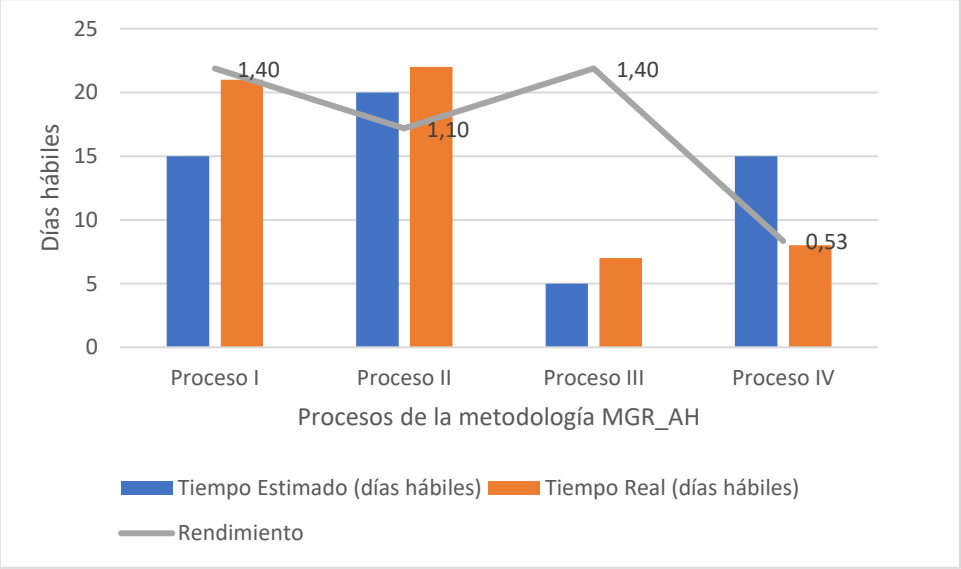


Figura 11. Rendimiento por procesos de la metodología MGR_AH. Fuente: Elaboración propia.

Para el segundo indicador de integridad se utilizó la siguiente fórmula:

$$I = \left(\sum_{j=1}^{p} \left(\frac{\sum_{i=1}^{m} C\ ij}{\sum_{i=1}^{n} Cij} \right) / p \right) * 100$$

Donde *C* son las características de los estándares y/o metodologías de la muestra utilizada en la investigación. La metodología propuesta integra en sus procesos 1 estándar, 2 metodologías y 1 marco de referencia. Cada uno de los cuales presenta un total de características que mediante un criterio de selección fueron elegidas para la metodología propuesta. Se consideró en un 50% al estándar ISO/ IEC 27005. Este estándar en comparación de los 4 métodos elegidos representa un 13% como promedio de cumplimiento de la metodología de gestión con los estándares y/o metodologías de la muestra. Ver Tabla N°9.

Tabla 9.

Resultado del análisis del indicador integridad.

Modelo	Tipo de modelo	Total, de características	Características elegidas	Porcentaje	Porcentaje Promedio
ISO/IEC 27005	Estándar	8	4	50%	13%
TARA	Metodología	3	1	33%	8%
MAGERIT v3.0	Metodología	3	1	33%	8%
RISK IT	Framework	6	2	33%	8%
Total	4	20	8	40%	10%

Nota: Elaboración propia.

El tercer indicador fue el nivel de complejidad del cuadro SIPOC:

$$C = \left(\sum_{i=1}^{n} Si / p \right) * 100$$

El nivel de complejidad (Si) fue determinado por criterio de observación de la cantidad de actividades que hay en cada proceso debido a que la metodología dividida en 4 procesos determinó 4 cuadros SIPOC. Por ejemplo, el proceso II y IV presentan 2 actividades por tanto el nivel de complejidad del cuadro SIPOC en estos procesos es “Complejo” en comparación con los procesos I y III que presentan 1 actividad. Ver tabla N°10.

Por lo tanto, el porcentaje de nivel de complejidad del cuadro SIPOC está equilibrado en un 50%, lo que significa que la metodología contempla actividades más complejas que otras. Ver figura 12.

Tabla 10.

Resultado del análisis del indicador complejidad

Procesos	Cantidad de Actividades	Cantidad Cuadro SIPOC	Nivel de Complejidad SIPOC
Proceso I	1	1	No complejo
Proceso II	2	1	Complejo
Proceso III	1	1	No complejo
Proceso IV	2	1	Complejo

Nota: Elaboración propia.

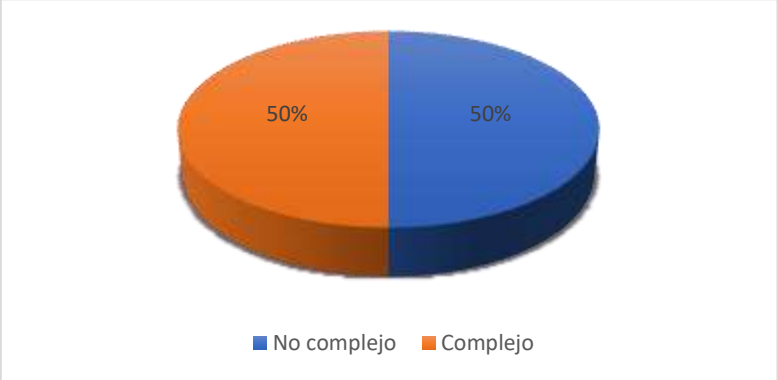


Figura 12. Complejidad de cuadros SIPOC de la metodología MGR_AH. Fuente: Elaboración propia.

El cuarto indicador ya tiene relación con los procesos propios de la gestión del ciber riesgo: la identificación de activos. El porcentaje de activos involucrados se calculó como sigue:

$$AI = \left(\frac{\sum_{i=1}^{m} A\,ij}{\sum_{i=1}^{n} Aij}\right) * 100$$

En la administración de la Gestión de ciber riesgos se identificó un total de 27(*n*) activos de los cuales 13 (*m*) fueron ciber activos priorizados (activos reales) lo que representa un 32% del porcentaje de activos involucrados en la gestión del riesgo. Ver figura 13.

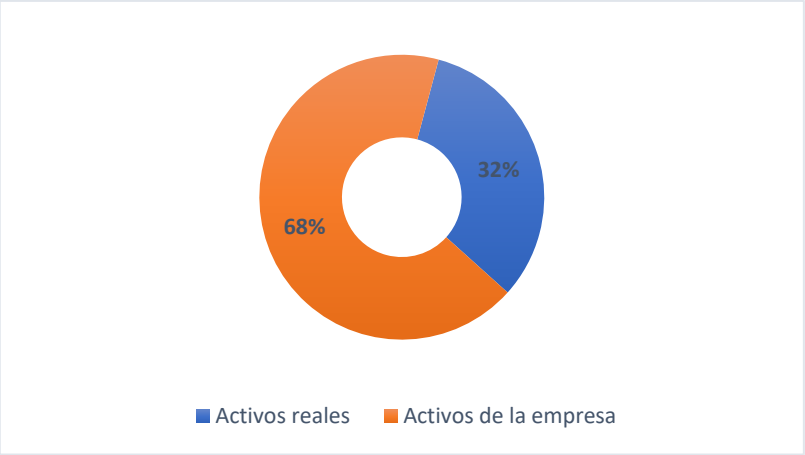


Figura 13. Porcentaje de activos involucrados en la Gestión de ciber riesgos. Fuente: *Elaboración propia.*

El quinto indicador fue porcentaje de riesgos críticos:

$$RC = \left(\frac{\sum_{i=1}^{m} R\ ij}{\sum_{i=1}^{n} Rij}\right) * 100$$

Estos activos determinaron un total de 23 riesgos relacionados con la gestión(*n*) de los cuales sólo 4 riesgos se consideraron con un nivel de criticidad (*m*) para la empresa. Estos riesgos representaron un porcentaje del 15% de criticidad de riesgo en la gestión de ciber riesgo como se observa en la figura 14.

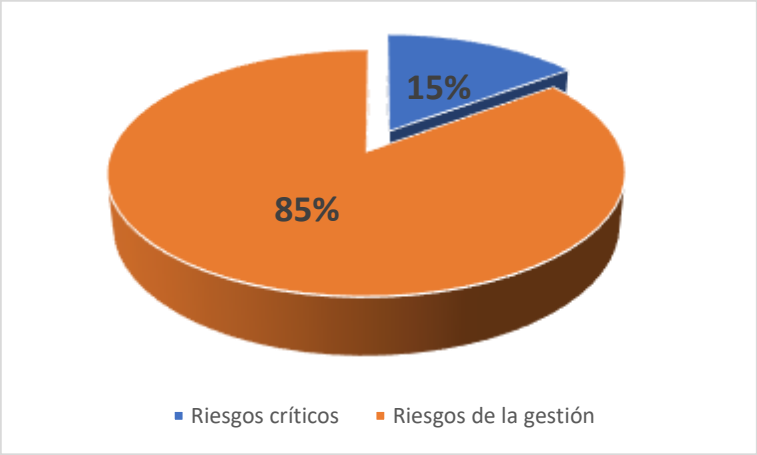


Figura 14. Porcentaje de riesgos críticos involucrados en la Gestión de ciber riesgos. Fuente: Elaboración propia.

Finalmente, el último indicador fue el porcentaje de controles seleccionados para el plan de tratamiento de riesgos:

$$CPT = \left(\frac{\sum_{i=1}^{m} C\ ij}{\sum_{i=1}^{n} Cij}\right) * 100$$

Los 19 controles (n) que fueron seleccionados para el plan de tratamiento de riesgos se determinaron con ayuda del catálogo de contramedidas de MAGERIT, pero sólo 3 controles fueron elegidos (m) para el plan de tratamiento de riesgos. Esto representó un 14%. Ver figura 15.

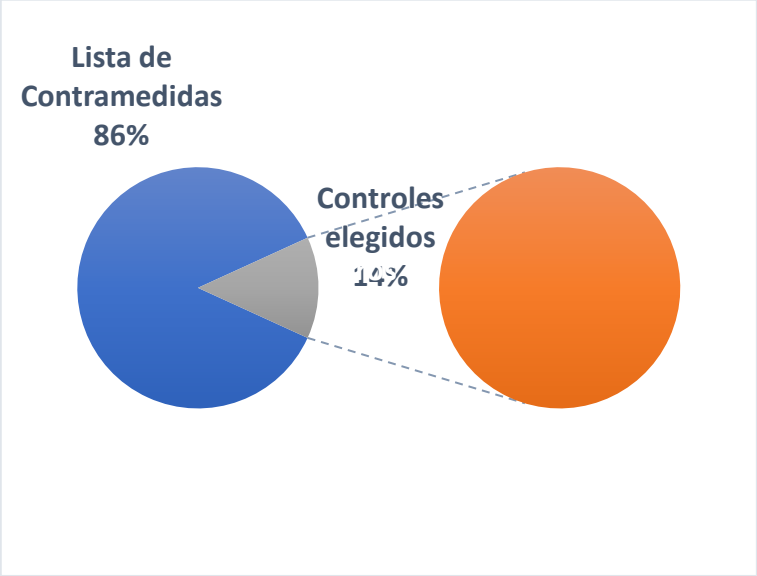


Figura 15. Porcentaje de controles involucrados en la Gestión de ciber riesgos. Fuente: Elaboración propia.

3.2. Discusión de resultados.

Los resultados obtenidos en la investigación pueden ser comparables con el indicador de integridad en relación a la cantidad de número de procesos que adoptan las diferentes metodologías del estándar internacional ISO /IEC 27005. Por ejemplo, Tran et al., (2019) utilizó en su diseño de metodología al estándar ISO /IEC 27005, FMVEA, Árbol de ataques, EVITA, MEHARI, ED202A/DO326 y SORA; adoptando de 5 procesos del estándar ISO /IEC 27005 considerando a los árboles de ataque en su etapa de análisis de riesgo. La investigación

también adoptó el 50% de los procesos de la norma ISO /IEC 27005 pero consideró los vectores de ataque en su etapa de análisis de riesgo.

Tran et al., (2019) en su metodología construyeron 6 árboles de ataque, y obtuvieron 24 requerimientos de ciberseguridad, para un Gestionar los ciberriesgos en Sistemas Aéreos no tripulados, ante posibles ciberataques terroristas a comparación de nuestra metodología que adoptó conceptos de cyberactivo y ciber riesgos que poco se utiliza en investigaciones locales tras lo cual decidimos utilizar TARA para simular a través de los vectores de ataques los requerimientos de ciberseguridad basados en los árboles de ataque, obteniendo 23 vectores de ataque basado en vulnerabilidades de los activos priorizados y 19 contramedidas.

3.3. Aporte práctico.

Se estableció una hoja de ruta para el desarrollo de la investigación, esta hoja de ruta consta de seis etapas. En la primera etapa (A); se revisó la bibliografía utilizando bases de datos que se consideran representativas en la rama de ciencias de la computación como IEEE Xplore y ACM Digital Library. Esta revisión se realizó con el fin de identificar metodologías, estándares y marcos de gestión de riesgos de seguridad de la información. Al término de este proceso se identificaron 15 métodos de cómo gestionar riesgos de seguridad de información. En la segunda etapa; (B) se realizó un cuadro para seleccionar las metodologías, estándares y marcos de trabajo apoyados en criterios de selección como: enfoque de riesgo basado en TI, tipo de empresa, casos de estudio aplicado y procesos enfocados a vulnerabilidades de activos; de esta etapa se seleccionaron 4 métodos. Para la tercera etapa (C); se contextualizó a la empresa en una ficha que registra los objetivos de la empresa, los objetivos de tecnologías de información alineados a los objetivos empresariales, los roles y funciones del personal y/o áreas involucradas en el giro del negocio. En la cuarta etapa(D); se definió el diseño de la metodología utilizando la herramienta SIPOC que describe las actividades de cada uno de los procesos de la metodología propuesta. En la quinta etapa (E); se validó la metodología propuesta ante expertos mediante la aplicación del método DELPHI y según

valoración se determinó si la implementación de la metodología propuesta cumplió con los indicadores antes planteados. Finalmente, la sexta etapa (F), permitió registrar las diferencias de los riesgos gestionados a través de la metodología propuesta. La ilustración de continuidad de las etapas se visualiza en la figura 16.

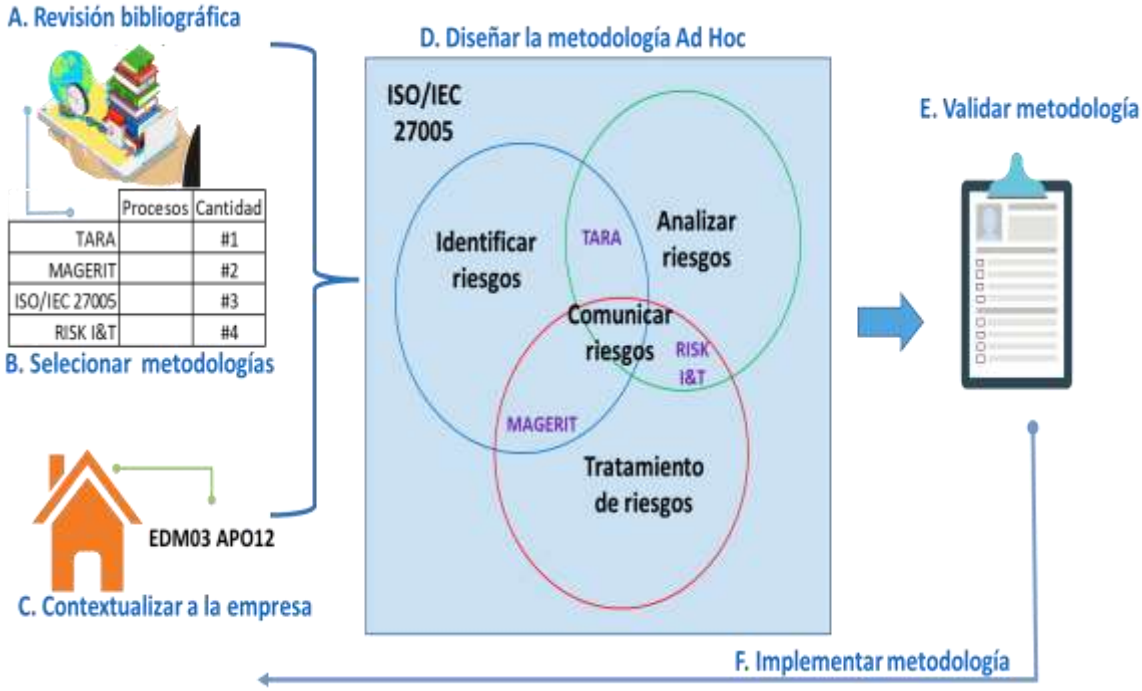


Figura 16. Propuesta de método. Fuente: Elaboración propia.

Para iniciar la búsqueda bibliográfica se realizó un listado de 11 palabras claves relacionadas a la gestión del riesgo teniendo, en cuenta términos relacionados con la empresa, el recurso humano, operacionalidad de metodologías, marcos de trabajo y seguridad en el ciberespacio, todos relacionados con las tecnologías de información (TI). Al realizar el análisis correspondiente, se listaron cada una de las palabras con su utilización y relación con los términos descritos en la tabla N°11 y de esta manera conocer qué modelos de gestión de riesgos relacionados con TI existen a nivel internacional, además de conocer sus autores y en qué países se utilizaron esos modelos.

Tabla 11.

Lista de palabras claves.

Palabras claves	Utilización
Companies	Caso de uso en pequeñas o medianas empresas
Cyber	Términos del ciberespacio.
Finance	Términos financieros en gestión de riesgos
Framework	Uso de marcos de trabajo relacionados con seguridad de la información.
Human Resource	Personas de las áreas de TI
Management	Términos de gestión relacionados con seguridad de la información.
Methodologies	Uso de metodologías relacionadas con seguridad de la información.
Operational	Términos de operacionalidad relacionado con TI.
Risk	Términos de riesgo relacionados en TI.
Security	Términos de seguridad relacionados en TI.
Standards	Uso de estándares relacionados con seguridad de la información.

Nota: Elaboración propia.

A partir de una matriz de combinación de palabras se registró las posibles cadenas de búsqueda verificables en el Anexo 10. Para la elección de estas cadenas se optó por las combinaciones que involucren las palabras: “risk”, y “management”, por estar relacionados al problema de estudio. Luego de esa elección se realizó un siguiente filtro relacionado con la teoría de gestión del riesgo de donde se registró con “Sí”: si la combinación se relacionó con la gestión del riesgo y “No”: si la combinación no se relacionó con la gestión de riesgo. El resultado de este cuadro de doble entrada se muestra en la tabla N°12.

Tabla 12.

Cadena de búsqueda.

Orden	Combinación de palabras	Relacionado con gestión del riesgo
1	companies management	No
2	companies risk	No
3	cyber management	No
4	cyber risk	Sí
5	finance management	No
6	finance risk	No
7	framework management	No
8	framework risk	No

9	human resource management	No
10	human resource risk	No
11	management companies	No
12	management cyber	No
13	management finance	No
14	management framework	No
15	management human resource	No
16	management management	No
17	management management	No
18	management methodologies	No
19	management operational	No
20	management risk	Sí
21	management risk	No
22	management security	No
23	management standards	No
24	methodologies management	No
25	methodologies risk	No
26	operational management	No
27	operational risk	No
28	risk companies	No
29	risk cyber	Sí
30	risk finance	No
31	risk framework	Sí
32	risk human resource	No
33	risk management	Sí
34	risk management	No
35	risk methodologies	Sí
36	risk operational	No
37	risk risk	No
38	risk risk	No
39	risk security	Sí
40	risk standards	Sí
41	security management	No
42	security risk	No
43	standards management	No
44	standards risk	No

Nota: Elaboración propia.

Una vez que se evaluó la cada cadena, se seleccionó los que cuentan con Sí, obteniendo como resultado un total de ocho cadenas para utilizarlos en búsquedas científicas. Ver Tabla N°13.

Tabla 13.

Selección de cadena de búsqueda.

Cadena de búsqueda
management risk
risk cyber
risk framework
risk management
risk methodologies
risk security
risk standards
cyber risk

Nota: Elaboración propia.

A través de estas cadenas de búsqueda se realizó la revisión bibliográfica en las bases de datos de IEEExplore y ACM Digital Library encontrando un total de 15 modelos para gestionar riesgos de la información conformados por 4 estándares, 8 metodologías y 3 marcos de trabajo.

Para la elección de estándares y metodologías; se determinó en mesa de trabajo ciertos criterios como: enfoque de riesgo basado en TI, tipo de empresa, casos de estudio identificado y procesos enfocados a vulnerabilidades de activos, ver tabla N°14.

Tabla 14.

Selección de cadena de búsqueda.

Criterio	**Detalle**
Criterio a:	Enfoque riesgo basado en TI, se refiere a los criterios de los procesos orientados específicamente a lo relacionado con TI.
Criterio b:	Tipo de empresa, se refiere a la cantidad de empleados de la empresa por lo tanto si es pequeña sería en un margen de 10 a 50 trabajadores y mediana de aproximadamente hasta 250 empleados.
Criterio c:	Casos de estudio, se refiere a si la metodología, estándar o framework fue implementado en estudio real de alguna empresa.
Criterio d:	Procesos enfocados a vulnerabilidades de activos, se refiere a los procesos de las metodologías, estándares o framework enfocados al estudio de cualquier debilidad del activo de riesgo.

Nota: Elaboración propia.

Cada modelo de gestión de riesgos identificado, fue evaluado en cada criterio definido. El mecanismo de evaluación consistió en asignar 1 o 0 a cada criterio en cada modelo; donde la puntuación “1” indica la afirmación del criterio en el modelo y “0” indica la negación del criterio en el modelo. Esto permitirá obtener un valor entre 0 a 4 por cada modelo, por lo que como se detalla en la Tabla N°15 para determinar la elección del modelo.

Tabla 15.

Escala de puntuación.

Puntaje	Detalle
0-2	no se elige
3	puede elegirse
4	se elige

Nota: Elaboración propia.

Luego de que los investigadores llegaron a un consenso de puntuación, se procedió a calcular la suma de calificaciones por los criterios de cada modelo. Ver Tabla N°16.

Tabla 16.

Cuadro de puntuación de estándares, metodologías y frameworks.

Criterio/ modelo	ISO/ IEC 270 05	AS/ NZS 436 0	FRAP/F RAAP -	OCT AVE -	IT Grunds chutz	MAG ERIT 3.0	MEH ARI	S R A	CRA MM - CCT A	FA IR	CO RAS	TA RA	RISK IT FRAME WORK	EBI OS - Et	ISO/ IEC 270 04
a.	1	0	1	0	0	1	0	0	1	0	0	0	1	0	0
b.	1	0	1	1	1	1	1	1	1	0	1	1	1	1	1
c.	1	0	0	0	0	1	0	0	0	0	0	1	0	0	0
d.	1	0	0	0	0	0	1	1	0	0	0	1	1	0	0
Total	4	0	2	1	1	3	2	2	2	0	1	3	3	1	1

Nota: Elaboración propia.

Con ello, según las escalas de puntuación por modelo, se lograron determinar cómo modelos seleccionables a: ISO/IEC 27005, MAGERIT 3.0, TARA y RISK IT. Ver Tabla 17.

Tabla 17.

Selección de estándares, metodologías y frameworks.

Nombre Modelo	Tipo de modelo	Puntuación
ISO/IEC 27005	Estándar	4
TARA	Metodología	3
MAGERIT	Metodología	3
RISK IT	Framework	3

Nota: Elaboración propia.

El estándar ISO/IEC 27005 (puntuado en 4) se eligió como norma internacional. Esta norma brindó la pauta a seguir en una gestión de riesgos de seguridad de la información, y luego de revisar los casos prácticos de la aplicación de esta norma en otras empresas se pudo entender sus procesos. La elección de las metodologías TARA y MAGERIT (puntuadas en 3) ayudaron en la identificación de activos, vulnerabilidades y contramedidas para la valoración de riesgos. TARA como metodología abarca el estudio de un activo cibernético conocido

como cyberactivo o activo del ciberespacio para luego evaluar los riesgos cibernéticos y sus mitigaciones además de ser apoyado por una evaluación de contramedida basado en costo/beneficio como estrategia de selección. Y MAGERIT como metodología sigue las pautas para el proceso de análisis de riesgos del estándar ISO/IEC 27005. La elección de MAGERIT en su versión 3.0 aportó formatos de estimación y planificación de riesgos. Y finalmente la elección RISK IT 2da. Edición (puntuado en 3) elegido como marco de trabajo el cual manifiesta que todo estudio del riesgo implica también la identificación de los ciberriesgos que afectan en un punto adicional a la seguridad de la información llamada ahora ciberseguridad ya que actualmente la principal gestión del riesgo son los relacionados con la Información y la Tecnología (TI).

Para determinar las características de gestión de riesgos de seguridad de una empresa se buscó como caso de estudio a una empresa manufacturera del Perú dentro del círculo de contactos directo de los investigadores logrando contactar con 2 empresas: CARROCERIAS Y MOTOTAXIS DIOS ES AMOR E.I.R.L ubicada en José L. Ortiz- Lambayeque y la empresa ASIU SELVA SOCIEDAD ANONIMA CERRADA ubicada en Maynas - Iquitos ambos dedicados a la venta, mantenimiento y reparación de motocicletas, sus accesorios y piezas. De acuerdo al criterio de disponibilidad de la información; necesarios para el avance de la propuesta y de un facilitador miembro del área de T&I de la empresa que brinde apoyo en los datos de los procesos de la misma; se decidió optar por la empresa ASIU SELVA S.A.C. porque cuenta con el apoyo del encargado del área soporte que está interesado en implementar mejoras en el área de TI de la empresa y por lo tanto, el acceso a la información es confiable y disponible.

La gerente de la empresa, Zoila Magali Asiu Saavedra y el encargado del Área de Sistema, Víctor Andree Campoverde Vega; desde ahora considerados como las partes interesadas, manifestaron a través de videoconferencias de la plataforma digital Zoom los procesos internos de la empresa limitando especificaciones de montos económicos por lo que se tomaron estas decisiones:

a. Primero se explicó el objetivo del proyecto al gerente de la empresa.

b. Se solicitó permiso para recopilar información sobre la gestión de los procesos principales, así como los lineamientos estratégicos de la empresa y de TI.

Se describió a la empresa a través de la ficha de contexto organizacional en el cual se describe información general y relevante para el alineamiento de gestión dentro de la empresa, esta ficha está basada en el marco de referencia de RISK IT (Ver anexo 13), que ofrece una guía a las empresas para orientar sus objetivos empresariales a lineados a los objetivos de TI del negocio. Para el registro de información en la ficha de contexto, se aplicó revisión documental del estatuto de constitución y ficha RUC, complementando con información obtenida en la entrevista con las partes interesadas. Para las secciones de Metas empresariales y Metas de alineamiento de TI, se utilizó la Guía de obtención de metas empresariales y metas de alineamiento de TI (Anexo 14). Ver Figura 17.

1-INFORMACIÓN EMPRESA			
Número de reunión:	1	Fecha de reunión:	Junio 2021
Empresa:	ASIU SELVA S.A.C.	RUC:	20604209316
Preparado por:	Bobadilla Campos Rolando Martín. Guevara Chambergo Jhon Dennis.		
Revisado por:	Víctor Andree Campoverde Vega.		
Autorizado por:	Zoila Magali Asiu Saavedra.		
2- CONTEXTO DE LA ORGANIZACIÓN			
La empresa ASIU SELVA S.A.C. está dedicada a la venta, mantenimiento y reparación de motocicletas, sus accesorios y piezas, cuenta con 21 años de experiencia en el rubro. Actualmente cuenta con un promedio de 50 trabajadores. La gerente Zoila Asiu Saavedra es la dueña de la empresa manifestó que la demanda de construcción y mantenimiento de mototaxis en la selva y norte del país, se ha mantenido en crecimiento exigiendo mejorar procesos internos para la importación de materiales o repuestos, automatización de información de compra y venta, y además capacitación de personal en los diversos procedimientos funcionales de la empresa.			
3- METAS EMPRESARIALES			
1. Establecer la identificación de riesgos generales para inicios del año 2022.			

2. Mantener el margen de tolerancia por debajo del límite, de los incidentes de continuidad del negocio.
4- METAS DE ALINEAMIENTO DE TI
1. Mantener la identificación de riesgos relacionados con el área de Sistemas. 2. Mantener los procedimientos del área de sistemas bajo los parámetros de los indicadores de rendimiento.
5- ROLES Y FUNCIONES
La empresa ha establecido sus diversas áreas a través de un organigrama descrito en el Anexo 8.

Figura 17. Formato para contextualizar a la empresa. Fuente: *COBIT 2019* (ISACA, 2019).

El diseño de la metodología propuesta, inició identificando los procesos que componen a cada estándar y metodologías seleccionados. Ver tabla N°18.

Tabla 18.

Descripción de procesos de ISO/IEC 27005, MAGERIT, TARA y RISK IT.

Modelo	Procesos	Total
ISO/IEC 27005	Establecimiento de contexto (EC). Identificación del riesgo (IR). Estimación de riesgos (ER). Evaluación del riesgo (VR). Tratamiento del riesgo (TR). Aceptación del riesgo (AR). Comunicación del riesgo (CR). Monitoreo del riesgo (MR).	8
MAGERIT	Método de análisis de riesgos (MAR). Proyecto de análisis de riesgos (PAR). Plan de seguridad (PS).	3
TARA	Alcance TARA (TS). Evaluación de susceptibilidad a amenazas cibernéticas (CTSA). Análisis de corrección de riesgos cibernéticos (CRRA).	3
RISK IT	Conectar con los objetivos de la empresa (COE). Alineamiento con el ERM (ERM). Balance de Costo/beneficio relacionado con el riesgo de IT (BCB). Promover una comunicación abierta y con ética (COM). Establecer un tono adecuado con los tomadores de decisión (TD). Utilizar un enfoque coherente alineado con la estrategia (EAE).	6

Nota: Procesos descritos en ISO 27005 (2011), MAGERIT versión 3.0 (2012). TARA (2014) y RISK IT (ISACA, 2020).

Luego del entendimiento de estos procesos, se elaboró una matriz de evaluación entre los procesos del estándar ISO/IEC 27005 contra las metodologías MAGERIT, TARA y RISK IT, marcando con "X" los procesos de estas metodologías alineadas al estándar ISO/IEC 27005, marcando con "XX" el proceso diferenciador, entre las metodologías, alineado al estándar ISO/IEC 27005, en caso de no presentarse un alineamiento con el estándar se marcó con "–"; por ejemplo, los procesos de: "Establecimiento de contexto, Identificación, Estimación y Tratamiento de los riesgos" de ISO/IEC 27005 estuvieron presentes en los procesos de TARA, MAGERIT y RISK IT. A excepción del proceso: "Comunicación del riesgo" que estuvo presente sólo en los procesos de MAGERIT y RISK IT. Los resultados de esta evaluación se registraron en la tabla N°19.

Tabla 19.

Evaluación de procesos de las metodologías alineados a ISO/IEC 27005.

Procesos ISO/IEC 27005	**MAGERIT**		**TARA**			**RISK IT**						
	MAR [1]	**PAR** [1]	**PS** [1]	**TS** [2]	**CTSA** [2]	**CRRA** [2]	**COE** [3]	**ERM** [3]	**BCB** [3]	**COM** [3]	**TD** [3]	**EAE** [3]
Establecimiento de contexto.	–	x	–	x	–	–	xx	–	–	–	–	–
Identificación del riesgo.	xx	–	–	–	x	–	x	–	–	–	–	–
Estimación de riesgos.	x	–	–	–	xx	–	–	–	x	–	–	–
Evaluación del riesgo.	x	–	–	–	x	–	–	–	–	–	–	–
Tratamiento del riesgo.	–	–	x	–	x	x	–	–	xx	–	–	–
Aceptación del riesgo.	–	–	–	–	–	x	–	–	x	–	–	–
Comunicación del riesgo.	–	x	–	–	–	–	–	–	–	x	x	x
Monitoreo del riesgo.	–	–	–	–	–	–	–	–	–	–	x	x

Nota: [1]Procesos de la metodología MAGERIT, [2] Procesos de la metodología TARA, [3] Procesos del Framework RISK IT.

La propuesta de la metodología ad hoc adoptó los procesos seleccionados de la ISO/IEC 27005 priorizando los procesos marcados "xx" en cada metodología. Por ejemplo, en la tabla N°18 el proceso "PAR" de MAGERIT obtuvo mayor

relación con el proceso “Estimación de riesgos” porque brinda guías de ayuda para una correcta estimación; a diferencia de los procesos de TARA y RISK IT. Estas valoraciones de la selección de procesos se visualizan en tabla N°20 y tabla N°21.

Tabla 20.

Procesos seleccionados del estándar ISO/IEC 27005.

Modelo	Procesos seleccionados	Cantidad
ISO/IEC 27005	Establecimiento de contexto. Identificación del riesgo. Estimación de riesgos. Tratamiento del riesgo.	4

Nota: Procesos descritos en ISO 27005 (2011)

Tabla 21.

Procesos seleccionados de las metodologías basado en ISO 27005.

Modelo	Procesos seleccionados	Cantidad
MAGERIT	Método de análisis de riesgos (MAR).	1
TARA	Evaluación de susceptibilidad a amenazas cibernéticas.	1
RISK IT	Conectar con los objetivos de la empresa. Balance de Costo/beneficio relacionado con el riesgo de IT.	2

Nota: Procesos descritos en MAGERIT versión 3.0 (2012). TARA (2014) y RISK IT (ISACA, 2020).

Luego de determinar los procesos seleccionados se construyó una tabla resumen con base en la tabla N°19 para definir los nombres de los procesos de la metodología Ad hoc. Se eliminaron las columnas de procesos de metodologías no seleccionadas y las filas de proceso del estándar ISO/IEC 27005 no seleccionadas, tras ello se reemplazó el valor “XX” por un nombre en particular. Ver tabla N°22.

Tabla 22.

Evaluación de procesos de las metodologías alineados a ISO/IEC 27005.

Procesos ISO/IEC 27005	**MAGERIT**	**TARA**	**RISK IT**	
	MAR[1]	**CTSA[2]**	**COE[3]**	**BCB[3]**
Establecimiento de contexto.			Definir Alcance	
Identificación del riesgo.	Valoración de ciber riesgo			
Estimación de riesgos.		Evaluación de ciber riesgo		
Tratamiento del riesgo.				Plantear registros de riesgos

Nota: [1]: Procesos de la metodología MAGERIT, [2]: Procesos de la metodología TARA, [3]: Procesos del Framework RISK IT.

Finalmente, la metodología de Gestión de Riesgos Ad Hoc en relación con los procesos seleccionados, se dividió en 4 procesos: i) Definir Alcance, ii) Evaluación de ciber riesgo, iii) Valoración de ciber riesgo y iv) Plantear registros de riesgos, y 6 actividades. Los cuales están descritos en la tabla N°23.

Tabla 23.

Actividades por proceso de la metodología Ad Hoc

Procesos	**Actividades**
Definir Alcance	Definir Alcance
Evaluación de ciber riesgo	Identificar eventos de riesgo
	Analizar riesgo
Valoración de ciber riesgo	Estimar riesgo
Plantear registros de riesgo	Priorizar respuestas a los riesgos
	Comunicar resultado

Nota: Elaboración propia.

Tras el análisis se diseñó visualmente la interacción de procesos y recursos de la metodología Ad Hoc según la figura 18.

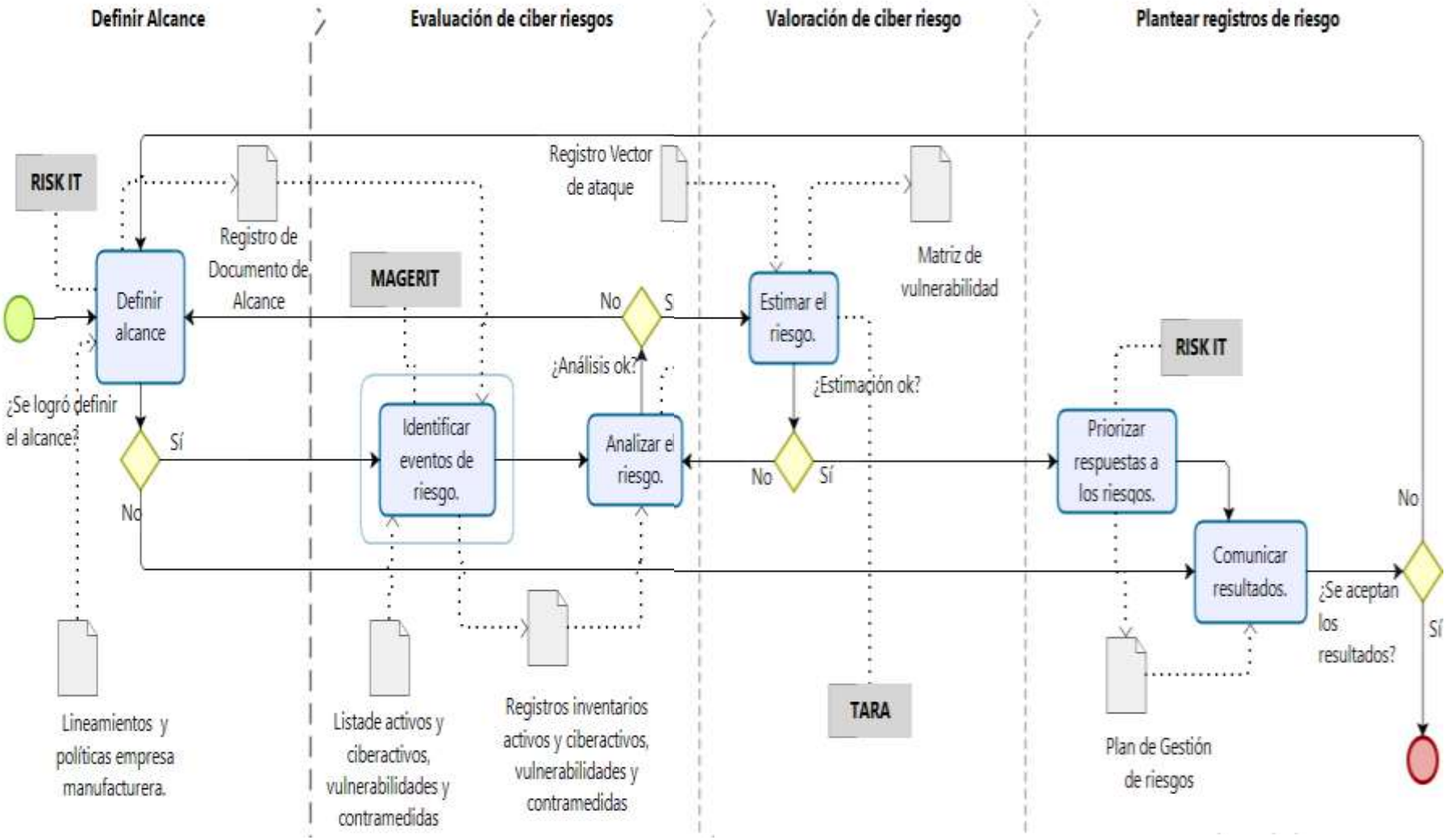


Figura 18. Metodología de Gestión de Riesgos Ad Hoc (MGR_AH). Fuente: Elaboración propia.

La descripción de cada proceso se realizó a través de la herramienta SIPOC. Estos 4 SIPOC sirvieron para clarificar de manera resumida y ordenada los documentos necesarios para la ejecución de cada actividad. Cada columna "Entrada" contiene documentos que ayudan a que la actividad de inicio apoyado de formatos adoptados de las metodologías seleccionadas por los investigadores y cada columna "Salida" son los productos obtenidos al desarrollar la actividad. Estos datos se visualizan en las tablas Tabla N°24, Tabla N°26, Tabla N°27, Tabla N°29. También se puede visualizar los días utilizados y los responsables en cada evento.

PROPUESTA DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC

A. PROCESO I: Definir Alcance.

En esta parte del proceso los interesados y los responsables de la información y seguridad de la información mantienen reuniones para determinar el alcance de la gestión del riesgo.

Este proceso tiene 1 actividad detallada a continuación:

A.1. Definir Alcance.

El responsable de información (RINFO) previa reunión con la parte interesada solicitó los documentos relevantes de la empresa para conocer su misión, visión, objetivos, roles y funciones además de las políticas generales y políticas por área. Luego de analizar la información el RINFO y el responsable de seguridad (RSEG) realizaron un contraste de información con ayuda de la "Lista de cotejo" que se visualiza en el "Documento de Alcance", el cual es un documento que registra la información fuente para el análisis y selección del alcance, ver Anexo 16. Luego del análisis de los documentos existentes en la organización y reuniones con las partes interesadas se establece a través de juicio de expertos cuales son las prioridades de la organización y se registran formalmente en el "Acta de definición de alcance" que se visualiza en el "Documento de alcance", si todo es conforme, se firma el acta y se entrega el Documento de Alcance a Dirección. Si los documentos entregados no ayudaron con la determinación

del alcance, el RINFO anota los datos en OBSERVACIONES y los notifica a Dirección y a RSEG a través del “Documento de alcance”. Si los resultados no son aceptados regresa a “Definir Alcance” y solicitar nuevamente la información, pero si los resultados son aceptados el proceso termina.

Para esta actividad se estimó una duración de 15 días hábiles. Ver Tabla N°24.

Tabla 24.

MGR_AH: Definir Alcance

Responsable P	**Entrada**	**Proceso**				**Salida**	**Responsable C**
		Actividad	**Descripción**	**Formato**	**Duración**		
Dirección	Lineamientos estratégicos de la empresa. Organigrama. Roles y funciones. Políticas de seguridad de la empresa.	Definir Alcance	Obtiene los requerimientos para identificar las metas de la empresa y metas del área de TI y así definir el alcance de gestión de riesgo.	Documento de Alcance. Ver Anexo 16.	15 días	Registro de Documento de Alcance.	Dirección, RINFO y RSEG

Nota: Elaboración propia.

B. PROCESO II: Evaluación de ciber riesgos

Este proceso tiene como finalidad conocer los riesgos relacionados con el alcance identificado, además gestiona un instrumento que registra los datos de activos, vulnerabilidades, riesgos y sus respuestas para una mejor estimación de los riesgos.

Este proceso presentó 2 actividades descritas a continuación:

A.2. Identificar eventos de riesgo.

Para identificar eventos de riesgos primero se deben conocer los activos, las vulnerabilidades de esos activos y las contramedidas que existen en la organización para proteger la información y de estos deducir los eventos de riesgo a gestionar.

Como primera medida fue importante analizar cómo centralizar todos los datos involucrados en la gestión de riesgos, y al observar la presencia de dos cargos participativos en la gestión (RINFO y RSEG) se consideró manejar una hoja de cálculo de manera compartida. Esa hoja de cálculo se denominó “Instrumento de gestión de riesgos (IGR)”. Ver Anexo 18. Se observó que este instrumento ayudará a la elaboración de resúmenes, búsquedas de datos y cálculos dentro de la implementación del caso de estudio de gestión de riesgos.

Se consideró como primer paso dentro del IGR, la identificación y tipificación de activos, los cuales quedarán registrados en la hoja de cálculo “GESTIÓN CENTRALIZADA”. Según MAGERIT la tipificación de activos se establece asignando un Código, Nombre, Descripción, Responsable, Ubicación, Número y Dependencia. Estos activos son agrupados por categorías para una mejor jerarquización de las dependencias entre activos. Las consideraciones para el paso a paso se puede visualizar en el Manual de uso para identificación, tipificación y registro del inventario de activos de información (Ver anexo 17). Con los datos registrados en esta hoja de cálculo tendremos el “Registro de activos y ciber activos identificados”. Ver figura 19.

Categoría Activ	Código	Nombre	Descripció	Responsabl	Ubicación	Númer	Dependencia
Red de comunicaciones	RC001	Red local	LAN Chiclayo	Responsable de TI	Oficina de Chiclayo	1	Red Privada

a.

	¿El activo se interelaciona entre …								
	… personas?		… software?		… internet?		… intranet/red local?		
Dependencia	SÍ	NO	SÍ2	NO2	SÍ3	NO3	SÍ4	NO4	Tipo de activo
Red Privada	1		1		1		1		Ciber activo

b.

Figura 19. Hoja de cálculo de Gestión centralizada para el Registro de activos y ciber activos identificados a. Parte 1/4, b. Parte 2/4. Fuente: Elaboración propia.

Como segundo paso dentro del IGR se identificó las contramedidas categorizadas en grupos con la finalidad de poder tener un control de la lista de contramedidas que mejor respuesta otorgue al riesgo a identificar. Estas contramedidas se registraron en la hoja “LISTA CONTRAMEDIDAS”. Según MAGERIT una contramedida es un procedimiento o mecanismo tecnológico que reduce el riesgo y lo clasifica de acuerdo al tipo de activo a proteger, también indica que las salvaguardas son cambiantes y es necesario modificar alguna de ellas conforme avanza la tecnología por lo que considera tomar como referencia su “catálogo de salvaguardas” (Libro II - Catálogo de Elementos, 2012). Por tanto, se realizó una selección de contramedidas de acuerdo a características comunes de agrupación como: C1. Protección de daño por recursos naturales, C2. Protección por daño de Error humano, C3. Protección por Identificación y autenticación gestionados incorrectamente, C4. Protección física y C5. Protección lógica. Este criterio de agrupación de contramedidas según mesa de trabajo se marcó con “x” en una matriz del catálogo de MAGERIT y el grupo de contramedidas propuestas. Ver tabla N°25. Finalmente, el “Registro de contramedidas identificadas” se registra en la hoja de cálculo correspondiente del IGR como se ilustra en la figura 20.

Tabla 25.

Matriz de selección de contramedidas

CONTRAMEDIDAS DE MAGERIT	GRUPO CONTRAMEDIDAS PROPUESTAS				
	C1	C2	C3	C4	C5
Protecciones generales u horizontales			X		
Protección de los datos / información			X		
Protección de las claves criptográficas			X		
Protección de los servicios		X			
Protección de las aplicaciones (software)					X
Protección de los equipos (hardware)				X	
Protección de las comunicaciones				x	X
Protección en los puntos de interconexión con otros sistemas				x	X
Protección de los soportes de información					X
Protección de los elementos auxiliares					X
Seguridad física – Protección de las instalaciones				X	
Salvaguardas relativas al personal		X			
Salvaguardas de tipo organizativo		X			
Continuidad de operaciones	X				
Externalización		X			
Adquisición y desarrollo				x	x

Nota: Elaboración propia.

LISTA DE CONTRAMEDIDAS

GRU	Lista de contramedidas	Código
C1	Continuidad de operaciones	RR1

Figura 20. Registro de contramedidas identificadas. Fuente: Elaboración propia.

El tercer paso dentro del IGR fue identificar las vulnerabilidades categorizadas en grupos con la finalidad de poder tener un control de la lista de vulnerabilidades que afectan al activo identificado. Estas vulnerabilidades se registraron en la hoja “LISTA VULNERABILIDADES”. La categorización se basó en características comunes de agrupación a criterio de expertos. Los 5 grupos elegidos fueron: V1. Vulnerabilidad en daño por recursos naturales, V2. Vulnerabilidad por error humano, V3. Vulnerabilidades de Identificación y autenticación, V4. Vulnerabilidades físicas (hardware) y V5.

Vulnerabilidades lógicas (software). Finalmente, el “Registro de vulnerabilidades identificadas” se registra en la hoja de cálculo correspondiente del IGR como se ilustra en la figura 21.

LISTA DE VULNERABILIDADES

ITEM	GRUPO	VULNERABILIDADES	Códi
V1	Vulnerabilidad en daño por recursos naturales	Enfermedades	V0001

Figura 21. Registro de vulnerabilidades identificadas. Fuente: Elaboración propia.

Para esta actividad se estimó una duración de 15 días hábiles.

A.3. Analizar el riesgo.

Para el análisis del riesgo se necesita criterios de valorización de activos, criterios de frecuencia y criterios de impacto que nos permita seleccionar al tipo de activo priorizado para luego identificar los riesgos a los que está expuesto.

Con ayuda de los interesados, se elaboró unas preguntas que ayudarían a la obtención de los criterios para la valorización del activo. Estas interrogantes fueron:

a. Para Disponibilidad: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
b. Para Confidencialidad: ¿qué daño causaría que lo conociera quien no debe?
c. Para Integridad: ¿qué perjuicio causaría que estuviera dañado o corrupto?

Las puntuaciones y descripciones correspondientes se observan en “Criterios de valorización de activos” del Anexo 19.

Luego dentro del IGR se registró estas puntuaciones en las columnas “disponibilidad, integridad y confidencialidad” de la hoja de cálculo

“GESTIÓN CENTRALIZADA”, después se calculó el promedio de estas 3 columnas redondeándose al número entero más próximo y se registró en la columna “puntaje”. Si este puntaje es 4 o 5 entonces el ciber activo se considera “PRIORIZAR”. Ver figura 22.

GESTIÓN CENTRALIZADA 3/4

				Valorizar activos				
Código	Nombre	Descripci	Tipo de activo	Disponibili	Integridad	Confidencialid	puntaje	Priorizar
RC001	Red local	LAN Chiclayo	Ciber activo	5	5	5	5	PRIORIZAR

Figura 22. Valorizar un ciber activo. Fuente: Elaboración propia.

Según TARA un ciber riesgo puede verse afectado por técnicas y procedimientos que vulneran sus principios de seguridad de información a los que denomina “Vectores de ataque”, estos vectores de ataque se pueden obtener de Datos de código abierto sobre patrones de ataque cuyas siglas en ingles es CAPEC, de debilidades de software (CWE), de vulnerabilidades (CVE), de incidentes de seguridad empresarial, de Investigación de seguridad publicada, etc. (Wynn, 2014). Por lo tanto, para conocer los riesgos que afectan a estos ciber activos priorizados se registró el código de la vulnerabilidad en la columna de Grupo de Vulnerabilidades de la hoja de cálculo “GESTIÓN CENTRALIZADA” con el objetivo de elaborar estos vectores de ataque basados en las vulnerabilidades de los activos.

Como primer paso se trabajó una matriz de activo priorizado por vulnerabilidades identificadas. Ver figura 23. Esta matriz se registró en la hoja de cálculo “VECTOR DE ATAQUE”, y se utilizó para combinar el nombre para obtener la definición del vector de ataque que sería el riesgo identificado.

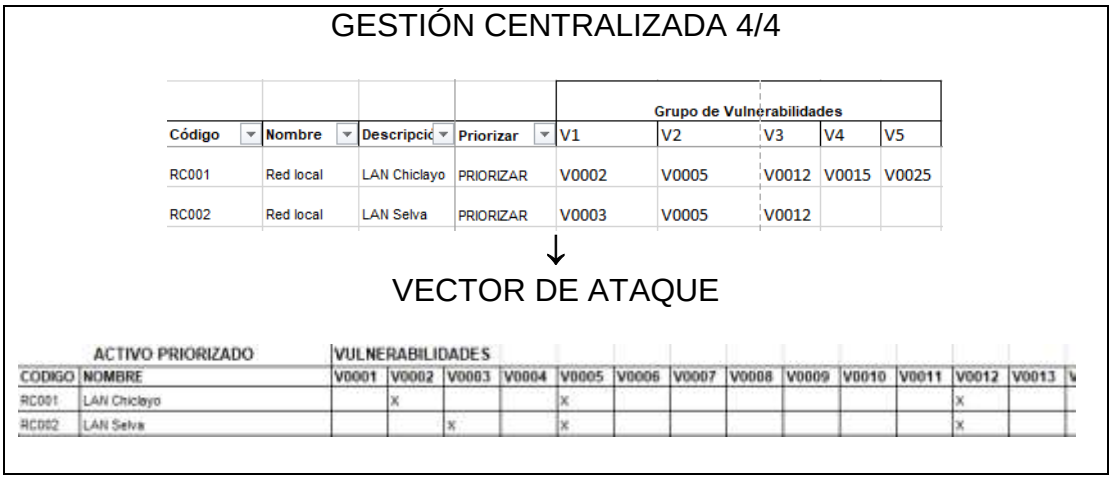


Figura 23. Analizar riesgo. Fuente: Elaboración propia.

Como último paso se registra todos los vectores de ataque con la nomenclatura R y un correlativo de 2 dígitos; por ejemplo, el nombre del riesgo R01: “Incendio en LAN Chiclayo” que resulta de la combinación de la vulnerabilidad “Incendio” y del ciber activo “LAN Chiclayo”. Estos datos se ilustran en la figura 24 y están a cargo del RINFO y RSEG.

VECTOR DE ATAQUE

Código	Código	VECTOR DE ATAQUE		Item de Grupo de vulnerabilidades				
Vulnerbilidad	Activo	Código	Descripción	V1	V2	V3	V4	V5
v002	RC001	R01	Incendio en LAN Chiclayo	X				
V003	RC002	R02	Inundacion en LAN Selva					

Figura 24. Registro de vector de ataque. Fuente: Elaboración propia.

Para esta actividad se estimó una duración de 5 días hábiles y el resumen de este segundo proceso se observa en la tabla N°26.

Tabla 26.

MGR_AH: Evaluación de ciber riesgo.

Responsable P	Entrada	Proceso				Salida	Responsable C
		Actividad	Descripción	Formato	Duración		
RINFO, RSEG	Registro de Documento de Alcance. Listado de activos existentes. Listado de vulnerabilidades existentes (AV). Listado de contramedidas existentes (CM).	Identificar eventos de riesgo	Se analizan los documentos de entrada para iniciar la actividad de identificación de eventos de riesgo. Se ejecuta el instrumento de gestión de riesgos para identificar los nuevos activos, vulnerabilidades y contramedidas.	Manual para registro de inventario de activos. Ver anexo 17. Instrumentos de gestión de riesgos. Ver anexo 18.	15 días	Registro e inventario de activos y ciber activos. Registro e inventario de vulnerabilidades Registro e inventario de contramedidas.	RINFO y RSEG
RINFO, RSEG	Registro e inventario de activos y ciber activos. Registro e inventario de vulnerabilidades.	Analizar riesgo.	Se filtra solo los ciber activos, las vulnerabilidades y las contramedidas relacionadas con el ciberespacio.	Instrumentos de gestión de riesgos. Ver anexo 18. Lista de criterios. Ver anexo 19.	5 días	Registro Vector de ataque.	RINFO y RSEG

Nota: Elaboración propia.

C. PROCESO III: Valoración de ciber riesgos

Este proceso sirve para estimar los riesgos de los activos priorizados en relación a su vector de ataque para valorar el ciber riesgo.

Este proceso presentó 1 actividad:

A.4. Estimar el riesgo.

Con ayuda del Registro del vector de ataque, el RINFO realizó la estimación del riesgo mediante la siguiente fórmula:

$$Riesgo = frecuencia * impacto$$

El cálculo del riesgo se realizó por cada vector de ataque identificado utilizando el mapa de calor de la "Lista de criterios" y se registró en la hoja de cálculo "MATRIZ VULNERABILIDAD" del IGR.

TARA manifiesta que para realizar el proceso de estimación de un riesgo se debe tener un vector de ataque ordenado por Score de riesgo de mayor a menor. Por tal motivo se ordenó esta matriz por valor de riesgo para identificar los riesgos muy altos (color rojo), altos (color gris), medio (color amarillo), bajo (color blanco) y muy bajo (color verde) para un mejor tratamiento del riesgo. Ver figura 25.

Evaluar el riesgo de TTP			Impacto					Vectores de ataque							
			MUY BAJO =1	BAJO =2	MEDIO=3	ALTO =4	MUY ALTO =5	R01	R02	R03	R04	R05	R06	…	R_n
Frecuencia	diaria y/o semanal	MUY ALTO= 5	5A	10B	15C	20D	25E	1A							
	mensual y/o 4 veces al año	ALTO= 4	4A	8B	12C	16D	20E								
	2 veces al año y/o 1 vez al año	MEDIO =3	3A	6B	9C	12D	15E								
	1 vez cada 2 años	BAJO= 2	2A	4B	6C	8D	10E								
	1 vez cada 5 años y/o 1 vez cada 10 años	MUY BAJO= 1	1A	2B	3C	4D	5E								
Score de Riesgo								SR 1	SR 2	…					S R_n

Figura 25. Formato de Matriz de vulnerabilidades. Fuente: *TARA* (2014)

Si al término de esta actividad el RSEG acepta la evaluación del riesgo se continúa con la siguiente actividad "*A.5. Priorizar riesgo*", de lo contrario se regresaría a la actividad "*A.3. Analizar el riesgo*".

Para esta actividad se estimó una duración de 5 días hábiles y el resumen de este tercer proceso se observa en la tabla N°27.

Tabla 27.

MGR_AH: Valoración de ciber riesgos.

Responsable P	Entrada	Proceso				Salida	Responsable C
		Actividad	Descripción	Formato	Duración		
RINFO, RSEG	Registro Vector de ataque.	Estimar riesgo	Se refiere al cálculo del riesgo inherente basado en vulnerabilidades del ciber activo	Formato de Matriz de vulnerabilidades ordenado por Score de riesgo. Lista de criterios.	5 días	Matriz de vulnerabilidad.	RINFO, RSEG

Nota: Elaboración propia.

D. PROCESO IV: Plantear registros de riesgo

En este proceso se planificó los tratamientos a seguir ante la estrategia de selección de riesgo basado en criterio de un coste/ beneficio del marco de referencia de Risk IT.

Este proceso presentó 2 actividades:

A.4. Priorizar respuestas a los riesgos

En esta actividad el RINFO y RSEG eligieron las contramedidas que mejor se ajuste al presupuesto brindado por la empresa para realizar el tratamiento. Según RIST IT la estrategia de selección se debe basar en respuestas a riesgos que consideren criterios de tratamiento por coste- beneficio, como se visualiza en la tabla N°28.

Tabla 28.

Criterios de tratamiento de riesgo

Nivel Riesgo[1]	Tratamiento	Coste- Beneficio[2]
Muy Bajo	Aceptar el riesgo o compartirlo según costo beneficio. (A)	El nivel de riesgo está muy alejado del nivel de tolerancia.
Bajo		
Medio	Mitigar, el riesgo. (M)	El coste del tratamiento es adecuado a los beneficios.
Alto	Compartir o transferir el riesgo (T)	El coste del tratamiento por terceros es más beneficioso que el tratamiento directo.
Muy Alto	Evitar el riesgo (E)	El coste del tratamiento es muy superior a los beneficios.

Nota: 1. Tratamiento de riesgo por niveles según Ruge (2012), 2. Tratamiento de riesgo por coste-beneficio según (Instituto Nacional de Ciberseguridad [INCIBE], 2015)

Para tal fin se elaboró en una hoja de cálculo “PLAN GR” del IGR un registro de estas contramedidas que den respuesta a los riesgos cuidando que los costos de estas medidas no excedan el presupuesto designado por la empresa. Por ejemplo, si el presupuesto designado es de 2000 soles se trataría de gestionar que respuesta al riesgo suma un monto igual o menor al presupuesto. Ver figura 26.

Contramedida (CM)			Efectividad de mitigación (por ID de vector de ataque)		
RR ID	Nombre	Índice Costos	R1	R3	R5
			muy alto	alto	bajo
RR01		50	M		
RR03		800		T	
RR04		1000	M		
RR10		300		A	
	PRESUPUESTO	2000	CANT1	CANT2	CANT3

Figura 26. Registro del PLAN GR. Fuente: (Risk IT Framework, 2nd Edition, 2020)

Tomando los datos de la figura anterior, las posibles estrategias serían:

a. Primera estrategia:

   Contramedidas: RR01, RR03 y RR04

   Costo: 1,850

Tratamiento 2 M, 1 T

Resultado: El coste del tratamiento es adecuado a los beneficios para los R1 en relación a la contramedida RR01 y RR04 y el coste del tratamiento por terceros es más beneficioso que el tratamiento directo para el riesgo R3 en relación a la contramedida RR3.

b. Segunda estrategia:

Contramedidas: RR01, RR04 y RR10

Costo: 1,350

Tratamiento 2 M, 1 A

Resultado: El coste del tratamiento es adecuado a los beneficios para los R1 en relación a la contramedida RR01 y RR04 y el nivel de riesgo está muy alejado del nivel de tolerancia por lo que se acepta el R3 en relación con la contramedida RR10.

Para esta actividad se estimó una duración de 15 días hábiles y el resumen de este tercer proceso se observa en la primera fila de la tabla N°29.

A.5.Comunicar resultado

Esta última actividad de la metodología describió como son los informes presentados a los interesados. Para ello se consideró elaborar un Informe de Plan de tratamiento como hoja Resumen que clarifique todo el análisis de riesgo y la mejor estrategia de selección de tratamiento de riesgos.

Este último proceso de la metodología se detalla en la tabla N°29.

INFORME DE PLAN DE TRATAMIENTO

1- CARACTERIZACION DEL DOCUMENTO			
Número de reunión:		Fecha de reunión:	
Siglas del documento:		Versión:	
Nivel de confidencialidad:			
Preparado por:			
Revisado por:			
Autorizado por:			

2- CONTROL DE VERSIONES			
Versión:	Fecha:	Elaborado por:	Observaciones:

OBJETIVO: Informar de un plan de tratamiento documentos para definir la gestión de riesgos en una organización.

Informe Plan de tratamiento

Activo priorizado	código	nombre	**valor**
Vectores de ataque	Codigo1	nombre	
	Codigo2	Nombre	
Respuesta al riesgo	Codigo1	nombre	Costo
	Codigo2	Nombre	costo
			Costo total

Tratamiento **Estrategia1**

Detalle

Firmas

_____ _____

RINFO Parte interesada

Tabla 29.

MGR_AH: Plantear registros de riesgo

Responsable P	Entrada	Proceso				Salida	Responsable C
		Actividad	**Descripción**	**Formato**	**Duración**		
RINFO, RSEG	Matriz de vulnerabilidad. Registro de contramedidas	Priorizar riesgo	Se refiere a las opciones de selección de respuesta al riesgo: evitarlo, reducirlo, transferirlo o aceptarlo.	Formato de Plan de gestión de riesgo. Lista de criterios.	15 días	Plan de gestión de riesgo.	Dirección y RSEG
Dirección, RINFO y RSEG	Plan de gestión de riesgo.	Comunicar resultado	Bajo una frecuencia establecida por el RINFO se notifica a Dirección el estado de los ítems del Plan Gestión de riesgo.	Sin formato.	Sin duración por ser algo una actividad frecuente.	Correo electrónico notificando el estado del plan.	Dirección, RINFO y RSEG

Nota: Elaboración propia.

Para la validación de la metodología, se procedió con un protocolo de búsqueda de perfiles de experto donde se consideró:

a. El experto puede debe ser de Latinoamérica de lengua castellana.
b. Debe tener un ORCID o pertenecer a la red social Linked In
c. Experiencia relacionada con el SGSI o Gestión de riesgos

De esta búsqueda se seleccionó a 3 expertos cuyos datos se pueden apreciar en el Anexo 19.

En la elaboración del cuestionario se consideró: criterios de claridad, criterio de objetividad, criterio de coherencia, criterio de pertinencia, criterio de suficiencia y criterio de relevancia. Estos criterios tuvieron una puntuación del 1 al 5 en una escala de Likert; donde 1 es muy malo hasta 5 que es muy bueno. Luego se aplicó la técnica DELPHI a los expertos y los valores de cada experto se tabularon en el primer envió del instrumento. Finalmente, la validez del instrumento se realizó teniendo en cuenta el Coeficiente de Validez de Contenido (CVC) de Hérnandez Nieto (2002), cuya fórmula es:

$$CVC_{ic} = CVC_i - p_{ei} = \left[\frac{\sum X_i / J}{Vmx}\right] - (1/J)^J$$

Donde:

CVC_{ic}: Coeficiente de Validez de Contenido por cada ítem corregido

$SX_{i:}$ Promedio de los puntajes asignados por cada juez a cada ítem

J: Número de jueces

Vmx: valor máximo de la escala

$p_{ei:}$ probabilidad de error

Interpretación:

a. CVC_{ic} < 60, validez y concordancia Inaceptables
b. 60 >= CVC_{ic} <=*70,* validez y concordancia deficientes
c. 71> CVC_{ic} <= 80, validez y concordancia aceptables
d. 80> CVC_{ic} <= 90, validez y concordancia buenas
e. CVC_{ic} *>90,* validez y concordancia excelentes

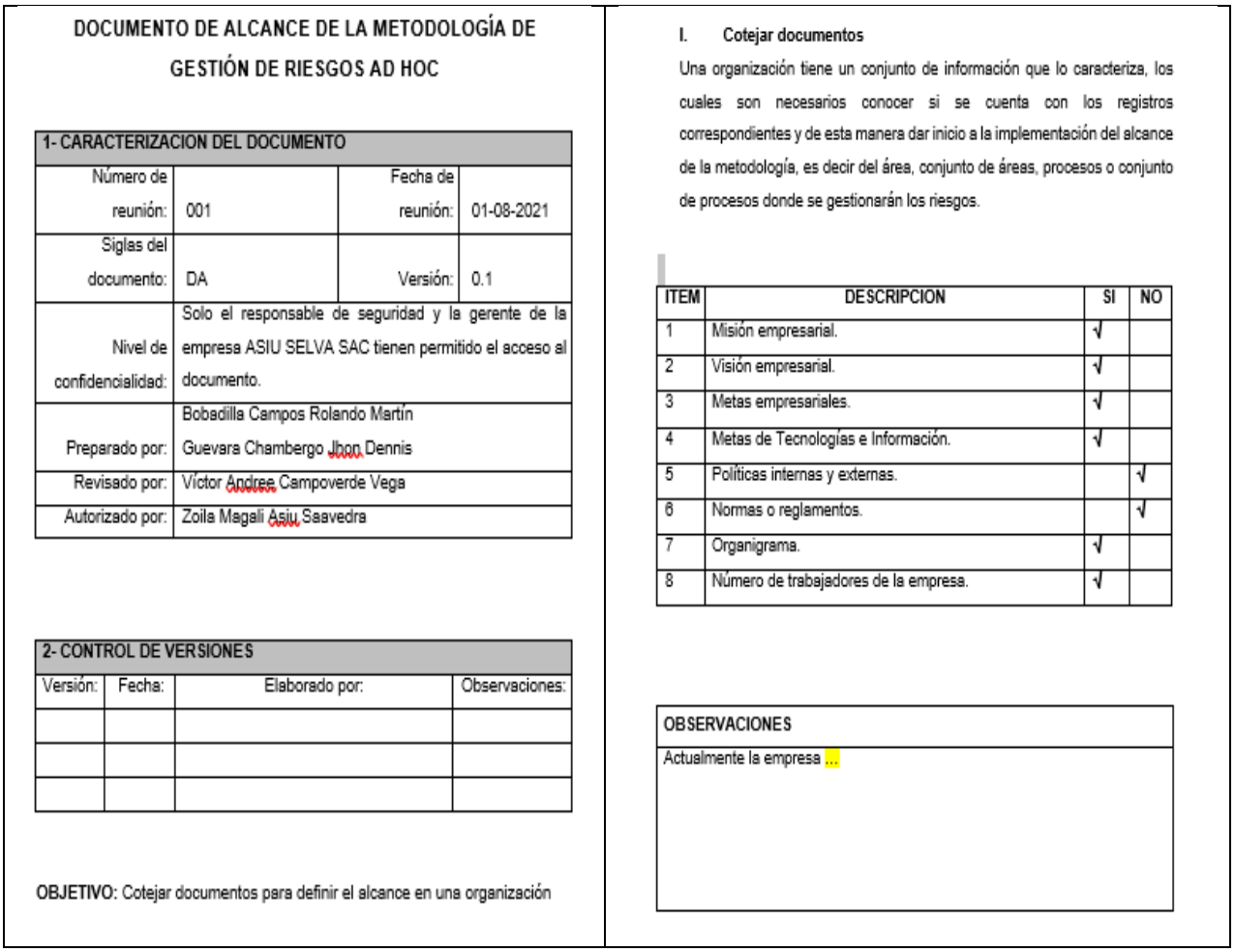
Como respuesta a esta primera ronda de preguntas la puntuación que se obtuvo de los expertos fue de 85.37 y este valor se encontró en el rango “validez y concordancia buenas”. Por tal razón la metodología propuesta es válida y se puede aplicar. La puntuación por cada ítem de acuerdo al criterio evaluado se muestra en el Anexo 3.

IMPLEMENTACIÓN DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC EN LA EMPRESA ASIU SELVA SAC.

A. PROCESO I: Definir Alcance.

A.1. Definir Alcance.

Después de las reuniones con la parte interesada, el RINFO y el RSEG solicitaron documentación sobre la misión, visión, objetivos, roles y funciones, políticas generales y políticas por área a la dirección de la empresa. Luego de que gerencia entregara la documentación solicitada el RINFO apoyado del Documento de Alcance de la metodología MGR_AH observó que la empresa ASIU SELVA SAC no cuenta o no conoce sus políticas ni tampoco tiene algún reglamento de seguridad por escrito. Ver figura 28.



DOCUMENTO DE ALCANCE DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC

1- CARACTERIZACION DEL DOCUMENTO			
Número de reunión:	001	Fecha de reunión:	01-08-2021
Siglas del documento:	DA	Versión:	0.1
Nivel de confidencialidad:	Solo el responsable de seguridad y la gerente de la empresa ASIU SELVA SAC tienen permitido el acceso al documento.		
Preparado por:	Bobadilla Campos Rolando Martín Guevara Chambergo Jhon Dennis		
Revisado por:	Víctor Andree Campoverde Vega		
Autorizado por:	Zoila Magali Asiu Saavedra		

2- CONTROL DE VERSIONES			
Versión:	Fecha:	Elaborado por:	Observaciones:

OBJETIVO: Cotejar documentos para definir el alcance en una organización

I. Cotejar documentos

Una organización tiene un conjunto de información que lo caracteriza, los cuales son necesarios conocer si se cuenta con los registros correspondientes y de esta manera dar inicio a la implementación del alcance de la metodología, es decir del área, conjunto de áreas, procesos o conjunto de procesos donde se gestionarán los riesgos.

ITEM	DESCRIPCION	SI	NO
1	Misión empresarial.	√	
2	Visión empresarial.	√	
3	Metas empresariales.	√	
4	Metas de Tecnologías e Información.	√	
5	Políticas internas y externas.		√
6	Normas o reglamentos.		√
7	Organigrama.	√	
8	Número de trabajadores de la empresa.	√	

OBSERVACIONES
Actualmente la empresa ...

a. b.

Figura 27. Documento de alcance de la metodología MGR_AH a. Hoja 1, b. Hoja 2. Fuente: Elaboración propia.

Por lo que en mesa de trabajo se identificó el proceso relacionado al mantenimiento informático preventivo en la red LAN de Chiclayo involucrado en la atención de los pedidos de sus clientes.

Este primer proceso se implementó en una duración de 21 días hábiles.

B. PROCESO II: Evaluación de ciber riesgos

A.2. Identificar eventos de riesgo.

El RINFO solicitó la lista de activos, la lista de vulnerabilidades y la lista de contramedidas existentes en la empresa para la identificación de activos de

Con el uso compartido del IGR se procedió a identificar los activos del proceso de negocio identificado con ayuda del documento de Alcance. Como la empresa no brindó esta información, el RINFO y el RSEG utilizaron el Manual de registro de inventario de activos para tipificar los activos relacionados con el alcance. El RINFO registró los datos obteniendo el Registro de activos y ciber activos identificados en la hoja de cálculo “GESTIÓN CENTRALIZADA”, obteniendo 27 activos identificados de los cuales 20 fueron considerados como ciber activos.

							¿El activo se interelaciona entre ...								
							... personas?		... software?		... internet?		... intranet/re		
Código	Nombre	Descripció	Responsable	Ubicación	Número	Dependencia	SÍ	NO	SÍ2	NO	SÍ3	NO	SÍ4	NO	Tipo de activo
HW0005	Informática personal	Computadora de gerente y administradores de Sedes.	Gerente General	Todas las sedes	3	Gerente General		1	1			1	1		Activo
RC001	Red local	LAN Chiclayo	Responsable de TI	Oficina de Chiclayo	1	Red Privada	1		1		1		1		Ciber activo
RC002	Red local	LAN Selva	Responsable de TI	Oficina de Selva	1	Red Privada	1		1		1		1		Ciber activo
RC003	Red privada	VPN ASIU	Responsable de TI	Ciberespacio ASIU	2	Servidor Web Servidor	1		1		1		1		Ciber activo
SE001	Internet	Proveedor de servicio de internet CLARO	Responsable de TI	Ciberespacio ASIU	2	Red Local	1		1		1		1		Ciber activo
SW002	Servidor Web	Internet Information Services (IIS)	Responsable de TI	Oficina de TI	1	Informática personal	1		1		1		1		Ciber activo
SW011	Desarrollo a medida	Sistema contable CONCAR	Responsable de TI	Computadora de contabilidad	1	Informática personal	1		1		1		1		Ciber activo
SW010	Servidor de ficheros	File zilla	Responsable de TI	Computadora de responsable de TI	1	Informática personal	1		1		1		1		Ciber activo
SW012	Desarrollo a medida	Sistema automatizado de emsamblado	Responsable de TI	Computadora de operaciones	1	Informática personal	1		1		1		1		Ciber activo
HW0004	Informática personal	Computadora de jefes	Gerente General	Todas las sedes	4	Jefe de seguridad física/		1	1			1	1		Activo

SW001	Base de datos	sql server 2014	Responsable de TI	Oficina de TI	1	Informática personal	1		1		1		1		Ciber activo
SW009	Gestor de máquinas virtuales	VM Ware	Responsable de TI	Computadora de responsable de TI	1	Informática personal	1		1		1		1		Ciber activo
HW0001	Servidor	servidor hp xlion 4 nucleos 5TB	Responsable de TI	Oficina de TI	1	Responsable de TI		1	1			1	1		Activo
HW0002	Servidor	servidor hp xlion 2 núcleos 5TB	Responsable de TI	Oficina de TI	1	Responsable de TI		1	1			1	1		Activo
HW0006	Informática personal	Cámaras de vigilancia	Jefe de seguridad física	Computadora de vigilantes	2	Jefe de seguridad física		1	1			1	1		Activo
SW013	Desarrollo a medida	Software de camara de vigilancia	Jefe de seguridad física	Computadora de vigilantes	2	Informática personal	1		1		1		1		Ciber activo
HW0003	Informática personal	Computadora de operadores	Responsable de TI	Todas las sedes	10	Responsable de TI		1	1			1	1		Activo
SW003	Ofimática	Microsoft Office	Responsable de TI	Computadoras de la organización	17	Informática personal	1		1		1		1		Ciber activo
SW005	Navegador web	Navegadores de internet	Responsable de TI	Computadoras de la organización	17	Informática personal	1		1		1		1		Ciber activo
SW006	Sistema de gestión de base de datos	SQL Management Studio	Responsable de TI	Computadora de responsable de TI	1	Informática personal	1		1		1		1		Ciber activo
SW007	Desarrollo a medida	Herramientas administrativas avanzadas de windows	Responsable de TI	Computadora de responsable de TI	1	Informática personal	1		1		1		1		Ciber activo
SW008	Desarrollo a medida	Visual Studio	Responsable de TI	Computadora de responsable de TI	1	Informática personal	1		1		1		1		Ciber activo
AUX001	Cableado	Cableado estructurado	Responsable de TI	Todas las sedes	2	Responsable de TI		1		1		1	1		Activo
SW004	Desarrollo a medida	Aplicación Zoom	Responsable de TI	Computadoras de la organización	17	Informática personal	1		1		1		1		Ciber activo

SW006	Sistema de gestión de base de datos	SQL Management Studio	Responsable de TI	Computadora de responsable de TI	1	Informática personal	1		1		1		1		Ciber activo
SW007	Desarrollo a medida	Herramientas administrativas avanzadas de windows	Responsable de TI	Computadora de responsable de TI	1	Informática personal	1		1		1		1		Ciber activo
SW008	Desarrollo a medida	Visual Studio	Responsable de TI	Computadora de responsable de TI	1	Informática personal	1		1		1		1		Ciber activo
AUX001	Cableado	Cableado estructurado	Responsable de TI	Todas las sedes	2	Responsable de TI		1		1		1	1		Activo
SW004	Desarrollo a medida	Aplicación Zoom	Responsable de TI	Computadoras de la organización	17	Informática personal	1		1		1		1		Ciber activo
PE001	Gerente General	Representante de la empresa	Gerente General	Oficina de Selva	1		1		1		1		1		Ciber activo
PE002	Responsable de TI	Personal de confianza encargado del area de TI.	Gerente General	Oficina de Selva	1		1		1		1		1		Ciber activo
PE003	Jefe de seguridad física	Responsable de la seguridad física de la empresa	Gerente General	Oficina de Chiclayo/ Oficina de Selva	2		1		1		1		1		Ciber activo

Figura 28. MGR_AH Registro de activos y ciber activos identificados. Fuente: Elaboración propia.

Para la identificación de contramedidas el RINFO se apoyó de la lista de contramedidas propuestas en la hoja de cálculo de "LISTA DE CONTRAMEDIDAS" del IGR. En total se identificaron 19 contramedidas.

GRI	Lista de contramedidas	Código
C1	Continuidad de operaciones	RR1
C2	Externalización	RR5
C2	Protección de los servicios	RR2
C2	Salvaguardas de tipo organizativo	RR4
C2	Salvaguardas relativas al personal	RR3
C3	Protección de las claves criptográficas	RR8
C3	Protección de los datos / información	RR7
C3	Protecciones generales u horizontales	RR6
C4	Adquisición y desarrollo (software)	RR13
C4	Protección de las comunicaciones (software)	RR10
C4	Protección de los equipos (hardware)	RR9
C4	Protección en los puntos de interconexión con otros sistemas (software)	RR11
C4	Seguridad física – Protección de las instalaciones	RR12
C5	Adquisición y desarrollo (hardware)	RR19
C5	Protección de las aplicaciones (software)	RR14
C5	Protección de las comunicaciones (hardware)	RR15
C5	Protección de los elementos auxiliares	RR18
C5	Protección de los soportes de información	RR17
C5	Protección en los puntos de interconexión con otros sistemas (hardware	RR16

Figura 29. MGR_AH Registro contramedidas identificadas. Fuente: Elaboración propia

Para la identificación de vulnerabilidades el RINFO se apoyó de la lista de vulnerabilidades propuestas en la hoja de cálculo de "LISTA DE VULNERABILIDADES" del IGR. En total se identificaron 24 vulnerabilidades.

ITEM	GRUPO	VULNERABILIDADES	Códi
V1	Vulnerabilidad en daño por recursos naturales	Enfermedades	V0001
V1	Vulnerabilidad en daño por recursos naturales	Incendios	V0002
V1	Vulnerabilidad en daño por recursos naturales	Inundación	V0003
V2	Vulnerabilidad por Error humano	Error de usuario	V0004
V2	Vulnerabilidad por Error humano	Error de administrador	V0005
V2	Vulnerabilidad por Error humano	Error de monitorizacion	V0006
V2	Vulnerabilidad por Error humano	Error de configuracion	V0007
V2	Vulnerabilidad por Error humano	Error de mantenimiento	V0008
V2	Vulnerabilidad por Error humano	Deficiencia en la organización	V0009
V3	Vulnerabilidades de Identificación y autenticación	Cambio de contraseña	V0010
V3	Vulnerabilidades de Identificación y autenticación	Contraseña no segura	V0011
V3	Vulnerabilidades de Identificación y autenticación	Acceso no autorizado	V0012
V4	Vulnerabilidades físicas (hardware)	Fallas en la climatizacion de	V0013
V4	Vulnerabilidades físicas (hardware)	Fallos de servicios de comunicaciones	V0014
V4	Vulnerabilidades físicas (hardware)	Interrupcion de suministros escenciales de…	V0015
V4	Vulnerabilidades físicas (hardware)	Vulnerabilidad del equipo	V0016
V4	Vulnerabilidades físicas (hardware)	Actualización del equipo	V0017
V4	Vulnerabilidades físicas (hardware)	Pérdida de equipo	V0018
V5	Vulnerabilidades lógicas (software)	Difusion de software dañino	V0019
V5	Vulnerabilidades lógicas (software)	Destruccion de informacion	V0020
V5	Vulnerabilidades lógicas (software)	Vulnerabilidad del programa	V0021
V5	Vulnerabilidades lógicas (software)	Actualizacion de programas	V0022
V5	Vulnerabilidades lógicas (software)	Caida del sistema por agotamiento de recursos	V0023
V5	Vulnerabilidades lógicas (software)	Manipulacion de los registros	V0024

Figura 30. MGR_AH Registro de vulnerabilidades identificadas. Fuente: Elaboración propia

Finalmente, el RINFO comunicó al RSEG para que valide el análisis. Esta actividad se realizó en 15 días hábiles.

A.3. Analizar el riesgo.

En este proceso el IGR obtuvo registros de los datos de los activos, vulnerabilidades y contramedidas para que el RINFO basado en la Lista de criterios de valoración de activo del Anexo 16 proceda con la valoración del activo y la obtención del ciber activo priorizado. En adición a la valoración del ciber activo priorizado, el RINFO consideró el registro de las vulnerabilidades a la que está expuesto el activo para luego elaborar el vector de ataque que contempla la metodología.

El resultado de este primer análisis se muestra en figura 32.

				Valorizar activos					Grupo de Vulnerabilidades				
Código	Nombre	Descripció	Tipo de activo	Disponibilic	Integridad	Confidencialid	punta	Priorizar	V1	V2	V3	V4	V5
RC001	Red local	LAN Chiclayo	Ciber activo	5	5	5	5	PRIORIZAR	V0002	V0005	V0012	V0015	
RC002	Red local	LAN Selva	Ciber activo	5	5	5	5	PRIORIZAR	V0003	V0005	V0012		
RC003	Red privada	VPN ASIU	Ciber activo	5	5	5	5	PRIORIZAR		V0005, V0007			
SE001	Internet	Proveedor de servicio de internet CLARO	Ciber activo	5	5	5	5	PRIORIZAR		V0014			
SW002	Servidor Web	Internet Information Services (IIS)	Ciber activo	5			5	PRIORIZAR					V0019
SW011	Desarrollo a medida	Sistema contable CONCAR	Ciber activo	5	5	5	5	PRIORIZAR					V0022
SW010	Servidor de ficheros	File zilla	Ciber activo	5	4	4	4	PRIORIZAR					V0019
SW012	Desarrollo a medida	Sistema automatizado de ensamblado	Ciber activo	5	4	4	4	PRIORIZAR		V0007			V0022
SW012	Desarrollo a medida	Sistema automatizado de ensamblado	Ciber activo	5	4	4	4	PRIORIZAR		V0007			V0022
SW001	Base de datos	sql server 2014	Ciber activo	5	4	3	4	PRIORIZAR					V0020
SW009	Gestor de máquinas virtuales	VM Ware	Ciber activo	4	4	4	4	PRIORIZAR					V0023
SW013	Desarrollo a medida	Software de camara de vigilancia	Ciber activo	5	3	3	4	PRIORIZAR			V0012		V0021
PE001	Gerente General	Representante de la empresa	Ciber activo	3	3	5	4	PRIORIZAR	V0001	V0009	V0010		
PE002	Responsable de TI	Personal de confianza encargado del area de TI	Ciber activo	3	3	5	4	PRIORIZAR	V0001	V0009	V0010		

Figura 31. MGR_AH Analizar riesgos. Fuente: Elaboración propia.

Finalmente, el RINFO utilizó la hoja de cálculo “VECTOR DE ATAQUE” para obtener la definición del vector de ataque que fue el nombre del riesgo identificado. Como resultado de la identificación del ciber activo se obtuvo 23 riesgos. Ver figura 33.

Esta actividad demandó 7 días hábiles.

Código Vulnerbilida	Código Activo	VECTOR DE ATAQUE		Item de Grupo de vulnerabilidades				
		Código	Descripción	V1	V2	V3	V4	V5
V0002	RC001	R01	Incendio en LAN Chiclayo	x				
V0003	RC002	R02	Inundacion en LAN Selva	x				
V0021	RC003	R03	Vulnerabilidad del programa en VPN ASIU					x
V0005	RC003	R04	Error de administrador en VPN ASIU		x			
V0005	RC001	R05	Error de administrador en LAN Chiclayo		x			
V0005	RC002	R06	Error de administrador en LAN Selva		x			
V0007	SW0012	R07	Error de configuración del Sistema automatizado de emsamblado		x			
V0001	PE001	R08	Enfermedad del representante de la empresa	x				
V0001	PE002	R09	Enfermedad del personal de confianza encargado del area de TI.	x				
V0009	PE001	R10	Deficiencia en la organización del representante de la empresa		x			
V0009	PE002	R11	Deficiencia en la organización del personal de confianza encargado del area de TI.		x			
V0012	RC001	R12	Acceso no autorizado en LAN Chiclayo			x		
V0012	RC002	R13	Acceso no autorizado en LAN Selva			x		
V0012	SW0013	R14	Acceso no autorizado al software de cámara de vigilancia			x		
V0014	SE0001	R15	Fallos de servicios de comunicaciones del proveedor de servicio de internet CLARO				x	
V0015	RC001	R16	Interrupción de suministros escenciales de LAN Chiclayo				x	
V0019	SW0002	R17	Difusión de software dañino en el Internet Information Services (IIS)					x
V0019	SW0010	R18	Difusión de software dañino en el File zilla					x
V0020	SW0001	R19	Destrucción de información de sql server 2014					x
V0021	SW0013	R20	Vulnerabilidad del programa de software de cámara de vigilancia					x
V0022	SW0011	R21	Actualización de programas del Sistema contable CONCAR					x
V0022	SW0012	R22	Actualización de programas del Sistema automatizado de emsamblado					x
V0023	SW0009	R23	Caída del sistema por agotamiento de recursos del VM Ware					x

Figura 32. MGR_AH Registro de vector de ataque. Fuente: Elaboración propia.

C. PROCESO III: Valoración de ciber riesgos

A.4. Estimar el riesgo.

El RINFO realizó la estimación del riesgo mediante la siguiente fórmula:

$$Riesgo = frecuencia * impacto$$

Evaluar el riesgo de TTP			Impacto			
			MUY BAJO=1	BAJO=2	MEDIO=3	ALTO=4
Frecuencia	diaria y/o semanal	MUY ALTO=5	5A	10B	15C	20D
	mensual y/o 4 veces al año	ALTO=4	4A	8B	12C	16D
	2 veces al año y/o 1 vez al año	MEDIO=3	3A	6B	9C	12D
	1 vez cada 2 años	BAJO=2	2A	4B	6C	8D
	1 vez cada 5 años y/o 1 vez cada 1	MUY BAJO=1	1A	2B	3C	4D
						Score d

a.

Vectores de ataque													
R5	R6	R7	R8	R9	R10	R11	R12	R13	R14	R15	R16	R17	R
12D	12C	15E	4A	9C	15E	15E	15E	15E	15E	15E	20E	8D	

b.

Figura 33. MGR_AH Matriz de vulnerabilidades, a. Parte 1; b. Parte 2. Fuente: *TARA* (2014).

Luego el RINFO ordenó la matriz de vulnerabilidad por valor de riesgo. Este reordenamiento de la matriz se visualiza en la figura 30. El visto bueno de este proceso por el RSEG demandó un total de 7 días hábiles.

Evaluar el riesgo de TTP			Impacto												
			MUY BAJO=1	BAJO=2	MEDIO=3	ALTO=4	MUY ALTO=5	R16	R5	R6	R7	R10	R11
Frecuencia	diaria y/o	MUY ALTO=5	5A	10B	15C	20D	25E	20E	12D	12C	15E	15E	15E
	mensual	ALTO=4	4A	8B	12C	16D	20E						
	2 veces al	MEDIO=3	3A	6B	9C	12D	15E						
	1 vez cada	BAJO=2	2A	4B	6C	8D	10E						
	1 vez cada	MUY BAJO=1	1A	2B	3C	4D	5E						
					Score deRiesgo								

a.

Vectores de ataque															
R12	R13	R14	R15	R18	R22	R17	R20	R21	R23	R8	R9	R19	R1	R2	R3	R4
15E	15E	15E	15E	15E	12C	8D	6B	4A	10E	4A	9C	5E	1A	2A	1A	1A

b.

Figura 34. MGR_AH Formato de Matriz de vulnerabilidades ordenada por Score de riesgo, a. Parte1; b. Parte 2. Fuente: *TARA* (2014).

D. PROCESO IV: Plantear registros de riesgo

A.4. Priorizar respuestas a los riesgos

En esta parte del proceso el RSEG determina con RINFO la mejor estrategia de respuesta al riesgo procurando de que esta estrategia no exceda el presupuesto que la empresa ha designado para la gestión de los riesgos.

El RSEG estableció como estrategia lo siguiente:

1. Seleccionar los riesgos valorados como “Muy alto” y “Alto”.

Contramedida (CM)			Efectividad de mitigación (por ID de vector de ataque)												
RR ID	Nombre	Índice Costos	R16	R5	R6	R7	R10	R11	R12	R13	R14	R14	R15	R18	R22
			Muy Alt	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto	Alto
RR01	Continuidad de operaciones	S/500.00					M	M							
RR05	Externalización	S/1,000.00	M	E	E	E									
RR02	Protección de los servicios	S/1,000.00					E	E	E	E					
RR04	Salvaguardas de tipo organizativo	S/800.00					E	E	E	E					
RR03	Salvaguardas relativas al personal	S/900.00					M	M							
RR08	Protección de las claves criptográficas	S/50.00							A	A		A			
RR07	Protección de los datos / información	S/100.00							A	A		A		M	
RR06	Protecciones generales u horizontales	S/100.00							A	A		A			
RR09	Protección de los equipos (hardware)	S/1,000.00	M	M	M	M							T		
RR12	Seguridad física – Protección de las instalaciones	S/1,000.00	M												M
RR19	Adquisición y desarrollo (hardware)	S/3,000.00	E	E	E	E									
RR15	Protección de las comunicaciones (hardware)	S/1,500.00											E		
RR18	Protección de los elementos auxiliares	S/300.00	A												
RR16	Protección en los puntos de interconexión con otros sistemas (hardware)	S/500.00													
RR13	Adquisición y desarrollo (software)	S/3,000.00													
RR10	Protección de las comunicaciones (software)	S/1,500.00				E								E	E
RR11	Protección en los puntos de interconexión con otros sistemas (software)	S/1,500.00												E	
RR14	Protección de las aplicaciones (software)	S/1,500.00													M
RR17	Protección de los soportes de información	S/1,500.00	M											M	

Figura 35. MGR_AH Plan de Gestión de Riesgos. Fuente: *TARA* (2014)

2. Elegir los tratamientos Mitigables por Coste-Beneficio de acuerdo a los criterios de tratamiento de riesgos de la MGR_AH.

Contramedida (CM)			Efectividad de mitigación (por ID de ve				
RR ID	Nombre	Costos	R16	R10	R11	R18	R22
			Muy Alto	Alto	Alto	Alto	Alto
RR14	Protección de las aplicaciones (software)	S/1,500.00					M
RR17	Protección de los soportes de información	S/1,500.00	M			M	
RR05	Externalización	S/1,000.00	M				
RR09	Protección de los equipos (hardware)	S/1,000.00	M				
RR12	Seguridad física – Protección de las instalaciones	S/1,000.00	M				M
RR03	Salvaguardas relativas al personal	S/900.00		M	M		
RR01	Continuidad de operaciones	S/500.00		M	M		
RR07	Protección de los datos / información	S/100.00				M	
	primera estrategia	S/7,500.00	4	2	2	2	2

Figura 36. MGR_AH Formato de Plan de Gestión de Riesgos. Fuente: *TARA* (2014)

3. Priorizar 2 contramedidas por ataque vector. Ante un presupuesto asignado de s/.3,000.00 para atención a la gestión de riesgos.

Contramedida (CM)			Efectividad de mitigación (por ID de ve				
RR ID	Nombre	Costos	R16	R10	R11	R18	R22
			Muy Alto	Alto	Alto	Alto	Alto
RR17	Protección de los soportes de información	S/1,500.00	M			M	
RR05	Externalización	S/1,000.00	M				
	primera estrategia	S/2,500.00	2	0	0	1	0

Figura 37. Plan de Gestión de Riesgos. Fuente: *TARA* (2014)

Contramedida: RR17 Protección de los soportes de información
RR05 Seguridad física – Protección de las instalaciones

Costo: s/.2,500.00

Tratamiento: El coste del tratamiento es adecuado a los beneficios para los riesgos R16 porque satisface la estrategia elegida.

La implementación de este proceso demandó del RINFO y del RSEG de 8 días hábiles.

A.5.Comunicar resultado

La implementación de esta última actividad es que mediante un correo el RSEG programe reuniones con la Dirección para informar el PLAN DE GESTIÓN DE RIESGOS.

INFORME DE PLAN DE TRATAMIENTO

1- CARACTERIZACIÓN DEL DOCUMENTO			
Número de reunión:	01	Fecha de reunión:	01-01-2022
Siglas del documento:	IPL	Versión:	0.1
Nivel de confidencialidad:	Sólo el responsable de seguridad y la gerente de la empresa ASIU SELVA SAC tienen permitido el acceso al documento.		
Preparado por:	Bobadilla Campos Rolando Martín Guevara Chambergo Jhon Dennis		
Revisado por:	Víctor Andree Campoverde Vega		
Autorizado por:	Zoila Magali Asiu Saavedra		

2- CONTROL DE VERSIONES			
Versión:	Fecha:	Elaborado por:	Observaciones:

OBJETIVO: Informar de un plan de tratamiento documentos para definir la gestión de riesgos en una organización.

a.

Informe Plan de tratamiento

Activo priorizado	RC001	LAN Chiclayo	**Muy alto**
Vectores de ataque	R16	Interrupción de suministros esenciales de LAN Chiclayo	
Respuesta al riesgo	RR17	Protección de los soportes de información	S/1,500.00
	RR05	Seguridad física – Protección de las instalaciones	S/1,000.00
			S/2,500.00

Tratamiento El coste del tratamiento es adecuado a los beneficios para la interrupción de suministros esenciales de LAN Chiclayo en relación a la contramedida RR17 y RR05.

RINFO

Parte interesada

b.

Figura 38. MGR_AH Informe del Plan de Gestión de Riesgos, a. Hoja 1; b. Hoja 2. Fuente: Elaboración propia

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones.

1. La búsqueda de la bibliografía con una lista de cadenas de búsqueda con base en palabras claves relacionadas con la estándares y metodologías internacionales en base de datos reconocidas en el área de ciencias de la computación como IEEExplore y ACM Digital Library; ayudó a seleccionar artículos científicos que nos permitió listar estándares y modelos justificando su selección y no selección para la propuesta de la metodología. Estos estándares y modelos fueron: ISO/IEC 27005, MAGERIT, TARA y RISK IT.

2. Conocer a la empresa permitió describir a la empresa e identificar el proceso donde se aplicó la gestión de riesgo. Para el caso de la empresa manufacturera ASIU SELVA SAC fue necesario implementar una ficha de contextualización de la empresa que adjunta una guía rápida de Metas empresariales y Metas de alineamiento de TI ya que uno de los procesos de la metodología fue adoptados del marco de referencia RISK IT. Este Framework manifiesta que los objetivos de TI deben estar alineados a los objetivos empresariales.

3. Diseñar la metodología de gestión de riesgos Ad Hoc (MGR_AH) permitió determinar los procesos generales de cada estándar y método internacional que adoptó 4 procesos de la norma internacional ISO/IEC 27005, 1 de la metodología MAGERIT, 1 de la metodología TARA, 2 del Framework RISK IT que representa un 13% como promedio de cumplimiento de la metodología de gestión con los estándares y un 8% con las metodologías y Framework de la muestra.

4. La selección de expertos con perfiles relacionados con el SGSI o Gestión de riesgos y la elaboración de un cuestionario para aplicar la técnica DELPHI permitió tabular las respuestas obteniendo un resultado del… que se considera…para la propuesta de nuestra metodología MGR_AH para la empresa ASIU SELVA SAC.

5. La aplicación de la metodología MGR_AH en un caso de uso registró un total de 27 activos de los cuales 13 se consideraron ciber activos priorizados. También se 4 riesgos críticos de los 23 riesgos identificados; pero por estrategia del responsable de información (RINFO) y del responsable de seguridad (RSEG) se eligieron 3 controles para la mitigación de un riesgo crítico por ser evaluado a través del criterio Costo/beneficio.

6. La utilización de un instrumento de Gestión de riesgos (IGR) como una hoja de cálculo ayudó a realizar los procesos de manera más eficiente para la manipulación de los datos.

4.2. Recomendaciones.

1. Para la búsqueda de la bibliografía se recomienda utilizar una combinación de 2 palabras clave para la formación de las cadenas de búsqueda como, por ejemplo: management risk, risk cyber, risk framework, risk management, risk methodologies, risk security, risk standards y cyber riskcon.

2. Se recomienda automatizar la hoja de cálculo del Instrumento IGR de manera integral a toda la empresa.

3. Se sugiere seguir en la línea de investigación sobre las bondades de evaluar el riesgo basado en vulnerabilidades a través de vectores de ataque de TARA o de otros modelos que involucren esta característica en sus procesos.

REFERENCIAS.

Carnero Garay, D. F., Carbajal Ramos, M. A., Armas Aguirre, J., & Madrid Molina, J. M. (2020). Information security risk management model for mitigating the impact on SMEs in Peru. *15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1-7.

Eling, M., McShane, M., & Nguyen, T. (2021). Cyber risk management: History and futureresearch directions. *Risk Management and Insurance Review, 24*, 93-125.

ENISA. (2007). *The European Union Agency for Cybersecurity*.

Falco, G., Eling, M., Jablanski, D., Weber, M., Miller, V., Gordon, L. A., . . . Lin, H. (2019). Cyber risk research impeded by disciplinary barriers. *Science, 366*, 1066-1069.

Ganin, A., Quach, P., Panwar, M., Collier, Z., Keisler, J., Marchese, D., & Linkov, I. (2017). Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management. *U.S. Government work*, 1-17.

Hernandez Ardieta, J. L., Blanco, P., & Vara, D. (2012). A methodology to construct Common Criteria security targets through formal risk analysis. *RECSI 2012*.

Hérnandez Nieto, R. (2002). *Contributions to Statistical Analysis: The Coefficients of Proportional Variance, Content Validity and Kappa.* Mérida: Universidad de los Andes.

Hiscox. (2021). *Cyber Readiness Report 2021 Don't let cyber be a game of chance.*

Houmb, S. (2007). Decision Support for Choice of Security Solution: The Aspect-Oriented Risk Driven Development (AORDD) Framework. *PhD thesis, Norwegian University of Science and Technology, Trondheim,*.

Instituto Nacional de Ciberseguridad [INCIBE]. (2015). Gestión de riesgos. Una guía de aproximación para el empresario. 1-25.

International Organization for Standardization. (2009). Gestión de Riesgos. Principios y directrices. *ISO 31000:2009*.

International Organization for Standardization. (2011). Information technology — Security techniques — Information security risk management. *ISO/IEC 27005:2011*.

International Organization for Standardization. (2013). Information technology — Security techniques — Information security management systems — Requirements. *ISO/IEC 27001:2013*.

International Organization for Standardization. (2018). Gestión del riesgo — Directrices. *ISO 31000:2018(es)*.

Ionita, D., Hartel, P., Pieters, W., & Wieringa, R. (2013). Established Risk Assessment Methodologies and Tools.

ISACA. (2009). *The Risk IT Practitioner Guide.* Rolling Meadows.

ISACA. (2019). *Marco de referencia COBIT® 2019: Introducción y metodología.* © 2018 ISACA.

ISACA. (2019). *Marco de Referencia COBIT® 2019: Objetivos de gobierno y gestión.* © 2018 ISACA.

ISACA. (2020). *Risk IT Framework, 2nd Edition.* Schaumburg, USA.

ISACA. (2020). Risk IT Practitioner Guide, 2nd Edition.

Krumay, B., Bernroider, E., & Walser, R. (2018). Evaluation of Cybersecurity Management Controls and Metrics of Critical Infrastructures: A Literature Review Considering the NIST Cybersecurity Framework.

Ministerio de Hacienda y Administraciones Públicas. (2012). Libro I - Método, MAGERIT – versión 3.0. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.*, 1-127.

Ministerio de Hacienda y Administraciones Públicas. (2012). Libro II - Catálogo de Elementos. *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.*, 1-75.

Ministerio de Hacienda y Administraciones Públicas. (2012). Libro III - Guía de Técnicas. *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.*, 1-42.

Mukhopadhyay, A., Chatterjee, S., Bagchi, K., Kirs, P., & Shukla, G. K. (2017). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance.

Nagaraju, V., Fiondella, L., & Wandji, T. (2017). A Survey of Fault and Attack Tree Modeling and Analysis for Cyber Risk Management. *IEEE*, 1-6.

NIST SP 800-30. (2002). *Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información.*

Papastergiou, S., & Polemi, N. (2017). MITIGATE: A Dynamic Supply Chain Cyber Risk Assessment Methodology.

Rea Guaman, M., Calvo Manzano, J. A., & San Feliu, T. (2018). Prototipo para Gestionar la Ciberseguridad en Pequeñas Empresas. *13th Iberian Conferen ce on Information Systems and Technologies (CISTI 2018)*, 680-685.

Real Academia Española. (2014). *Diccionario de la lengua española.*

Ruge Pinzon, J. N. (2012). *Metodología para identificación y valoración de riesgos y salvaguardas en una mesa de ayuda tecnológica.* Universidad Piloto de Colombia, Colombia.

Sayyed G, M. (2020). UAE Cybersecurity Perception and Risk Assessments Compared to Other Developed Nations. *3rd International Conference on Information and Computer Technologies (ICICT), 1*, 432-439.

Shetty, S., McShanea, M., Zhangb, L., Kesanb, J. P., Kamhouac, C. A., Kwiatc, K., & Njillac, L. L. (2018). Reducing Informational Disadvantages to Improve Cyber Risk Management. *The Geneva Papers on Risk and Insurance - Issues and Practice, 43*(224-238).

Svilicic, B., Kamahara, J., Rooks, M., & Yano, Y. (2019). Maritime Cyber Risk Management: An Experimental Ship Assessment. *The Journal of Navigation*, 1-13.

Tran, T. D., Thiriet, J.-M., Marchand, N., El Mrabti, A., & Luculli, G. (2019). Methodology for risk management related to cyber-security of Unmanned Aircraft Systems. *IEEE*, 695-702.

World Economic Forum. (2021). *The Global Risks Report 2021* (16 th ed.). World Economic Forum®.

Wynn, J. (01 de Octubre de 2014). Threat Assessment and Remediation Analysis (TARA). (M. Corporation, Ed.)

Wynn, J., Whitmore, J., Upton, G., Spriggs, L., McKinnon, D., McInnes, R., . . . Clausen, L. (octubre de 2011). Threat Assessment & Remediation Analysis (TARA) Methodology Description Version 1.0. (MITRE, Ed.)

Zambon, E., Etalle, S., Wieringa, R. J., & Hartel, P. (2011). Model-based quali- tative risk assessment for availability of it infrastructures. *Software & Systems Modeling, 10*, 553–580.

ANEXOS.

Anexo 1. Resolución de aprobación del proyecto de investigación.

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N° 0700-2021/FIAU-USS
Pimentel, 02 de Agosto de 2021

VISTO:
Las Actas de reunión N° 2306 – 2021, N° 1307 - 2021 y la N° 1507 - 2021 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida el 15 de Julio de 2021 mediante oficio N°0250-2021/FIAU-IS-USS de la Dirección de Escuela de INGENIERÍA DE SISTEMAS, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y *tesis* son *aprobados por el Comité de Investigación* y derivados a la Facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El *periodo de vigencia de los mismos será de dos años*, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; *es individual o en pares para obtener un título profesional*. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C.".

Que, según documentos de Vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerda aprobar los temas de las Tesis a cargo de los egresados que se detallan en el anexo de la presente Resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR, los **Temas de Tesis** perteneciente a la línea de investigación de **INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE**, a cargo de los **alumnos y egresados** del Programa de estudios de **INGENIERÍA DE SISTEMAS,** según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: ESTABLECER, que la inscripción de los Temas de Tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Dr. Mario Fernando Ramos Moscol
Decano - Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Mag. Luis Roberto Larrea Colchado
Secretario Académico (e)
Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.

Cc: Interesado, Archivo

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N° 0700-2021/FIAU-USS
Pimentel, 02 de Agosto de 2021

INGENIERÍA DE SISTEMAS	VILCHEZ SILVA OMAR JHONATHAN	ANÁLISIS COMPARATIVO DE ALGORITMO DEVITERBI Y BAM-WELCH DE RECONOCIMIENTO DE VOZ PARA LA IDENTIFICACIÓN DE PERSONAS	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	FERNANDEZ SALDAÑA CARLOS ALDAIR	DESARROLLO DE UN MÉTODO DE CLASIFICACIÓN AUTOMÁTICA DE CITRUS AURANTIFOLIA USANDO PROCESAMIENTO DIGITAL DE IMÁGENES	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
	IDROGO CORNEJO LEONCIO		
INGENIERÍA DE SISTEMAS	SUCLUPE CHAPOÑAN MANUELA DEL ROSARIO	EVALUACIÓN DE LA CALIDAD DE UN SISTEMA DE INFORMACIÓN LOGÍSTICA DE CONTROL DEL PROCESO DE ALMACENAMIENTO DE UNA CONSTRUCTORA DE LA SELVA PERUANA	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	PISFIL JAUREGUI JOSE LAURENT	IMPLEMENTACIÓN DE MICROSERVICIOS PARA MEJORAR LA INTEROPERABILIDAD DEL PROCESO DE CONSULTAS DE ARBITRIOS TRIBUTARIOS EN MUNICIPALIDADES	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	CHIMPEN SERQUEN MERLINA JESSICA	DISEÑO DE UNA MESA DE AYUDA BASADO EN ITIL V3 Y BPM PARA EL AREA DE TI DE UNA MUNICIPALIDAD PROVINCIAL DE LAMBAYEQUE	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	CIEZA CELIS JESUS ABELARDO	EVALUACIÓN DEL DESEMPEÑO DE PROTOCOLOS DE SEGURIDAD DE REDES PARA COMBATIR VULNERABILIDADES EN REDES INALÁMBRICAS WI-FI	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
	OJEDA ROMERO ANTHONNY JHONATAN		
INGENIERÍA DE SISTEMAS	FERNANDEZ RIOJA JUAN NICANOR	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN BASADO EN ITIL PARA MEJORAR LAS ATENCIONES DE INCIDENCIAS DE TI EN UNA MUNICIPALIDAD DISTRITAL DE LA REGIÓN LAMBAYEQUE	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
	RIOJA MESIA CHARLES SEGUNDO		
INGENIERÍA DE SISTEMAS	TEMOCHE GÓMEZ LENNIN BILLEY	MÉTODO PARA DETECTAR CON EFICIENCIA LOS ATAQUES CROSS-SITE SCRIPTING UTILIZANDO TÉCNICAS DE APRENDIZAJE AUTOMÁTICO	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	BOBADILLA CAMPOS ROLANDO MARTÍN	IMPLEMENTACIÓN DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN ESTÁNDARES INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
	GUEVARA CHAMBERGO JHON DENNIS		
INGENIERÍA DE SISTEMAS	CALDERON YNOÑAN PAMELA DEL CARMEN	DESARROLLO DE UN MÉTODO BAJO EL ENFOQUE ÁGIL Y DISEÑO CENTRADO EN USUARIO (DCU) PARA LA MEJORA DE EXPERIENCIA DE USUARIO (UX)	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
	PRIETO NEIRA FRANCK ALBERSON		
INGENIERÍA DE SISTEMAS	CASTRO MEDINA MIGUEL ANGEL	IMPLEMENTACIÓN DE UN MODELO AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA EDITORA DE DIARIO REGIONAL PERUANO	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE

Anexo 2. Carta de aceptación de la empresa para la recolección de datos.

ASIU SELVA

20604209316-ASIU SELVA S.A.C.

JR. TRUJILLO NRO. 726A P.J. SAN ANTONIO LORETO - MAYNAS – IQUITOS
074-524001 – www.grupoasiu.com

"Año del Bicentenario del Perú: 200 años de Independencia"

Chiclayo, 05 de julio del 2021

Sr.

Mg. Víctor Alexci Tuesta Monteza

Director Académico de Escuela Profesional de Ingeniería de Sistemas de la Universidad Señor de Sipán.

Asunto:

Aceptación para realizar proyecto de investigación.

Tengo el agrado de dirigirme a usted para manifestarle nuestro cordial saludo y a la vez, en atención al documento sobre la recolección de información de nuestra empresa a los alumnos **GUEVARA CHAMBERGO JHON DENNIS** con código universitario **2161803368**, e identificado con DNI **45635122**, **BODADILLA CAMPOS ROLANDO MARTÍN** con código universitario **2131811278**, e identificado con DNI **70356823**, ambos estudiantes del IX ciclo de la escuela profesional de ingeniería de sistemas, doy a conocer a usted que a los alumnos antes mencionado se les acepta recojan información en nuestra empresa a fin que cumplan con su proyecto de investigación titulado **"Implementación de una metodología de gestión de riesgos ad hoc basada en estándares internacionales y buenas prácticas para una empresa manufacturera peruana"** . Se expide la presente a solicitud de los interesados, para los fines que crean conveniente.

Sin otro particular, me suscribo de usted no sin antes expresarle la muestra de mi consideración y estima personal.

ASIU SELVA S.A.C.
Zoila Magali Asiu Saavedra
GERENTE

Anexo 3. Instrumento de recolección de datos con su respectiva validación.

INFORME DE OPINIÓN DE EXPERTO

El presente informe proyecto tiene como objetivo principal someter a evaluación la Metodología de Gestión de Riesgos Ad Hoc (MGR_AH) basada en estándares internacionales como ISO/IEC 27005 apoyadas en metodologías de MAGERIT y TARA y marco de referencia internacional como RISK IT cuya finalidad es comprobar los criterios de claridad, objetividad, coherencia, pertinencia, suficiencia y relevancia de los ítems considerados.

1. **Datos del Experto**

DATOS GENERALES DEL EXPERTO	
Nombres y apellidos:	
Grado académico y profesión:	
Áreas de experiencia laboral:	
Empresa donde labora:	
Tiempo de experiencia:	

2. **Criterios de validación**

CRITERIOS DE VALIDACIÓN DEL MODELO		
Indicador	**Criterio**	**Valoración**
OBJETIVIDAD	El contenido presentado es objetivo y concreto, y está expresado en conductas observables y medibles.	Rango del 1 al 5 donde: 1=Muy Malo 2=Malo 3=Medio 4=Bueno 5=Muy Bueno
CLARIDAD	El contenido se presenta utilizando un lenguaje apropiado que facilita su entendimiento.	
SUFICIENCIA	El contenido presenta un conjunto de actividades que facilitan su aplicación.	
COHERENCIA	Existe correspondencia lógica entre el contenido presentado y la teoría.	
PERTINENCIA	El contenido se mantiene acorde con la dimensión expuesta, no está fuera de lugar.	
RELEVANCIA	El contenido presentado es importante y determinante para lograr el entendimiento del tema.	

3. **Ficha de Evaluación**

Instrucciones: Asigne una valoración del 1 al 5 que corresponda para cada criterio en cada actividad de acuerdo al cuadro de valoración presentado en el ítem anterior y finalmente conteste la pregunta.

FASE	Actividad	Puntaje asignado por Experto 1						Observaciones
		Objetividad	Claridad	Suficiencia	Coherencia	Pertinencia	Relevancia	
PROCESO I. Definir Alcance.	Definir Alcance							
PROCESO II. Evaluación de ciber riesgo.	Identificar eventos de riesgo							
	Analizar riesgo							
PROCESO III. Valoración de ciber riesgo.	Estimar riesgo							
PROCESO IV. Plantear registros de riesgo	Priorizar respuestas a los riesgos							
	Comunicar resultado							

Pregunta: ¿Considera Ud. que el número de procesos y el nombre es apropiado en contexto con lo presentado en el contenido?

Sí, porque….

No, porque… Sugerencia.

VALIDACIÓN DE INSTRUMENTO

1. Criterio de evaluación de experto por Ítem

ITEMS	Puntuación experto 1							Puntuación experto 2							Puntuación experto 3						
	Objetividad	Claridad	Suficiencia	Coherencia	Pertinencia	Relevancia	**Experto1**	Objetividad	Claridad	Suficiencia	Coherencia	Pertinencia	Relevancia	**Experto2**	Objetividad	Claridad	Suficiencia	Coherencia	Pertinencia	Relevancia	**Experto3**
Definir alcance	4	4	4	4	4	4	**24**	5	5	5	5	5	5	**30**	4	5	4	4	4	4	**25**
Identificar eventos de riesgo	4	4	4	4	4	4	**24**	5	5	5	5	5	5	**30**	5	5	5	5	5	4	**29**
Analizar riesgo	4	4	4	4	4	4	**24**	5	5	5	5	5	5	**30**	5	5	5	5	5	5	**30**
Estimar riesgo	4	4	4	4	4	4	**24**	5	5	5	5	4	4	**28**	5	5	4	5	5	4	**28**
Priorizar respuestas a los riesgos	4	3	4	3	4	4	**22**	5	5	5	5	4	4	**28**	5	5	4	4	5	4	**27**
Comunicar resultado	4	3	4	3	4	4	**22**	5	5	5	5	5	5	**30**	5	4	4	5	4	4	**26**

2. Aplicación de la fórmula Coeficiente de Validez de Contenido (CVC) de (Hérnandez Nieto, 2002)

$$CVC_{ic} = CVC_i - p_{ei} = \left[\frac{\sum X_i / J}{Vmx}\right] - (1/J)^J$$

Donde:

CVC_{ic}: Coeficiente de Validez de Contenido por cada ítem corregido

$SX_{i:}$ Promedio de los puntajes asignados por cada juez a cada ítem

J: Número de jueces

Vmx: valor máximo de la escala

$p_{ei:}$ probabilidad de error

Ítem	Experto 1	Experto 2	Experto 3	∑Xi	(∑Xi)/J	CVCi	Pei	CVCic	Interpretación CVCic
Definir alcance	24.00	30.00	25.00	79.00	26.33	0.88	0.04	0.84	validez y concordancia buenas
Identificar eventos de riesgo	24.00	30.00	29.00	83.00	2.77	0.92	0.04	0.89	validez y concordancia buenas
Analizar riesgo	24.00	30.00	30.00	84.00	2.8	0.93	0.04	0.9	validez y concordancia buenas
Estimar riesgo	24.00	28.00	28.00	80.00	2.67	0.89	0.04	0.85	validez y concordancia buenas
Priorizar respuestas a los riesgos	22.00	28.00	27.00	77.00	2.57	0.86	0.04	0.82	validez y concordancia buenas
Comunicar resultado	22.00	30.00	26.00	78.00	2.6	0.87	0.04	0.83	validez y concordancia buenas

3. Observaciones de evaluación de experto por Ítem

ITEMS	Observación Experto 1	Observación Experto 2	Observación Experto 3
Definir alcance			En base a la experiencia laboral, más aún el trabajar en una entidad financiera la cual es supervisada por la SBS (super intendencia de banca y seguros), es recomendable agregar un proceso que permita realizar el seguimiento y monitoreo post implementación de planes de acción, a manera de mejora continua, informar resultados y retro alimentación. Otro proceso que también se viene aplicando en la empresa y nos ayuda mucho es el análisis de impacto BIA, nos ayudó mucho en el inventario de los procesos principales de la empresa, sus sistemas e infraestructura que los soporta, del cual decantaron riesgos a tratar. Queda claro que lo enunciado está en base al contenido recepcionado, quizás en el detalle del proyecto los puntos que he mencionado si los tienen contemplados bajo otros criterios.
Identificar eventos de riesgo			
Analizar riesgo			
Estimar riesgo		¿Cómo influye TARA en esta sección?	
Priorizar respuestas a los riesgos	Si la gestión es todo, ¿Por qué en la última fase recién se genera un Plan de Gestión? Creo que debería llamarse Tratamiento de riesgo, igual el proceso, ya que se llama “Plantear registro de riesgo” pero el registro ya se realiza en las actividades del Proceso II.	¿Cómo influye RISK IT en esta sección?	
Comunicar resultado			

Anexo 4. Envío de correo con Informe de opinión de experto

12/11/21 10:11 Correo de UNIVERSIDAD SENOR DE SIPAN - Validación de Metodología

UNIVERSIDAD SEÑOR DE SIPÁN

Jhon Guevara Chambergo <gchambergojhond@crece.uss.edu.pe>

Validación de Metodología

Jhon Guevara Chambergo <gchambergojhond@crece.uss.edu.pe> 12 de noviembre de 2021, 10:10
Para: JUNIOR EUGENIO CACHAY MACO <cmacojunio@crece.uss.edu.pe>
Cco: ROLANDO MARTIN BOBADILLA CAMPOS <bcamposrolandom@crece.uss.edu.pe>

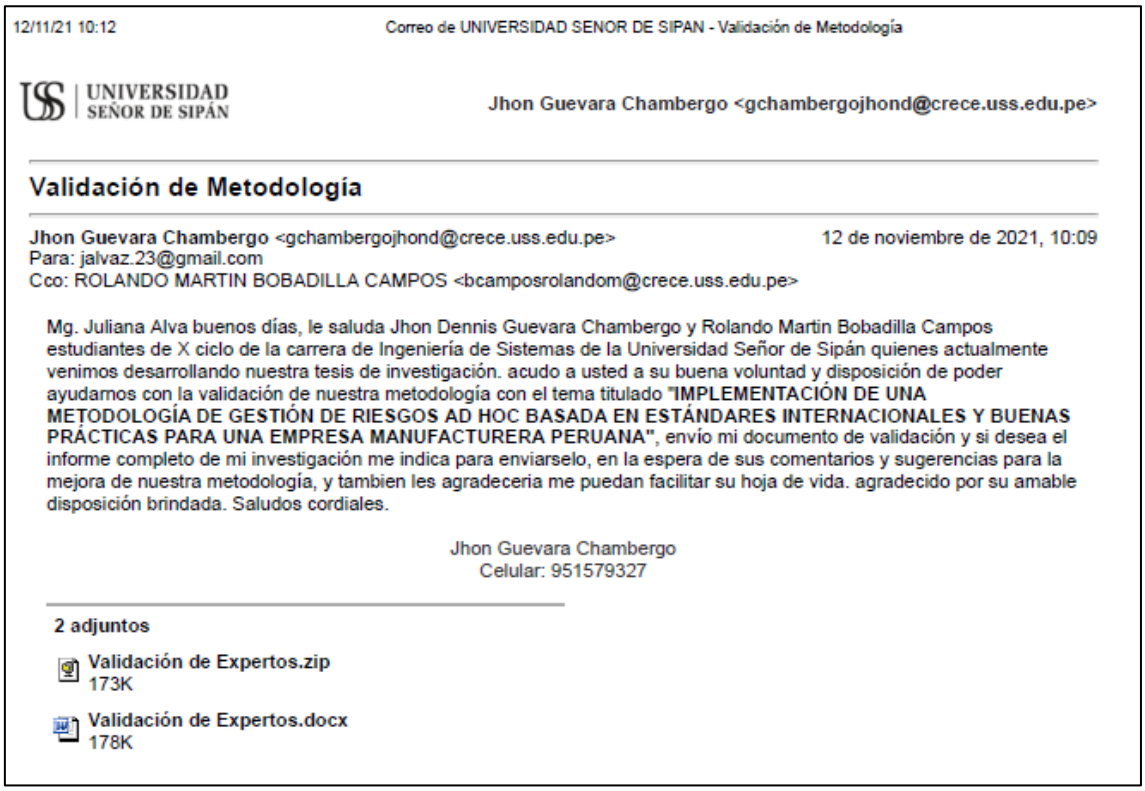
Ing. Junior Cachay buenos días, le saluda Jhon Dennis Guevara Chambergo y Rolando Martin Bobadilla Campos estudiantes de X ciclo de la carrera de Ingeniería de Sistemas de la Universidad Señor de Sipán quienes actualmente venimos desarrollando nuestra tesis de investigación. acudo a usted a su buena voluntad y disposición de poder ayudarnos con la validación de nuestra metodología con el tema titulado "**IMPLEMENTACIÓN DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN ESTÁNDARES INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA**", envío mi documento de validación y si desea el informe completo de mi investigación me indica para enviarselo, en la espera de sus comentarios y sugerencias para la mejora de nuestra metodología, y tambien le agradeceria me puedan facilitar su hoja de vida. agradecido por su amable disposición brindada.
Saludos cordiales.

Jhon Guevara Chambergo
Celular: 951579327

2 adjuntos

Validación de Expertos.docx
178K

Validación de Expertos.zip
173K



12/11/21 10:12 Correo de UNIVERSIDAD SENOR DE SIPAN - Validación de Metodología

UNIVERSIDAD SEÑOR DE SIPÁN

Jhon Guevara Chambergo <gchambergojhond@crece.uss.edu.pe>

Validación de Metodología

Jhon Guevara Chambergo <gchambergojhond@crece.uss.edu.pe> 12 de noviembre de 2021, 10:09
Para: jalvaz.23@gmail.com
Cco: ROLANDO MARTIN BOBADILLA CAMPOS <bcamposrolandom@crece.uss.edu.pe>

Mg. Juliana Alva buenos días, le saluda Jhon Dennis Guevara Chambergo y Rolando Martin Bobadilla Campos estudiantes de X ciclo de la carrera de Ingeniería de Sistemas de la Universidad Señor de Sipán quienes actualmente venimos desarrollando nuestra tesis de investigación. acudo a usted a su buena voluntad y disposición de poder ayudarnos con la validación de nuestra metodología con el tema titulado "**IMPLEMENTACIÓN DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN ESTÁNDARES INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA**", envío mi documento de validación y si desea el informe completo de mi investigación me indica para enviarselo, en la espera de sus comentarios y sugerencias para la mejora de nuestra metodología, y tambien les agradeceria me puedan facilitar su hoja de vida. agradecido por su amable disposición brindada. Saludos cordiales.

Jhon Guevara Chambergo
Celular: 951579327

2 adjuntos

Validación de Expertos.zip
173K

Validación de Expertos.docx
178K

UNIVERSIDAD SEÑOR DE SIPÁN

Jhon Guevara Chambergo <gchambergojhond@crece.uss.edu.pe>

Validación de Metodología

Jhon Guevara Chambergo <gchambergojhond@crece.uss.edu.pe> 12 de noviembre de 2021, 10:06
Para: guillermobarbozat@gmail.com
Cco: ROLANDO MARTIN BOBADILLA CAMPOS <bcamposrolandom@crece.uss.edu.pe>

Ing. Guillermo Barboza buenos días, le saluda Jhon Dennis Guevara Chambergo y Rolando Martin Bobadilla Campos estudiantes de X ciclo de la carrera de Ingeniería de Sistemas de la Universidad Señor de Sipán quienes actualmente venimos desarrollando nuestra tesis de investigación. acudo a usted a su buena voluntad y disposición de poder ayudarnos con la validación de nuestra metodología con el tema titulado "**IMPLEMENTACIÓN DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN ESTÁNDARES INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA**", envío mi documento de validación y si desea el informe completo de mi investigación me indica para enviarselo, en la espera de sus comentarios y sugerencias para la mejora de nuestra metodología, y tambien les agradeceria me puedan facilitar su hoja de vida. agradecido por su amable disposición brindada. Saludos cordiales.

Jhon Guevara Chambergo
Celular: 951579327

2 adjuntos

Validación de Expertos.docx
178K

Validación de Expertos.zip
173K

Anexo 5. Curriculum de Expertos.

JUNIOR EUGENIO CACHAY MACO

Calle Los Filántropos 188 Urb Latina – José Leonardo Ortiz
Celular: 978777026
E-mail: jcachay@audit.pe

Como fundador de audit, mi misión se enfoca en empoderar a las empresas con estrategias de Gobierno, Riesgo y Cumplimiento en Tecnologías de la Información.

DATOS PERSONALES

APELLIDOS Y NOMBRES
Cachay Maco Junior Eugenio

FECHA DE NACIMIENTO
27/04/1987

DNI
44404838

NRO. RUC ACTIVO
10444048382

Nº COLEGIATURA VIGENTE
179375

MEMBRESÍAS

ISACA ID
974787

IDIOMAS

ESPAÑOL ●●●●●
INGLÉS ●●●●●

CONTACTOS

CELULAR
978777026

EMAIL
jcachay@audit.pe

SITIO WEB
http://www.audit.pe/

ISACA

FORMACIÓN ACADÉMICA

MAESTRÍA	Universidad Nacional Pedro Ruiz Gallo	Maestro Maestro en Ingeniería de Sistemas con Mención en Gerencia de Tecnologías de Información y Gestión del Software. 2017
TÍTULO UNIVERSITARIO	Universidad Nacional Pedro Ruiz Gallo	Ingeniero Ingeniería en Computación e Informática 2015
BACHILLER	Universidad Nacional Pedro Ruiz Gallo	Bachiller Ingeniería en Computación e Informática 2009

PROYECTOS

MUNICIPALIDAD PROVINCIAL DE CHICLAYO	Asesoría en investigación sobre implementación de metodologías de gestión de riesgos basado en ISO 27005.	Realizado en Diciembre 2020
MUNICIPALIDAD DISTRITAL DE LA VICTORIA	Asesoría en investigación sobre implementación de gobierno corporativo basado en el marco COBIT 2019.	Realizado en Diciembre 2020
SIEMPRESOFT EIRL	Implementación y obtención de la Certificación Internacional de la Norma ISO 27001:2013.	Realizado en Diciembre 2019.

EXPERIENCIA LABORAL

AUDIT AND CONTROL OF INFORMATION SYSTEMS SAC	Cargo Gerente general	Del 22/06/2018 hasta la actualidad, Chiclayo - Perú
SIEMPRESOFT	Jefe de seguridad de la información	Del 05/06/2017 al 30/03/2018, Chiclayo - Perú
SIEMPRESOFT	Jefe de Producción	Del 05/01/2015 al 30/03/2016, Chiclayo - Perú
SIEMPRESOFT	Jefe de Proyectos de Software	Del 02/01/2013 al 30/01/2015, Chiclayo - Perú
SIEMPRESOFT	Analista Programador	Del 15/03/2010 al 31/12/2012, Chiclayo - Perú
SUNARP	Operador Informático	Del 15/01/2009 al 15/01/2010, Chachapoyas - Perú

DOCENCIA

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	Catedrático de Postgrado	Septiembre/2019, Lambayeque-Perú
UNIVERSIDAD SEÑOR DE SIPÁN	Docente Catedrático a tiempo parcial	De 19/05/2018 hasta la actualidad, Chiclayo-Perú
CENTRO DE ENTRENAMIENTO EN TECNOLOGIAS DE INFORMACIÓN	Docente Especialista a tiempo parcial	De 2016 hasta el 2019

CAPACITACIONES

CURSO DE FUNDAMENTOS COBIT 2019	Institución ISACA	Abril 2020.

DOMINIOS DE TECNOLOGÍAS

MARCOS DE TRABAJO O ESTÁNDARES INTERNACIONALES	COBIT, ISO 27001, ISO 9001, VAL IT, RISK IT e ITIL.
PLATAFORMAS SAAS	Microsoft Azure.
LENGUAJES DE PROGRAMACIÓN	VB, C# en Visual Studio .Net, PHP, 4GL, Powershell, Android y Swi-Prolog.
HERRAMIENTAS DE GESTIÓN	Trello (Kanban online), Team Foundation Server y Asana.
BASES DE DATOS	SQL Server, MySQL y MongoDB.

Contactar

jalvaz@outlook.com

www.linkedin.com/in/juliana-alva-zapata-5aa491bb (LinkedIn)

Aptitudes principales

Administración y dirección de empresas

Gestión de proyectos

SQL

Languages

Inglés (Professional Working)

Certifications

ISO/IEC 27001:2013 FOUNDATIO

Scrum Foundation Professional Certificate

JULIANA ALVA ZAPATA

Catedrático universitario en UNTRM

Perú

Extracto

Ing. En computación e informática, Mg. En gestión estratégica de tecnologías de la información, con experiencia en desarrollo de sistemas, gestión de proyectos y riesgos, en empresas del rubro financiero y comercial.

Experiencia

UNIVERSIDAD TORIBIO RODRIGUEZ DE MENDOZA
Catedrático universitario
mayo de 2020 - Present (1 año 2 meses)
Chachapoyas, Amazonas, Perú

Caja Rural de Ahorro y Crédito Sipan S.A.C.
Analista de riesgos
mayo de 2018 - abril de 2019 (1 año)
Chiclayo

Financiera Efectiva S.A
Analista programador
abril de 2010 - marzo de 2018 (8 años)

Sunarp Oficial
Practicas en Archivo Registral
febrero de 2009 - febrero de 2010 (1 año 1 mes)
Chiclayo

Educación

Universidad Católica Santo Toribio de Mogrovejo
maestría en gestión estratégica de TI, Ingeniería de sistemas · (2015 - 2017)

Universidad Nacional Pedro Ruiz Gallo
Grado en Ingeniería, Computación e informática · (2003 - 2008)

Lambayeque – Perú Fco. Cuneo 570 Dpto. 503 – Urb. Patasca Distrito Chiclayo Fecha Nacimiento: 15-Abril-1978 DNI: 16800588	Teléfono Particular Casa : (511) 074 224419 Teléfono Móvil : (511) 947651082 RPM : #947651082 guillermobarbozat@gmail.com

ANTONIO GUILLERMO BARBOZA TENORIO

Perfil

Profesional con habilidades para la coordinación, análisis y gestión de Requerimientos y/o proyectos de TI, aptitud para el manejo de relaciones interpersonales y equipos de trabajo, proactivo y responsable.
Con 6 años de experiencia en el sector retail y más de 10 años en el sector financiero (micro financiero-consumo). Experiencia en Gestión de Proyectos de desarrollo de Software, desde la hoja de nacimiento hasta el cierre del mismo, liderando equipos de trabajo multidisciplinarios.
Experiencia en la toma de requisitos, relevamiento, reuniones con usuarios, análisis funcional, análisis técnico y diseño de prototipos, plataformas Web, Escritorio, Microsoft.net, informix.

Objetivo

Afrontar nuevos retos, aportando mis conocimientos en pro de crecimiento personal y de la empresa.
Trabajar en una empresa de prestigio

Experiencia Profesional

Febrero 2019 a la Fecha.

Financiera Efectiva S.A. - Grupo Efe

Jefe de Integración y Migración.

Proyectos de Participación:

- **Proyecto Nuevo Core Bantotal.**
  Proyecto que comprende reemplazar el core de la financiera SFI Sistema Integrado Financiero por el nuevo core BANTOTAL
  Encargado de:
  - Migración de la información de los diferentes módulos del core vigente hacia el nuevo core.
  - Integración de los diferentes sistemas satélites vigentes con el nuevo core, entre ellos está el Sistema de Evaluación de Líneas de Crédito, SAP, BI, ICS (cobranzas), entes recaudadores como Banco de la Nación, BCP, Scotiabank, etc.

Personal a Cargo: 4 Analistas desarrolladores internos, y 4 Analistas externos.

Plataforma: 4gl, Informix, Ge Nexus, DB2, Microsoft.net

Enero 2018 a Enero 2019

Financiera Efectiva S.A. - Grupo Efe

Analista Funcional Senior.

Proyectos de Participación:

- **Proyecto CrediFED Financiera Efectiva Digital**
  Proyecto que comprende reemplazar la plataforma de evaluaciones de línea de crédito con una suite adquirida a IBM que contiene:
  - BPM, aloja el workflow del proceso de evaluación de líneas de crédito.
  - BUS Integrador, herramienta que administra los diferentes servicios web con las que se conectaran los diferentes clientes con el BPM
  - ODM Motor de Reglas, herramienta donde se administran las diferentes reglas del negocio sobre las que fluye el proceso de evaluación de líneas de crédito.

- **Proyecto CotiFED – Financiera Efectiva Digital**
  Proyecto que compre en la implementación de una herramienta que permite pre-evaluar clientes y realizarles cotizaciones, integrado con el módulo de campañas de la financiera

Enero 2016 a Diciembre 2017

Financiera Efectiva S.A. - Grupo Efe

Jefe Gestión de Demanda.

Gestión de Proyectos y/o requerimientos bajo la metodología PMI, adaptada a la financiera.
Responsable de la atención, seguimiento y monitoreo de los requisitos de las diferentes áreas que constituyen a la financiera, tanto del proceso del negocio como de los procesos back office

Personal a Cargo: 3 Analistas funcionales

Proyectos de Participación:

- **Motor de Reglas IBM (C&D):**
  Proyecto que comprende extraer las reglas del negocio y plasmarlas en un software que administre las reglas, el objetivo principal es que los usuarios administren sus reglas y que en lo futuro si se adquiere un nuevo core financiero, simplemente se integre al motor
  Este proyecto está en proceso de Implementación.

  Plataforma:
  Java Enterprise, base de datos Netezza, Microsoft.net

- **Proyecto Nuevo Módulo Hipotecario – Netbank.**
  Sistema que administra la evaluación y generación de créditos Hipotecarios, mediante un workflow parametrizable
  Este proyecto está en proceso de Implementación.

  Plataforma:
  4gl, Php, Microsoft.net, base de datos Informix.

- Mantenimiento y Mejoras del core financiera SFI (sistema financiero integrado)

  Plataforma:
  4gl, base de datos Informix.

Enero 2010 a diciembre 2015

Financiera Efectiva S.A. - Grupo Efe

Jefe de Proyectos.

Asignado a la gestión de Proyectos y/o requerimientos requeridos por el área de riesgos de la financiera, esto incluye:

- Riesgo Financiero
- Riesgo Crediticio
- Riesgo Operacional
- Riesgo Analítico y Sistematización

Implementación de los diferentes modelos de evaluación crediticia, conectándose con Boreu Externos (Equifax, Xchange, DataCredito-Expirian) obteniendo información del sistema financiero
Implementar la conexión de servicios web desde aplicativo Core Financiero SFI con herramienta de programación 4gl y .net

Personal a Cargo: 4 Analistas Programadores Internos, 5 programadores externos.

Proyectos Asignados

- **Proyecto Motor de Reglas Interno (MDI).**
  Desarrollo Inhouse, comprende extraer las reglas del negocio y plasmarlas en un parametrizador administrable, el objetivo principal es que el área de riesgos realice cambios de reglas y modelos desde el mismos parametrizador
  Estructuras los aplicativos que participan en el proceso de evaluación crediticia y soporten la conexión con el motor interno.

  Plataforma:
  .net. 4gl, base de datos Informix, Servicios Web C#

Proyectos de Participación:

- **Proyecto Barlovento – Absorción Empresa La Curacao.**
  Preparar el core financiero SFI para que administre el proceso de Originación de líneas de créditos y generación de créditos de clientes provenientes del Retail La Curacao, migración de información y unificación de agenda.
  Iteración entre software comercial de La Curacao "Genesis" con el core financiero SFI vía servicios web, para la lectura de la línea de crédito y generación de desembolsos.

  Plataforma:
  4gl, base de datos Informix, Servicios Web C#

- **Proyecto Gestión de Agenda de Cobranza.**
  Desarrollo Inhouse del Modelo de Gestión de Cobranza, comprende lógica para la asignación de agenda de cuentas a los administradores de cartera, gestión de registro de la gestión, migraciones, etc.

  Plataforma:
  4gl, base de datos Informix.

Marzo 2005 a diciembre 2009
Financiera Efectiva S.A. - Grupo Efe
Analista Programador.
Asignado a la implementación de requerimientos requeridos por las diferentes áreas de la empresa Retail Tiendas Efe, realizando adecuaciones y mejoras al ERP SAI Sistema Administrativo Integrado, enfocando más la demanda hacia la atención del flujo de Ventas, Logística e Inventarios.

Plataforma:
4gl, base de datos Informix.

Octubre 2004 a Febrero 2005
Clínica del Pacífico SA – Chiclayo
Asistente Administrativo

Enero 2003 a Junio 2003
Grifo Grand Prix Clínica del Pacífico SA – Chiclayo
Asistente Logístico

Educación

Universidad Particular Santo Toribio de Mogrovejo USAT
Maestría en Ingeniería de Sistemas y Computación con Mención en Dirección Estratégica de TI
2017 – 2020

Universidad Particular Santo Toribio de Mogrovejo USAT
Ingles Intermedio – Modalidad Virtual.
Julio 2020 a Febrero 2021.

Universidad Nacional Pedro Ruiz Gallo
Facultad de Ciencias Física y Matemáticas
Bachiller en Ingeniería Computación e Informática
1996 – 2002

Universidad Nacional Pedro Ruiz Gallo
Curso de Titulación – Grado de Ing. en Computación
Facultad de Ciencias Física y Matemáticas
Septiembre 2004 – Marzo 2005

Instituto Cultura Peruano Norte Americano IPCNA
Ingles Intermedio
Junio 2001 – Mayo 2002

Colegio Nacional San José
Primaria: 1984 - 1989
Secundaria: 1990 – 1994

ASIU SELVA

20604209316-ASIU SELVA S.A.C.

JR. TRUJILLO NRO. 726A P.J. SAN ANTONIO LORETO - MAYNAS – IQUITOS

074-524001 – www.grupoasiu.com

ASIU SELVA S.A.C.
Zoila Magali Asiu Saavedra

Anexo 6. Mapa de procesos de ASIU SELVA SAC.

Anexo 7. Lineamientos empresariales de ASIU SELVA SAC.

ASIU SELVA

20604209316-ASIU SELVA S.A.C.

JR. TRUJILLO NRO. 726A P.J. SAN ANTONIO LORETO - MAYNAS – IQUITOS
074-524001 – www.gruposiu.com

MISIÓN:

Satisfacer todas las necesidades de nuestros clientes en el menor tiempo posible combinando experiencia, tecnología y eficacia.

VISIÓN:

Situamos en el mercado como la empresa número 1 en servicios de transformación, producción y ensamblaje de motocicletas, trimotos de pasajeros y de carga en todo el Perú.

VALORES EMPRESARIALES:

ÉTICA: Actuar con honestidad, rectitud y transparencia demostrando integridad.

COMPROMISO: Responder a las necesidades de los clientes en forma incondicional y satisfacerlas. "Al elegirnos, el cliente se convierte en el jefe de la empresa."

RESPETO A LAS PERSONAS: En nuestro grupo queremos crear un entorno que permita a los trabajadores desarrollar sus capacidades, su creatividad con una adecuada motivación para beneficio de nosotros y de nuestros clientes.

ACTITUD DE SERVICIO: Demostrar responsabilidad e interés por los requerimientos del cliente.

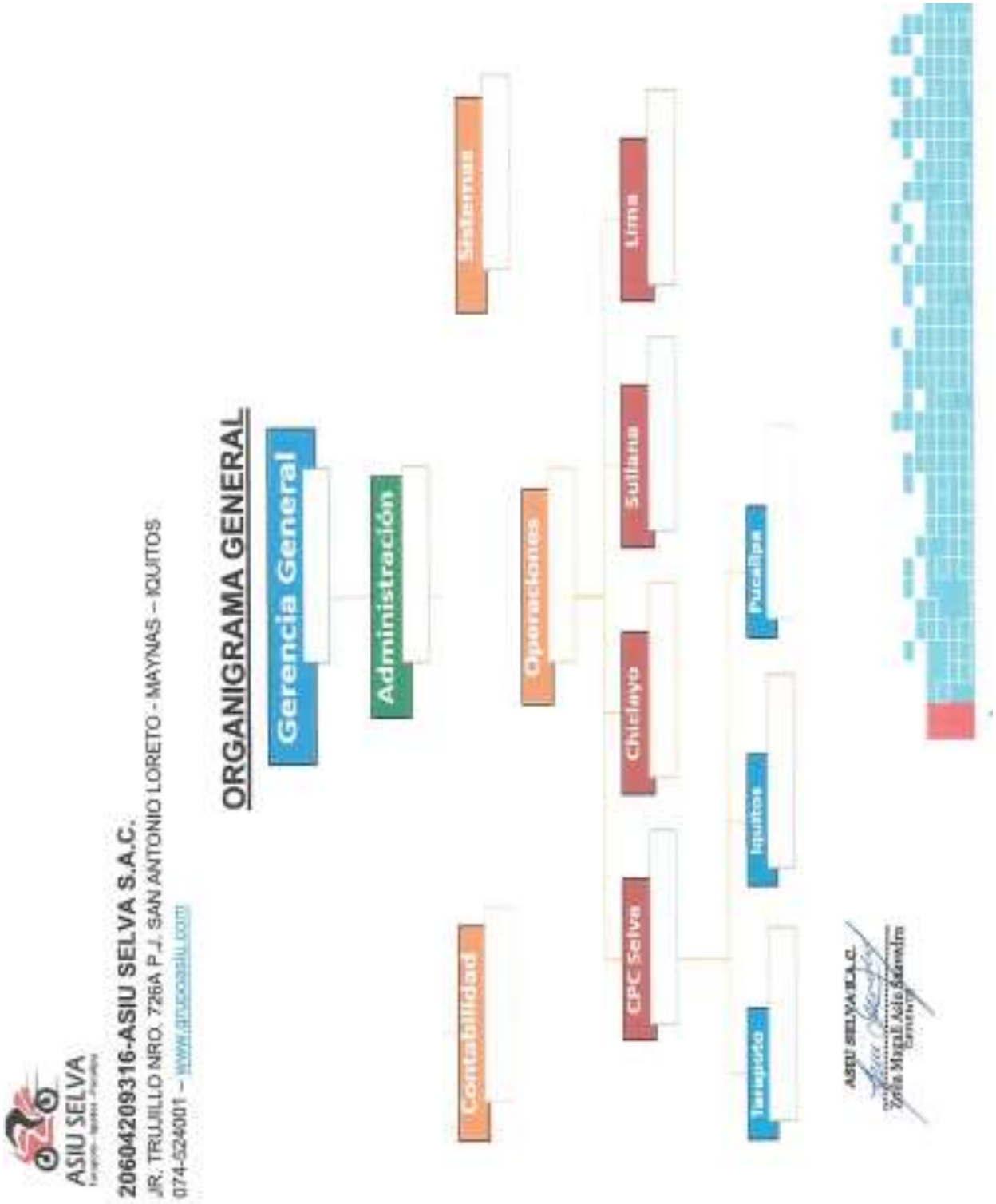
PROFESIONALISMO: Ser competente y eficiente en el desempeño de las diferentes actividades.

RESPONSABILIDAD SOCIAL: Ser consciente de la realidad del país y comprometido con el desarrollo nacional.

PROACTIVIDAD: Actuar con oportunidad e iniciativa en busca de mejores resultados.

ASIU SELVA S.A.C.
Zoila Magali Asiu Saavedra

Anexo 8. Organigrama general de ASIU SELVA



.

Anexo 9. Imágenes de la empresa ASIU SELVA SAC

Equipo de huella dactilar

Router

Servidor

Lap top de administrativos

PC del personal

Cámara de seguridad

Archivos

Encargado del Área de Sistema, Víctor Andree Campoverde Vega

Anexo 10. Combinaciones de palabras claves.

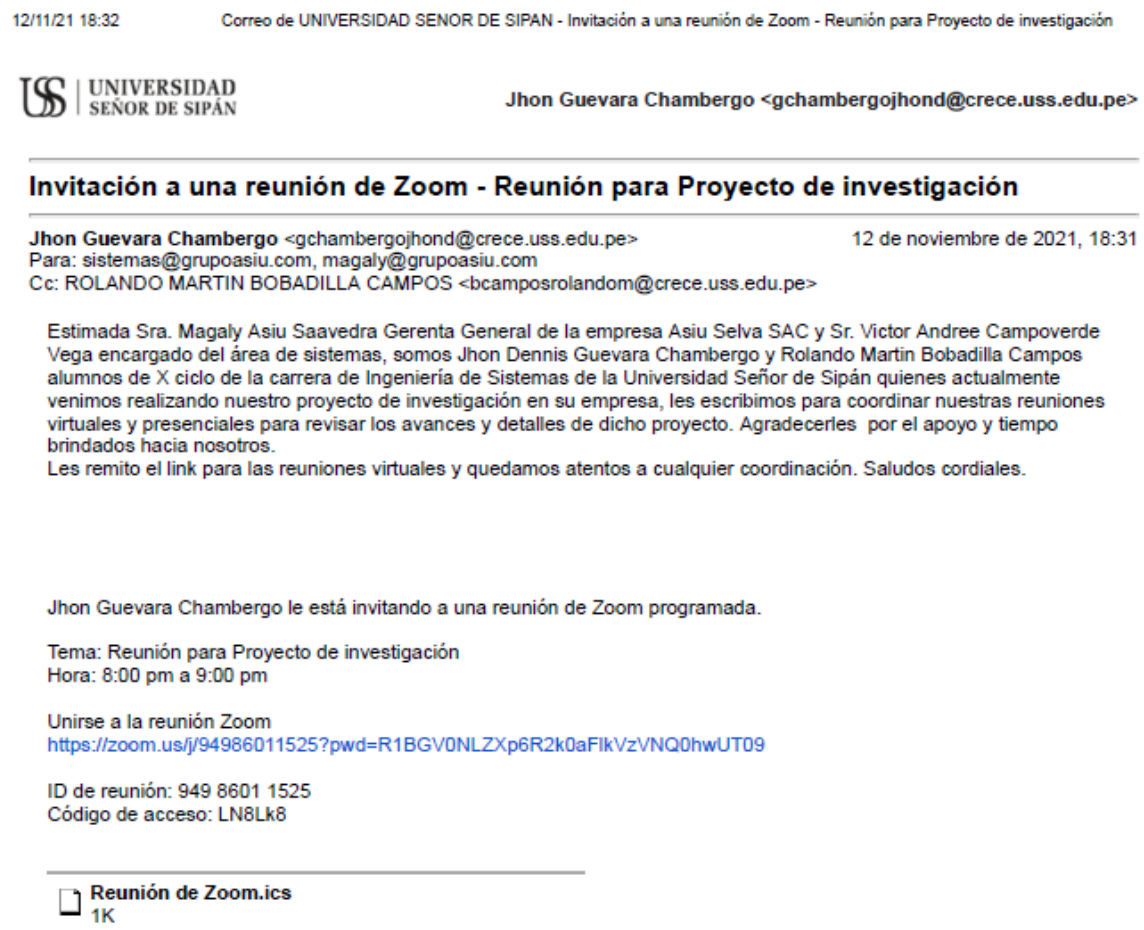
	Companies	**Cyber**	**Finance**	**Framework**	**Human Resource**	**Management**	**Methodologies**	**Operational**	**Risk**	**Security**	**Standards**
Companies	companies companies	companies cyber	companies finance	companies framework	companies human resource	companies management	companies methodologies	companies operational	companies risk	companies security	companies standards
Cyber	cyber companies	cyber cyber	cyber finance	cyber framework	cyber human resource	cyber management	cyber methodologies	cyber operational	cyber risk	cyber security	cyber standards
Finance	finance companies	finance cyber	finance finance	finance framework	finance human resource	finance management	finance methodologies	finance operational	finance risk	finance security	finance standards
Framework	framework companies	framework cyber	framework finance	framework framework	framework human resource	framework management	framework methodologies	framework operational	framework risk	framework security	framework standards
Human Resource	human resource companies	human resource cyber	human resource finance	human resource framework	human resource human resource	human resource management	human resource methodologies	human resource operational	human resource risk	human resource security	human resource standards
Management	management companies	management cyber	management finance	management framework	management human resource	management management	management methodologies	management operational	management risk	management security	management standards
Methodologies	methodologies companies	methodologies cyber	methodologies finance	methodologies framework	methodologies human resource	methodologies management	methodologies methodologies	methodologies operational	methodologies risk	methodologies security	methodologies standards
Operational	operational companies	operational cyber	operational finance	operational framework	operational human resource	operational management	operational methodologies	operational operational	operational risk	operational security	operational standards
Risk	risk companies	risk cyber	risk finance	risk framework	risk human resource	risk management	risk methodologies	risk operational	risk risk	risk security	risk standards
Security	security companies	security cyber	security finance	security framework	security human resource	security management	security methodologies	security operational	security risk	security security	security standards
Standards	standards companies	standards cyber	standards finance	standards framework	standards human resource	standards management	standards methodologies	standards operational	standards risk	standards security	standards standards

Anexo 11. Cuadro comparativo de estándares, metodologías internacionales de gestión de riesgos publicadas en artículos científicos de los últimos 5 años.

	ISO/IEC 27005 Tecnología de la Información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información	AS/NZS 4360	FRAP/FRAAP - Facilitated Risk Analysis and Assement Process	OCTAVE - Operational Critical Threat, Asset and Vulnerability Evaluation	IT Grundschutz (IT baseline Protection Manual)	MAGERIT 3.0 (Risk Analysis and Management Methodology for Information Systems)	MEHARI (Method for Harmonized	SRA (Structured Risk Analysis)
País	Suiza	Australia/Nueva Zelanda	Canadá	Estados Unidos	Alemania	España	Francia	Reino Unido
Responsable	International Organization for Standardization - The International Electrotechnical Commission	Estándar de Australia y Nueva Zelanda	Peltier Associates	Universidad de Carnegie Mellon	Oficina federal Alemana de Seguridad de la Información	Consejo Superior de Administración Electrónica.	Comisión de métodos de Clusif (Club Francés de la Seguridad de la Información)	Consult Hyperion
Enfoque	Seguridad de la Información	Gestión de Riesgo de Seguridad de Información	Tecnologías de Información	Análisis y gestión de riesgo de seguridad	Gestión de sistemas de seguridad de la información	Gestión de riesgos TIC	Seguridad de la Información	Valoración de los riesgos a menor escala
Métodos	NULL	NULL	NULL	OCTAVE, OCTAVE-S, OCTAVE Allegro	Metodología IT-Grundschutz	NULL	NULL	NULL
Procesos	- Establecimiento del contexto. - Valoración del riesgo (Identificación, Estimación y evaluación). - Tratamiento de riesgos. - Aceptación de riesgos. - Comunicación de riesgos. - Monitorización y revisión de riesgos.	- Establecimiento de contexto. - Identificar riesgos. - Analizar los riesgos. - Evaluar los riesgos. - Tratamiento de riesgos. - Monitorización y revisión. - Comunicación y consulta.	- Identificar roles e introducción. - Revisar el enfoque. - Identificar amenazas. - Establecer niveles de riesgo. - Priorizar Amenazas. - Identificar controles.	- Visión organizativa. - Visión tecnológica. - Estrategia y desarrollo del plan	- Preparar un informe general de las amenazas. - Determinar amenazas adicionales. - Evaluar las amenazas. - Seleccionar salvaguardas para riesgos críticos. - Consolidar resultados.	- Caracterización de los activos. - Caracterización de las amenazas. - Caracterización de las salvaguardas. -Estimación del estado de riesgo.	- Analizar los principales problemas. - Analizar las vulnerabilidades. - Disminuir y controlar los riesgos. - Supervisar la seguridad de la información.	- Modelo de servicio. - Valoración de las amenazas del modelo de servicio. - Modelo del sistema Valoración de las vulnerabilidades del sistema. - Valoración de Riesgos. - Identificación de contramedidas.
Herramienta de Soporte	NULL	NULL	FRAP	NULL	IT-Grundschutz Catalogs	PILAR	RISCARE	NULL
Elementos	Activos, Recursos, Vulnerabilidades, Amenazas y controles.	NO ENCONTRADO	Activo, Amenazas y Controles.	Procesos, Activos, Recursos, Vulnerabilidades, Amenazas y controles.	Activo, Amenazas, Contramedidas	Activo, Amenazas, Vulnerabilidades, Salvaguardas y Controles	Activo, Amenazas, Vulnerabilidades y Controles.	Amenazas, Vulnerabilidades y Contramedidas
Tipo de empresas	Grande / Mediana / Pequeña.	NO ENCONTRADO	Grande / Mediana / Pequeña.	Grande / Mediana / Pequeña.	Grande / Mediana / Pequeña.	Grande / Mediana / Pequeña.	Grande / Mediana / Pequeña.	Pequeña.
Tipo	Estándar	Estándar	Framework	Metodología	Estándar	Metodología	Metodología	Metodología
Iso 27005 Fase con mayor involucramiento	Todas las fases	Todas las fases	Análisis de riesgo	Todas las fases	Análisis y Tratamiento de riesgos	Análisis y Tratamiento de riesgos	Análisis y evaluación de riesgos	Análisis y Tratamiento de riesgos

	CRAMM - CCTA Risk Analysis and Management Method	FAIR (Factor Analysis of Information Risk)	CORAS - Construct a plataform for Risk Analysis of Security critical systems	TARA (Threat Agent Risk Assessment)	RISK IT FRAMEWORK	EBIOS - Et Identification des Objectifs de Sécurité	ISO/IEC 27004 Evaluación de la Seguridad de la Información
País	Reino Unido	EE. UU	Europeo (Noruega)	EE. UU	NO ENCONTRADO	Francia	Suiza
Responsable	Agencia Central de Cómputo y Telecomunicaciones (CCTA)	Lee Iacocca	SINTEF	MITRE	ISACA	Central Information Systems Security División	International Organization for Standardization - The International Electrotechnical Commission
Enfoque	Tecnologías de Información	Único modelo de valor en riesgo (VaR) estándar internacional para la ciberseguridad y el riesgo operativo en términos financieros.	Seguridad de la Información	Metodología para identificar y evaluar las amenazas cibernéticas y seleccionar contramedidas eficaces en mitigar esas amenazas.	Gobierno de los riesgos para la empresa, derivados de las TIC	Seguridad de Sistemas de Información	Seguridad de la Información
Métodos	NULL	NULL	NULL	NULL	NULL	NULL	NULL
Procesos	- Establecimiento de objetivos de seguridad. - Evaluación de riesgos. - Identificación y selección de contramedidas.	- Identificación de componentes inherentes del escenario (s) de riesgo. - Evaluación de la frecuencia de eventos de pérdida. - Evaluación de la magnitud de pérdida probable (PLM). - Derivación y articulación del riesgo.	Presentación. - Análisis de alto nivel. - Aprobación. - Identificación de riesgos. - Estimación de riesgo. - Evaluación de riesgo. - Tratamiento del riesgo.	- Análisis de susceptibilidad a amenazas cibernéticas (CTSA). - Análisis de corrección de riesgos cibernéticos (CRRA). - Desarrollo de datos y herramientas.	- Identificación de riesgo.	- Fase 1, Análisis del contexto. - Fases 2 y 3, Análisis de las necesidades de seguridad y de las amenazas. - Fases 4 y 5, Resolución del conflicto con pruebas de su cumplimiento.	Presenta cláusulas sobre: - Qué monitorizar, qué medir. - Cuándo monitorizar, medir, analizar y evaluar. - Quién monitorea, mide, analiza y evalúa. - Tipos de medida. - Procesos con anexos para la construcción de medidas.
Herramienta de Soporte	OCCTA Risk Analysis	RiskLens	Coras Editor	NULL	NULL	DCSSI - EBIOS	NULL
Elementos	Activos, Recursos, Vulnerabilidades, Amenazas y controles.	NO ENCONTRADO	Activos, Recursos, Vulnerabilidades, Amenazas y Controles.	Ciber activo, TTP, Vector de ataque, Contramedida	NO ENCONTRADO	Activo, amenazas, vulnerabilidades.	NO ENCONTRADO.
Tipo de empresas	Grande / Mediana / Pequeña	NO ENCONTRADO	Grande / Mediana / Pequeña	NO ENCONTRADO	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña	Grande / Mediana / Pequeña
Tipo	Metodología	Framework	Metodología	Metodología	Framework	Metodología	Estándar
Iso 27005 Fase con mayor involucramiento	Análisis y Evaluación de Riesgo	Análisis y evaluación de riesgo	Todas las fases	Análisis, Evaluación Y Tratamiento de Riesgo	Análisis y Evaluación de Riesgo	Todas las fases	Evaluación del riesgo

Anexo 12. Reunión con los interesados de la empresa ASIU SELVA SAC.



12/11/21 18:32 Correo de UNIVERSIDAD SENOR DE SIPAN - Invitación a una reunión de Zoom - Reunión para Proyecto de investigación

UNIVERSIDAD SEÑOR DE SIPÁN

Jhon Guevara Chambergo <gchambergojhond@crece.uss.edu.pe>

Invitación a una reunión de Zoom - Reunión para Proyecto de investigación

Jhon Guevara Chambergo <gchambergojhond@crece.uss.edu.pe> 12 de noviembre de 2021, 18:31
Para: sistemas@grupoasiu.com, magaly@grupoasiu.com
Cc: ROLANDO MARTIN BOBADILLA CAMPOS <bcamposrolandom@crece.uss.edu.pe>

Estimada Sra. Magaly Asiu Saavedra Gerenta General de la empresa Asiu Selva SAC y Sr. Victor Andree Campoverde Vega encargado del área de sistemas, somos Jhon Dennis Guevara Chambergo y Rolando Martin Bobadilla Campos alumnos de X ciclo de la carrera de Ingeniería de Sistemas de la Universidad Señor de Sipán quienes actualmente venimos realizando nuestro proyecto de investigación en su empresa, les escribimos para coordinar nuestras reuniones virtuales y presenciales para revisar los avances y detalles de dicho proyecto. Agradecerles por el apoyo y tiempo brindados hacia nosotros.
Les remito el link para las reuniones virtuales y quedamos atentos a cualquier coordinación. Saludos cordiales.

Jhon Guevara Chambergo le está invitando a una reunión de Zoom programada.

Tema: Reunión para Proyecto de investigación
Hora: 8:00 pm a 9:00 pm

Unirse a la reunión Zoom
https://zoom.us/j/94986011525?pwd=R1BGV0NLZXp6R2k0aFlkVzVNQ0hwUT09

ID de reunión: 949 8601 1525
Código de acceso: LN8Lk8

Reunión de Zoom.ics
1K

Anexo 13. Ficha de contexto organizacional.

1-INFORMACIÓN EMPRESA			
Número de reunión:		Fecha de reunión:	
Empresa:		RUC:	
Preparado por:			
Revisado por:			
Autorizado por:			
2- CONTEXTO DE LA ORGANIZACIÓN			
Cuáles son los objetivos de la empresa relacionado con los perseguidos en el proyecto.			
3- METAS EMPRESARIALES			
Establecer las metas u objetivos estratégicos de negocio para cumplir con su misión. *Nota*: *De no existir metas empresariales aplicar Guía de Metas empresariales y Metas de alineamiento de TI*			
4- METAS DE ALINEAMIENTO DE TI			
Establecer las metas u objetivos estratégicos del área de TI o de Sistemas para cumplir con las metas u objetivos estratégicos del negocio. *Nota*: *De no existir metas empresariales aplicar Guía de Metas empresariales y Metas de alineamiento de TI*.			
5- ROLES Y FUNCIONES			
Cuál es el equipo de trabajo detallando roles, responsabilidades y autoridades organizacionales.			
Organigrama empresarial.			

Anexo 14. Guía de Metas empresariales y Metas de alineamiento de TI

GUÍA RÁPIDA DE OBTENCIÓN DE METAS EMPRESARIALES Y METAS DE ALINEAMIENTOS DE TI

1- CARACTERIZACION DEL DOCUMENTO			
Número de reunión:		Fecha de reunión:	
Siglas del documento:		Versión:	
Nivel de confidencialidad:			
Preparado por:			
Revisado por:			
Autorizado por:			

2- CONTROL DE VERSIONES			
Versión:	Fecha:	Elaborado por:	Observaciones:

OBJETIVO: Definir las metas empresariales y metas de alineamiento de TI, si la empresa no las tuviera formalizada para integrar la gestión del riesgo empresarial relacionado con la TI y equilibrar los costes y beneficios de la gestión del riesgo empresarial relacionado con las TI.

I. Definir metas empresariales y metas de alineamientos de TI relacionadas con el objetivo de gestión: gestionar el riesgo

Las metas definidas en la empresa relacionada con las TI deben identificar, evaluar y reducir continuamente los riesgos relacionados con TI dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa. Por lo que se debe considerar la tabla N°1 como metas empresariales y la tabla N°2 como metas de alineamiento TI.

Con estas tablas se ayuda a la empresa a definir

META EMPRESARIAL COBIT 2019
EG02 Gestión de riesgo del negocio
EG06 Continuidad y disponibilidad del servicio del negocio

Tabla 30. Meta empresarial identificadas según COBIT 2019**. Fuente.** *COBIT 2019.*

METAS ALINEAMIENTO TI DE COBIT 2019
AG02 Gestión de riesgo relacionado con TI
AG07 Seguridad de la información, infraestructura de procesamiento y aplicaciones, y privacidad.

Tabla 31. Meta empresarial identificadas según COBIT 2019**. Fuente.** *COBIT 2019*

Anexo 15. Matriz RACI según MAGERIT. (Ministerio de Hacienda y Administraciones Públicas, 2012, págs. 56-57)

	rol	descripción
R	Responsible	Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI. Es quien debe ejecutar las tareas.
A	Accountable	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.
C	Consulted	Este rol posee alguna información o capacidad necesaria para terminar el traba-jo. Se le informa y se le consulta información (comunicación bidireccional).
I	Informed	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Tarea — Matriz RACI - ENS	Dirección	RINFO	RSERV	RSEG	RSIS	ASS
niveles de seguridad requeridos por la información		A	I	R	C	
niveles de seguridad requeridos por el servicio		I	A	R	C	
análisis de riesgos		I	I	A/R	C	
declaración de aplicabilidad		I	I	A/R	C	
aceptación del riesgo residual	I	A	A	R	I	
implantación de las medidas de seguridad		I	I	C	A	R
supervisión de las medidas de seguridad				A	C	R
estado de seguridad del sistema	I	I	I	A	I	R
planes de mejora de la seguridad				A	C	
planes de concienciación y formación				A	C	
planes de continuidad				C	A	
seguridad en el ciclo de vida				C	A	

Siendo:

Dirección – Alta Dirección, Órganos de Gobierno.

RINFO – Responsable de la Información.

RSERV – Responsable del Servicio.

RSEG – Responsable de la Seguridad.

RSIS – Responsable (operacional) del Sistema.

ASS – Administrador(es) de la Seguridad del Sistema.

Anexo 16. Documento de alcance

DOCUMENTO DE ALCANCE DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC

1- CARACTERIZACION DEL DOCUMENTO			
Número de reunión:		Fecha de reunión:	
Siglas del documento:		Versión:	
Nivel de confidencialidad:			
Preparado por:			
Revisado por:			
Autorizado por:			

2- CONTROL DE VERSIONES			
Versión:	Fecha:	Elaborado por:	Observaciones:

OBJETIVO: Cotejar documentos para definir el alcance en una organización

I. Cotejar documentos

Una organización tiene un conjunto de información que lo caracteriza, los cuales son necesarios conocer si se cuenta con los registros correspondientes y de esta manera dar inicio a la implementación del alcance de la metodología, es decir del área, conjunto de áreas, procesos o conjunto de procesos donde se gestionarán los riesgos.

ITEM	DESCRIPCIÓN	SÍ	NO
1	Misión empresarial.		
2	Visión empresarial.		
3	Metas empresariales.		
4	Metas de Tecnologías e Información.		
5	Políticas internas y externas.		
6	Normas o reglamentos.		
7	Organigrama.		
8	Número de trabajadores de la empresa.		

OBSERVACIONES

II. Definición de alcance.

La definición de alcance se determinará a través de **reuniones** establecidas por el responsable de información basándose en el **juicio de expertos** de los consultados con el fin de obtener la firma de la parte interesada correspondiente en la siguiente acta.

ACTA DE DEFINICION DE ALCANCE

Mediante la presente acta se define como área, conjunto de áreas, procesos o conjunto de procesos, a los siguientes descritos:

1. ……
2. ……
3. ……

Responsable del alcance: ……

Colaboradores, empleados o trabajadores involucrados en el alcance: ……

Firmas

_____	_____
RINFO	Parte interesada

Anexo 17. Manual para registro de inventario de activos

MANUAL DE USO PARA IDENTIFICACIÓN, TIPIFICACIÓN Y REGISTRO DEL INVENTARIO DE ACTIVOS DE INFORMACIÓN

1- CARACTERIZACION DEL DOCUMENTO			
Número de reunión:		Fecha de reunión:	
Siglas del documento:		Versión:	
Nivel de confidencialidad:			
Preparado por:			
Revisado por:			
Autorizado por:			

2- CONTROL DE VERSIONES			
Versión:	Fecha:	Elaborado por:	Observaciones:

OBJETIVO: Identificar los activos de información relacionados con la gestión de riesgo de la empresa ASIU SELVA SAC, tipificarlos de acuerdo a la metodología AD HOC para después registrarlo de manera adecuada en el instrumento de gestión de riesgo.

I. IDENTIFICACIÓN Y TIPIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN DE ASIU SELVA SAC

Los activos de información serán clasificados en 8 categorías. Estas categorías se describen a continuación:

1. **Datos/Información**: es un activo que será almacenado en equipos, en ficheros o en base de datos. Entre ellos esta:
    a. La información presente en ficheros y en documentos virtuales (archivos Excel, Word, etc.)
    b. Copias de respaldo.
    c. Datos de configuraciones del sistema de información.
    d. Datos de gestión interna.
    e. Datos de contraseñas.
    f. Datos de validación de credenciales (licencias de software).
    g. Datos de prueba.
    h. Código fuente.
    i. Código ejecutable.

2. **Servicios**: contempla los servicios prestados por el sistema, tales como:
    a. Gestión de identidades (alta y bajas de usuarios de los sistemas).
    b. Almacenamiento de ficheros.
    c. Transferencia de ficheros.
    d. Servicios en www.

3. **Software**: son los programas, aplicativos, desarrollos, etc. Tareas automatizadas para su desempeño, por ejemplo:
    a. Desarrollo propio.
    b. Desarrollo subcontratado.
    c. Ofimática.
    d. Navegador web.
    e. Servidor de aplicaciones, de presentación, de correo electrónico, de ficheros, de correo electrónico.
    f. Sistema operativo, de gestión de base de datos, de backup.
    g. Gestor de máquinas virtuales.

4. **Hardware**: son los medios materiales, físicos, destinados a soportar las aplicaciones informáticas o responsable de la trasmisión de datos.
    a. Grandes equipos que requieren un entorno específico para su operación y son difícilmente reemplazables en caso de destrucción.
    b. Informática personal son fácilmente reemplazables y un coste pequeño.
    c. Medios de impresión, escáner.
    d. Soporte de red como módems, conmutadores, encaminadores, cortafuegos.
    e. Teléfono IP.

5. **Redes de comunicación**: medios de transporte que llevan los datos de un sitio a otro, por ejemplo:
    a. Red telefónica.
    b. Red inalámbrica.
    c. Red local.
    d. Internet.

6. **Soporte de información**: son los medios electrónicos y no electrónicos que nos permiten almacenar información tales como:
    a. Discos virtuales, CD, DVD, memorias USB, tarjetas de memoria.
    b. Material impreso, tarjetas perforadas.

7. **Equipamiento auxiliar**: se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos, por ejemplo:
    a. Fuentes de alimentación.
    b. Equipos de climatización.
    c. Cableado.
    d. Equipos de destrucción de soportes de información.
    e. Mobiliario: armarios, cajas, etc.

8. **Instalaciones**: son los lugares donde se hospedan los sistemas de información y comunicaciones pueden considerarse los edificios y los cuartos.

9. **Personal**: se refiere a las personas relacionadas con los sistemas de información.

La categorización del activo servirá para crear los códigos del activo. Esta abreviatura de la categorización del activo se detalla en el siguiente cuadro:

Categorías de activos	**Abreviatura**
Datos/Información	DI
Servicios	SE
Software	SW
Hardware	HW
Redes de comunicación	RC
Soporte de información	SI
Equipamiento auxiliar	EA
Instalaciones	IF
Personal	PE

Para la tipificación del activo se debe considerar los siguientes campos:

1. **Código:** es el identificador del activo en la gestión de riesgo. La formación del código se realiza respetando esta nomenclatura:

   $$< abreviatura\ categoria > + < número\ correlativo 3\ dígitos >$$

   Por ejemplo: DI001, EA001.
2. **Nombre**: adjetivos del activo que se relaciona con la categorización.
   Por ejemplo: Red local (perteneciente a la categoría de Redes de comunicación).
3. **Descripción:** especificación detallada del nombre del activo.
   Por ejemplo: LAN Chiclayo (relacionado con la Red local del ejemplo anterior).
4. **Responsable:** encargado del activo.
5. **Ubicación:** lugar físico o espacio donde se aloja o se encuentra ubicado el activo.
6. **Número:** cantidad numérica de ese activo en la organización.

7. **Dependencia:** es la estructura de dependencia entre activos, considerando una jerarquía de arriba hacia abajo. Por ejemplo, cuanto se afectaría “un activo superior” si un incidente de seguridad ocurriera en un “activo inferior”.
8. **Tipo de activo:** El tipo de activo puede ser “activo” o “ciber activo”. Para ser considerado como ciber activo debe responder de manera afirmativa a 4 preguntas:
    a. ¿el activo se interrelaciona entre personas?
    b. ¿el activo se interrelaciona con el software?
    c. ¿el activo se interrelaciona con el internet?
    d. ¿el activo se interrelaciona con una red interna o red local?

Líneas abajo se detalla un ejemplo de tipificación de un activo:

Código: RC001.

Nombre: Red Local.

Descripción: LAN Chiclayo.

Responsable: Responsable de TI.

Ubicación: Oficina de Chiclayo.

Número: 1.

Dependencia: Red privada.

Tipo de activo: ciber activo.

Anexo 18. Hoja GESTIÓN CENTRALIZADA del Instrumento de Gestión de Riesgos.

GESTIÓN CENTRALIZADA 1/4

Categoría Activ	Código	Nombre	Descripció	Responsabl	Ubicación	Número	Dependencia
Red de comunicaciones	RC001	Red local	LAN Chiclayo	Responsable de TI	Oficina de Chiclayo	1	Red Privada

GESTIÓN CENTRALIZADA 2/4

	¿El activo se interelaciona entre ...								
	... personas?		... software?		... internet?		... intranet/red local?		
Dependencia	SÍ	NO	SÍ2	NO2	SÍ3	NO3	SÍ4	NO4	Tipo de activo
Red Privada	1		1		1		1		Ciber activo

GESTIÓN CENTRALIZADA 3/4

				Valorizar activos				
Código	Nombre	Descripció	Tipo de activo	Disponibili	Integridad	Confidencialid	puntaje	Priorizar
RC001	Red local	LAN Chiclayo	Ciber activo	5	5	5	5	PRIORIZAR

GESTIÓN CENTRALIZADA 4/4

Valorizar activos					Grupo de Vulnerabilidades				
Disponibili	Integridad	Confidencialida	punta	Priorizar	V1	V2	V3	V4	V5
5	5	5	5	PRIORIZAR	V0002	V0005	V0012	V0015	

Anexo 19. Lista de criterios

Criterios de valorización de activos

Disponibilidad ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?

Confidencialidad ¿qué daño causaría que lo conociera quien no debe?

Integridad ¿qué perjuicio causaría que estuviera dañado o corrupto?

	Disponibilidad	**Confidencialidad**	**Integridad**	**puntaje**
Muy alto	Es muy grave el perjuicio que causaría a la empresa no poder tenerlo o no poder utilizarlo	Es muy grave el daño que causaría a la empresa que lo conociera quien no debe	Es muy grave el desperfecto que causaría si estuviera dañado o corrupto	**5**
Alto	Es grave el perjuicio que causaría a la empresa no poder tenerlo o no poder utilizarlo	Es grave el daño que causaría a la empresa que lo conociera quien no debe	Es grave el desperfecto que causaría si estuviera dañado o corrupto	**4**
Medio	Es parcial el perjuicio que causaría a la empresa no poder tenerlo o no poder utilizarlo	Es parcial el daño que causaría a la empresa que lo conociera quien no debe	Es parcial el desperfecto que causaría si estuviera dañado o corrupto	**3**
Bajo	Es bajo el perjuicio que causaría a la empresa no poder tenerlo o no poder utilizarlo	Es bajo el daño que causaría a la empresa que lo conociera quien no debe	Es bajo el desperfecto que causaría si estuviera dañado o corrupto	**2**
Muy bajo	Es irrelevante el perjuicio que causaría a la empresa no poder tenerlo o no poder utilizarlo	Es irrelevante el daño que causaría a la empresa que lo conociera quien no debe	Es irrelevante el desperfecto que causaría si estuviera dañado o corrupto	**1**

Criterios basados en la frecuencia

RANGO	**MUY ALTO**		**ALTO**		**MEDIO**		**BAJO**	**MUY BAJO**	
TIEMPO ENTRE EVENTOS	Diario	Semanal	Mensual	4 veces al año	2 veces al año	1 vez al año	1 vez cada 2 años	1 vez cada 5 años	1 vez cada 10 años
FRECUENCIA /DÍAS	365	52	12	4	2	1	0.5	0.2	0.1

Criterios para la estimación de riesgo

FRECUENCIA	5	5A	10B	15C	20D	25E
	4	4A	8B	12C	16D	20E
	3	3A	6B	9C	12D	15E
	2	2A	4B	6C	8D	10E
	1	1A	2B	3C	4D	5E
RIESGO		1	2	3	4	5
		IMPACTO				

FRECUENCIA	Muy Alto	ALTO	MUY ALTO	MUY ALTO	MUY ALTO	MUY ALTO
	Alto	MEDIO	ALTO	ALTO	MUY ALTO	MUY ALTO
	Medio	BAJO	MEDIO	MEDIO	ALTO	ALTO
	Bajo	MUY BAJO	BAJO	BAJO	MEDIO	MEDIO
	Muy Bajo	MUY BAJO	MUY BAJO	MUY BAJO	BAJO	BAJO
RIESGO		Muy Bajo	Bajo	Medio	Alto	Muy Alto
		IMPACTO				

Criterios para el tratamiento de riesgo

Nivel Riesgo[1]	Tratamiento	Coste- Beneficio[2]
Muy Bajo	Aceptar el riesgo o compartirlo según costo beneficio. (A)	El nivel de riesgo está muy alejado del nivel de tolerancia.
Bajo		
Medio	Mitigar, el riesgo. (M)	El coste del tratamiento es adecuado a los beneficios.
Alto	Compartir o transferir el riesgo (T)	El coste del tratamiento por terceros es más beneficioso que el tratamiento directo.
Muy Alto	Evitar el riesgo (E)	El coste del tratamiento es muy superior a los beneficios.

Tratamiento de riesgo por niveles según Ruge (2012), 2. Tratamiento de riesgo por coste-beneficio según (Instituto Nacional de Ciberseguridad [INCIBE], 2015)

Anexo 20. Programa de medición para la metodología de gestión de riesgos.

Descripción:

El módulo está basado en los procesos de la norma ISO 27004.

Objetivos:

- Mantener la mejora continua de la gestión de riesgos de seguridad de la información de la empresa ASIU SELVA SAC.
- Controlar los riesgos de seguridad de la información de la empresa ASIU SELVA SAC, lo más cercano al ambiente real de producción.
- Mantener un sistema integral de alertas ante riesgos que se están materializando o están encaminados a materializarse, con el fin de realizar rectificaciones de amenazas lo antes posible.
- Motivar al personal respecto a la gestión de riesgos de seguridad de la información.
- Realizar comparaciones de niveles de riesgos obtenidos con el historial de incidentes sucedidos en los activos de información de ASIU SAC.

Indicadores:

ID	Descripción	Método de cálculo	Criterios de evaluación
1	Número total de incidentes de seguridad	Se revisará el historial de riesgos cuyo origen se manifestó desde un incidente reportado.	Alto: > 10 al mes. Medio: > 5 al mes Bajo: > 1 al mes
2	Interacciones de los empleados fuera de horario.	Se revisará la bitácora de acceso al sistema fuera de horario.	Alto: > 100 al mes Medio: > 50 al mes Bajo: > 1 al mes
3	Tiempo medio de identificación / detección	Se medirá desde el primer reporte hasta el manifiesto de identificación del responsable.	Alto: > 2 horas Medio: > 40 min. Bajo: > 1 minuto
4	Tiempo medio de contención / resolución	Se medirá el tiempo trascurrido desde la identificación formal y	Alto: > 1 hora Medio: > 20 min. Bajo: > 1 minuto

		resolución evidenciada por el usuario.	
5	Costo por incidente	La resolución sobrepasa el presupuesto establecido para la atención de materialización de riesgo.	Alto: > 70% del p. Medio: > 30% del p. Bajo: > 5% del presupuesto.
6	Inactividad del sistema	Tiempo transcurrido de inactividad del sistema.	Alto: > 90 minutos Medio: > 30 min. Bajo: > 5 minutos
7	Cumplimiento de controles	Porcentaje de controles cumplidos del total de controles definidos por la metodología de gestión de riesgos.	Alto: > 1% Medio: > 60% Bajo: > 95%