Revista Peruana de Computación y Sistemas 2019 2(1):43-60
DOI: http://dx.doi.org/10.15381/rpcs.v2i2.17103

ISSN Online: 2617-2003
Facultad de Ingeniería de Sistemas e Informática
Universidad Nacional Mayor de San Marcos

Artículo de revisión

Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte

Information security risk management model: A state of the art review

Mauro Néstor Zevallos Morales
Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática. Lima, Perú
Email: mauro.zevallos@unmsm.edu.pe, cebayoz@gmail.com

Resumen

Las organizaciones tanto públicas como privadas, atraviesan escenarios dinámicos con el surgimiento e irrupción de las nuevas tecnologías de información, haciendo un uso cada vez más intensivo de la información. Al analizar los procesos e interrelaciones de estas organizaciones con los recursos de información a los que acceden, es fundamental considerar los nuevos riesgos a los que las organizaciones se exponen. Esto requiere desarrollar estrategias de gestión de riesgos que faciliten el análisis, identificación y tratamiento de riesgos inherentes a activos de información, con el propósito de buscar medios para minimizar el impacto negativo. En este escenario son útiles el empleo de modelos de gestión de riesgos que simplifica y sistematiza dichas tareas.

El presente estudio abarca una revisión de la literatura referente a marcos, modelos y metodologías de gestión de riesgos, para identificar las actividades, elementos y componentes a desarrollar para la elaboración de un modelo de gestión de riesgos orientado a la seguridad de la información, que permita cubrir asuntos referentes a la seguridad de la información , ciberseguridad y dar cumplimiento a los requerimientos particulares de la organización para el desarrollo de un modelo alineado a las necesidades y requerimientos propias de una organización.

Palabras clave: Riesgo; gestión de riesgos; seguridad de la información; ISO 27001.

Abstract

Both public and private organizations are going through dynamic scenarios with the emergence and inrush of new information technologies, making an increasingly intensive use of information. When analyzing the processes and interrelationships of these organizations with the information resources they access, it is essential to consider the new risks to which organizations are exposed. This requires developing risk management strategies that facilitate the analysis, identification and treatment of the risks associated with information assets in order to find ways to minimize the negative impact. In this scenario, the use of risk management models that simplify and systematize these tasks are useful.

The present study includes a review of the literature referring to risk management frameworks, models and methodologies, to identify the activities, elements and components to develop for the development of a risk management model oriented to information security, which allows covering issues related to information security, cybersecurity and compliance with the particular requirements of the organization for the development of a model aligned to the needs and requirements of an organization.

Keywords: Risk; risk management; information security; ISO / IEC 27001.

Correspondencia:
Dirección: Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática. Calle Germán Amézaga N° 375, Ciudad Lima 1.

Recibido 13/11/2019 - Aceptado 27/12/2019

Citar como:
Zevallos, M. (2019) Modelo de gestión de riesgos de seguridad de la información: Una revisión del estado del arte. Revista Peruana de Computación y Sistemas, 2(2):43-60. http://dx.doi.org/10.15381/rpcs.v2i2.17103

1. Introducción

La seguridad es un aspecto relevante de toda actividad de procesamiento de información, sobre todo en ámbitos donde la información presenta una naturaleza crítica y confidencial [1] que pueden brindar una ventaja estratégica y competitiva a las organizaciones.

A medida que se realiza una adopción gradual de las nuevas tecnologías de la información, transformando las actividades, procesos y procedimientos mecánicos y manuales de las organizaciones, surgen brechas de seguridad no contempladas que incrementan el riesgo de las operaciones y control de procesos. En este contexto en el que se produce una sinergia entre la protección de activos de la información contenida, tanto en medios digitales como en físicos, resulta imperativo la utilización de marcos que permitan la correcta protección y gobierno de los mismos, a fin de contribuir a alcanzar los objetivos estratégicos que la organización persigue. Considerando esto, Guerrero (2011) expresa que: aun cuando en las organizaciones existe interés en la aplicación de una gestión de riesgos, esto no genera el impacto esperado debido al poco entendimiento respecto a la gestión del riesgo y a la carencia de procesos que generen cambios organizacionales.". [2]

El desarrollo de las operaciones, procesos y procedimientos propios de las organizaciones se da en este contexto, en el que se pretende impulsar iniciativas de transformación digital e impulsar la utilización de tecnologías emergentes, cuya adopción colisiona con procesos manuales y mecánicos que se encuentran vigentes, (los cuales son de valor para la organización), y otros que presentan un fuerte arraigo a la cultura organizacional, presentando una resistencia al cambio. Esta coyuntura se hace más compleja al considerar que los operadores de los procesos de la organización no siempre tienen identificado plenamente todos los activos de información que manejan, desconociendo el valor de los mismos, así como su adecuado tratamiento. Mariño como se citó en Mercado (2016) manifiesta a su vez que: "respecto a las responsabilidades de asuntos pertenecientes a la seguridad de los activos de información, existe un desentendimiento en las organizaciones", especialmente las del sector público, manifestándose en el nivel de liderazgo, que usualmente es responsabilidad de las áreas tecnológicas, sin contar con el apoyo de la alta dirección, teniendo una orientación hacia la seguridad informática, sin considerar plenamente aspectos integrales de seguridad orientado a los activos de información, ya sean físicos o digitales; incrementando con ello los riesgos a los cuales la organización queda expuesta. [3]

En este escenario, la utilización de modelos que contribuyan a la gestión adecuada de dichos los riesgos, puede reducir los impactos negativos de riesgos inherentes a los activos de información con que cuenta la organización, aplicando técnicas analíticas que permitan conocer el nivel de sucesos peligrosos, a fin de evaluar el impacto, probabilidad y las consecuencias que pudieran generar, contribuyendo con el análisis, identificación y tratamiento de dichos riesgos. [1] [4]

El presente trabajo se enfoca en realizar una revisión de la literatura referente a modelos de gestión de riesgos, con el propósito de identificar los elementos y actividades a considerar durante la elaboración de marcos que permitan gestionar riesgos pertenecientes a la seguridad de la información.

En la segunda sección del documento, como parte del desarrollo del marco teórico, se realizará una definición de términos y conceptos básicos relacionados a la gestión de riesgos. Posterior a ello, la tercera sección contiene una revisión de la literatura referente al tema, lo cual nos permite identificar los elementos, actividades y procesos utilizados en la elaboración de modelos de gestión de riesgos. En la cuarta sección se presenta elementos, actividades y procesos enriquecidos, los cuales permitirán establecer una línea base para la concepción y desarrollo de un modelo de gestión que brinde los lineamientos a seguir respecto a seguridad de la información. La quinta sección plantea las conclusiones obtenidas a partir de la revisión de la literatura, así como recomendaciones sobre investigaciones futuras.

2. Marco Teorico

El marco teórico comprende la definición de conceptos esenciales para el adecuado entendimiento de los modelos de gestión de riesgos.

RIESGO

Las directrices de gestión del riesgo lo definen como "Efecto de la incertidumbre sobre los objetivos". [5]

Dentro del ámbito de seguridad de la información, se considera al riesgo como la "Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias". [6]

El nivel de riesgo se puede "estimar y valorar cuantitativamente", como el producto del impacto, por la probabilidad de ocurrencia. [7]

GESTION DEL RIESGO

Se define como las "actividades coordinadas para dirigir y controlar la organización con relación al riesgo". [5]

Cuyo propósito es "gestionar el riesgo" a fin de establecer controles" e indicadores que puedan contribuir a garantizar aspectos que permitan resguardar la información. [8]

MARCOS DE GESTION DEL RIESGO

Conjunto integral de políticas que apoyan y sustentan la gestión de riesgo, cuyo objetivo es minimizar el impacto de riesgos asociados a los servicios o productos generados por la organización. [9]

La gestión del riesgo cambia con el tiempo. Cada marco de gestión de riesgos tiene sus ventajas y desventaja, debiendo considerarse el uso del marco más simple que cumpla con los requisitos organizacionales y usar el sentido común para asegurar su correcta implementación. A medida que se realicen evaluaciones periódicas, se debe asegurar que la selección del marco satisfaga sus necesidades. [10]

SEGURIDAD DE LA INFORMACION (SI)

Contempla la protección de datos o activos que almacenen información, que sea esencial para una organización. El manejo de dichos activos puede o no implicar el uso de la tecnología. [11] Es fundamental un proceso o planificación proactiva a fin de proteger la información, que garantice un uso eficiente en el procesamiento de la información. [12]

Para tal fin es determinante que las organizaciones consideren medidas que incrementen los aspectos relacionados a la seguridad de los activos de información. [13] [14]

3. Estado del Arte

Comprende inicialmente una revisión de las metodologías, herramientas y técnicas empleadas en la elaboración de marcos de gestión de riesgos; para luego presentar modelos de gestión de riesgos propiamente dichos, elaborados para distintas empresas u organizaciones particulares.

3.1. Enfoques para la construcción de modelos de gestión de riesgos

El enfoque planteado en esta etapa, comprende el aspecto metodológico a seguir a fin de posibilitar la identificación de elementos, procesos, herramientas, etc. que permitan conocer los lineamientos a seguir en la elaboración y establecimiento de modelos de gestión de riesgos, en ese sentido, con respecto al tratamiento de riesgos referente a proyectos de tecnologías de la información Nehari Talet et al (2014) sugiere considerar los siguientes pasos: [15]

– Identificación de riesgos mediante el uso de técnicas como lluvia de ideas.

– Análisis de riesgos para determinar el tratamiento de un determinado riesgo.

– Planificación de riesgos para establecer una seriedad del riesgo según su impacto.

– Monitoreo de riesgo que implique la evaluación de los riesgos a fin de generar conocimiento respecto a la eficacia de las respuestas existentes.

Lo cual se refleja en la figura 1.

Las implementaciones de los conceptos descritos en los modelos existentes, permiten determinar planes de acción ante riesgos, incluyendo sistemas de monitoreo y evaluación, así como canales de comunicación, consulta y comentarios que pueden brindar una gestión de riesgos más ágil. [16] [17]

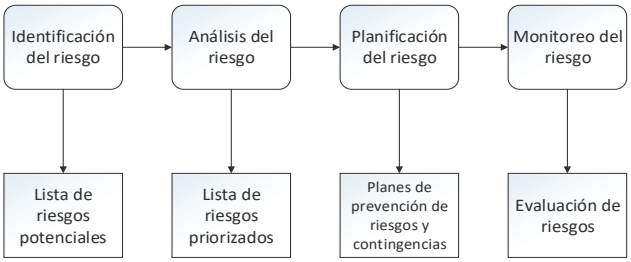

Figura 1 Tratamiento de Riesgos en Proyectos de TI. [15]

El propósito de este tipo de instrumentos es que se aplique fácilmente a cualquier organización, a fin de evaluar su capacidad de gestión de riesgos, [18] estas soluciones permiten brindar valor añadido a la organización como:

– Almacenar información histórica de riesgo y conocimiento.

– Guiar a las empresas y organizaciones a desarrollar una capacidad adecuada de respuesta a sus riesgos, de acuerdo con el modelo establecido.

– Llevar a cabo la evaluación y el monitoreo de la madurez de sus procesos respecto a sus riesgos.

– Disponer de manuales, tutoriales y poder educar a los colaboradores sobre gestión de riesgos por medio de la gestión del conocimiento.

– Tener la capacidad de almacenar y recuperar las buenas prácticas, a fin de mejorar su desempeño.

– Diseñar una metodología adaptada a las características de la organización.

– Proporcionar todas las plantillas necesarias para los procesos a desarrollar.

– Desarrollar el registro de riesgo del proyecto.

– Adaptar la metodología de gestión de riesgos a futuros proyectos u organizaciones similares.

La organización, debe comprender no solo cómo, sino cuándo usar los métodos o marcos de riesgo, el cual debe cubrir todas las situaciones y ser personalizado a las amenazas y vectores actuales que afectan a los activos de la información [10]. En ese sentido, de acuerdo a los modelos planteados, en el desarrollo de las metodologías propuestas, se toma como base distintos marcos como: PMBoK, ISO 27000, Cobit, ISO 31000, NIST, etc. y mediante procesos como el mapping y matching, se generan modelos que se adaptan a circunstancias particulares y puede implicar diversas clasificaciones de riesgos en grupos específicos dependiendo del sector en el que se desenvuelve la organización.

En este contexto, Pardo et al (2016) desarrolla una investigación enfocada en realizar una armonización entre

la ISO 27001 e ISO 20000-2 en términos de las necesidades particulares de una organización, considerando una estrategia a seguir que consiste en la implementación de un proceso y un conjunto de métodos, incluido un mapping, con la finalidad de establecer el grado de relación entre componentes de dichas normas. [19]

Sobre la base de los componentes identificados, se define y configura una estrategia de armonización según dos roles: ejecutantes y revisores, junto con tres métodos de armonización con sus respectivas actividades:

Método 1. Homogeneización. Considera las siguientes actividades:

– Adquisición de conocimiento sobre los modelos involucrados.

– Análisis de la estructura y terminología.

– Identificación de requisitos.

– Correspondencia.

Método 2. Comparación. Considera las siguientes actividades:

– Diseñar el mapping.

– Llevar a cabo el mapping.

– Presentar los resultados del mapping.

– Analizar los resultados del mapping.

Método 3. Integración. Considera las siguientes actividades:

– Diseño de la integración.

– Establecimiento de criterios de integración.

– Realización de la integración.

– Análisis de la integración realizada.

– Presentación del modelo integrado.

Como parte de un estudio enfocado en identificar los procesos del "Sistema de Gestión de Seguridad de la Información" (SGSI) Haufe et al. (2016) propone un modelo, describiendo los procesos existentes entre la norma ISO/IEC 27000, COBIT e ITIL; a través de un mapping realizado entre estas normas y estándares, se realiza la identificación, descripción y se especifica la interacción e interfaces de dichos procesos, así como permite identificar cuáles son los procesos centrales de un SGSI, [20] [21] A fin de alinear dichos procesos con los objetivos y la misión de la organización, para ello busca dar respuesta a dos interrogantes de investigación planteadas: ¿Qué procesos son mencionados en el establecimiento de los estándares de gestión de seguridad y en qué medida están relacionados?, ¿Cuáles de los procesos identificados son procesos de un SGSI? [21] tal como se muestra en la Figura 2.

Los autores consideran que una comprensión actualizada de las necesidades de las partes interesadas con la seguridad de la información (SI), es clave para lograr los propósitos del SGSI. Para la identificación de los procesos se utilizó el siguiente método:

Se analiza las series ISO 27000 con relación a los procesos identificados en una investigación anterior [21]. Se analiza ITIL y COBIT realizando un matching con respecto a los procesos identificados de un SGSI. Los resultados obtenidos de los pasos anteriores se consolida por medio de un mapping que se documenta en una investigación similar en la que se realiza la identificación e interacción de los procesos a nivel alto. [22]

El valor agregado que ofrece este marco es un cambio en el enfoque orientado al control de las normas hacia un enfoque más profesional y orientado a las operaciones, permitiendo alinear la madurez de los procesos del SGSI y con ello a los requisitos de la organización. Esto ayuda a los profesionales a gestionar la SI de manera más eficiente y efectiva, enfocándose en procesos de SGSI y no perderse en la cantidad cada vez más inmanejable de controles y medidas de seguridad de distintos marcos.

En este escenario es fundamental la identificación de los procesos centrales de un SGSI y las medidas de seguridad controladas por dichos procesos. Al mismo tiempo realizar una identificación de criterios para procesos centrales de un SGSI. En una investigación similar, llevadas a cabo por Haufe et al (2016) a través de la participación de especialistas y expertos en el área, se realiza una discriminación entre; procesos centrales, que ofrecen un valor directo a la organización; procesos de gestión, los cuales definen los objetivos de la organización, y controlan y supervisan el logro de dichos objetivos; y procesos de soporte, que proporcionan y administran los recursos necesarios sin entregar el valor directo al cliente. [21]

Los autores identificaron los siguientes criterios básicos para la identificación de los procesos centrales de SGSI:

Criterio 1 - Regularidad.

Criterio 2 - Transformación.

Criterio 3 - Operativo.

Criterio 4 - Responsabilidad.

Criterio 5 - Generación de valor.

Para la identificación de los procesos centrales del SGSI, se definen tres categorías:

– Procesos centrales del SGSI: procesos que fueron identificados por el 80% o más de los expertos.

– Procesos no identificados claramente como procesos centrales del SGSI: fueron identificados por no menos del 20% pero no más del 80% de los expertos.

– Procesos identificados como no centrales del SGSI: identificados por menos del 20% de los expertos.

PROCESOS CENTRALES
Evaluación de riesgos de SI (100%)
Asegurar la conciencia y competencia necesaria (100%)
Controlar procesos subcontratados (100%)
Auditoría interna (100%)
Gestión de incidentes de SI (100%)
Tratamiento de riesgos de SI (99%)
Mejora de SI (99%)
Gestión de la relación con el cliente (95%)
Evaluación del desempeño (88%)
Gestión de cambio de SI (87%)
PROCESOS NO IDENTIFICADOS CLARAMENTE
Control de la documentación (72%)
Gestión de recursos (47%)
Comunicación (41%)
Gestión de requisitos (40%)
Gestión de la disponibilidad y continuidad del servicio (40%)
Gobernanza de SI (24%)
PROCESOS NO CENTRALES
Gestión de la configuración (16%)
Gestión de la capacidad (8%)
Presupuesto y contabilidad de servicios (5%)
Gestión de problemas (4%)
Planificación del SGSI (0%)
Gestión de nivel de servicio (0%)
Relaciones comerciales (0%)
Gestión de proveedores (0%)
Solicitudes de incidentes de servicio (0%)
Gestión de cambios (0%)
Gestión de lanzamiento y despliegue (0%)

Figura 2. Identificación de procesos del SGSI [21]

A fin de establecer el grado de relación entre los diversos componentes o elementos, se utiliza una escala de similitud, propuesta por Baldassarre (2010) que guía el proceso de armonización, a través de un enfoque sistemático por etapas, [23] lo suficientemente general como para aplicarse a cualquier modelo de referencia que se tenga en cuenta, el cual considera:

(N) Not related (No relacionado)

(W) Weakly related (Débilmente relacionado)

(P) Partially related (Parcialmente relacionado)

(S) Strongly related (Fuertemente relacionado)

(Pimchangthong & Boonjing, 2017) realizan un estudio como los factores organizacionales y la gestión de riesgos influyen en el éxito de proyectos de TI, considerando que solo el 12% de los proyectos habían finalizado a tiempo y dentro del presupuesto estimado y el 70% de los proyectos de software falla, debido a requisitos deficientes. [24]

Se considera que, entre varios factores, la gestión del riesgo fue uno de los factores importantes de éxito de los proyectos por lo que la gestión de riesgos es la herramienta de gestión más importante que un gerente de proyecto puede utilizar para aumentar la probabilidad de éxito del proyecto.

Los resultados muestran que la identificación de riesgos y el análisis de riesgos, tuvieron un alto nivel de importancia e influyeron en el rendimiento del proceso y el éxito de los proyectos.

La identificación del riesgo fue la mayor influencia positiva en el rendimiento del producto, seguida de cerca por la respuesta al riesgo, mientras que el análisis del riesgo no influyó en alto grado en el rendimiento del producto. El aspecto de la planificación de la respuesta, la monitorización y el control del riesgo se encontraban en un nivel moderado de importancia. Las diferencias en los tipos de organización afectaron el éxito del proyecto de TI en todos los aspectos. Sin embargo, las diferencias en los tamaños organizacionales no afectaron el éxito del proyecto.

(Boiko & Shendryk, 2017) estudian el incremento constante de acciones no autorizadas a los sistemas de información, considerando que más de la mitad de estas acciones son realizadas por usuarios internos se le considera como "grupo de riesgo". El estudio aborda aspectos como: desarrollo de medidas organizacionales, compatibilidad de herramientas de procesamiento de hardware y software, así como de los respaldos de la información, desarrollo de normativas que aseguren la continuidad y la recuperación de las operaciones. [25]

Se propone medidas que permitan la implementación de políticas de seguridad y control, para lo cual la Figura 3 presenta un esquema con la siguiente estructura:

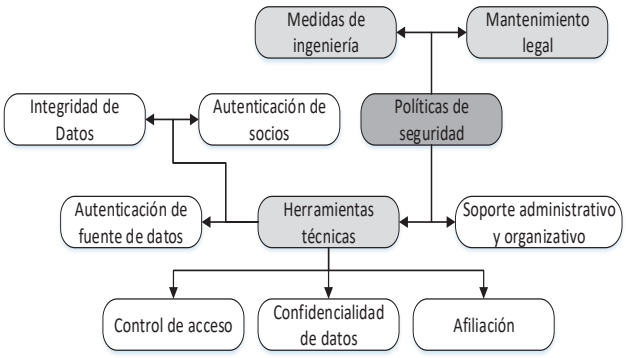

Figura 3. Estructura de la política de seguridad [25]

Se recomienda que la estrategia de protección planteada debe ser revisada y actualizada frecuentemente. Las funcionalidades de las herramientas tecnológicas no garantizan la completa protección ante ataques desde la red interna, a fin de optimizar la protección de la misma es necesario la utilización de sistemas de detección de intrusos y un monitoreo activo de las actividades de los equipos terminales, este enfoque integral contribuye significativamente en el nivel de seguridad.

A fin de hacer frente a la cada vez más creciente y sofisticada cantidad de amenazas y ciberataques, se con-

sidera tener información respecto a vulnerabilidades, ataques, amenazas, entre otros. Sauerwein et al. (2019) conlleva un estudio de triangulación con el propósito de identificar y analizar las fuentes de datos de seguridad de la información pública. Se presenta una taxonomía de comparación y clasificación en seis dimensiones: (1) Tipo de información, (2) Integridad, (3) oportunidad, (4) Originalidad, (5) Tipo de fuente, (6) Confiabilidad. Se concluye que la gran variedad de fuentes de datos de seguridad de la información dificulta tanto la integración como el uso para la adecuada gestión de riesgos. [26]

3.2. Modelos de Gestión de Riesgos

A continuación, se presentan diversos estudios que plantean modelos, marcos, metodologías y procedimientos para gestionar los riesgos, a fin de que puedan servir como guía, tanto del proceso constructivo, así como brindar una referencia de los elementos, módulos, y demás aspectos comprendidos en su desarrollo. Se identifica aspectos relevantes de los mismos, que puedan contribuir a la formulación de modelos, alineados a las características y requerimientos particulares de una organización.

Practical Application of Information Security Models. [27]

El estudio desarrolla un marco de seguridad GRC (Government, Risk and Compliance) partiendo de la interrogante; ¿Por qué es importante la seguridad? Y lo costoso que puede llegar a ser la inversión tecnológica a implementar. Teniendo al cumplimiento de los objetivos del negocio y el establecimiento de políticas de alto nivel, como uno de sus enfoques principales. Recomienda que la ejecución del modelo debe ser responsabilidad del encargado de Seguridad de la Información (CISO), teniendo una supervisión y aceptación de la alta dirección.

El modelo que propone, plantea una gestión de seguridad, comprendido por tres marcos:

– Marco de políticas, que define los controles de seguridad considerando políticas, estándares y artefactos.

– Marco de procesos, el cual ejecutará los controles definidos en el módulo anterior, enfocándose en procesos de SI, personas y tecnología.

– Marco de métricas el cual permitirá medir la madurez de los controles de seguridad.

El estudio realiza una correlación entre los objetivos del negocio con los procesos de seguridad; lo cual permite alinear los objetivos de seguridad, a los objetivos que persigue la alta dirección.

A Framework for Risk Assessment [18]

Esta investigación es realizada en el ámbito del desarrollo de proyectos gestionados con presupuesto público, presenta un marco de evaluación de riesgos para abordar los múltiples objetivos de la reducción del riesgo de desastres, coherente con la planificación del desarrollo social y económico, considerando que, la base legal para las políticas de reducción de riesgos es esencial en la toma de decisiones de manera transparente, así como la asignación de fondos públicos para la mitigación de desastres.

(S. Proag & V. Proag, 2014) presentan un enfoque orientado a la continuidad del negocio, llevado a cabo en tres niveles o periodos diferentes, que contempla el ciclo de una gestión de riesgos el cual es clasificado por estadios, según lo indicado en la Tabla 1.

Tabla 1. *Ciclo de Gestión de Riesgos*

PERIODO	MEDIDAS
Antes del desastre	Técnicas de prevision.
	Técnicas de monitoreo.
	Advertencia.
	Estrategias de reducción de riesgos.
	Simulación, simulacros.
Durante el evento	Reducir la magnitud del desastre.
	Gestión del tiempo.
	Herramientas de gestión de crisis.
	Geografía de la gestión de crisis.
Después del desastre	Evaluar los impactos.
	Compensación/alivio.
	Principios de reconstrucción.

Fuente: S. Proag & V. Proag [18]

Metodología para la seguridad de tecnologías de información en la Clínica Ortega [28]

Guzmán (2015) se enfoca su investigación en función a la interrogante: "¿Cómo definir un modelo de metodología de seguridad de tecnologías de información y comunicaciones que permita mejorar la seguridad en la protección y continuidad de procesos de una clínica de salud?" (p. 8). El objetivo de la investigación es estimar el nivel de relevancia de los asuntos pertinentes a la seguridad de la información y cómo influyen en la continuidad de los servicios ofrecidos por la organización. Para lo cual se realiza una investigación de tipo cualitativa con enfoque cuantitativo, se realiza una recolección de datos mediante entrevistas, encuestas, consultas y observación.

El estudio permitió conocer las amenazas a los cuales se encuentran expuestas los activos de información, tanto internas como externas, se propone una serie de controles por cada área de la organización a fin de brindar una correcta protección de los activos de información y se plantean procesos de implantación de controles, tratamiento, así como un monitoreo y evaluaciones periódicas, con el propósito de validar la efectividad de los controles establecidos.

La Investigación considera el ciclo Deming (PDCA - Plan, Do, Check, Act) aplicado a la norma ISO 27005,

para así plantear la gestión riesgo, tal como muestra la Tabla 2.

Tabla 2. *Ciclo Deming considerando la ISO 27005*

Ciclo PDCA	Proceso de Gestión de riesgo
Plan	Establecimiento del contexto. Identificación y evaluación de riesgos. Plan de tratamiento de riesgos. Aceptación de riesgos.
Do	Implementación de los controles y del plan de tratamiento de riesgos.
Check	Monitoreo y revisión continua de riesgos y del plan. (métricas, análisis, etc.).
Act	Mantenimiento y mejora del proceso.

Fuente: Guzman, Goyo [28]

Evaluating risk management practices in construction organizations [29]

El estudio desarrolla un marco que permite medir la capacidad de una organización de construcción para realizar la gestión de riesgos de manera efectiva. Este instrumento se ha aplicado tanto a clientes como a contratistas y forma parte de un sistema de conocimiento general. Los resultados de esta investigación permitirán primero a un cliente o contratista, desarrollar su capacidad de gestión de riesgos de proyectos basada en las mejores prácticas internacionales y, en segundo lugar, mejorar continuamente el rendimiento de esta función a lo largo de la realización de nuevos proyectos. La novedad de este enfoque es que aborda la función de gestión de riesgos desde una perspectiva basada en el conocimiento y que se basará en una aplicación web que estará disponible para todas las organizaciones.

La investigación se llevó a cabo con el apoyo financiero de una agencia gubernamental. La metodología de investigación ha involucrado cinco etapas hasta el momento, de la siguiente manera:

a. Una revisión exhaustiva de la literatura para comprender cómo se lleva a cabo la gestión del riesgo.

b. La construcción de un modelo preliminar a partir de la literatura existente.

c. Validación del modelo a través de la participación de paneles de expertos.

d. Construcción del instrumento para la medir el nivel de madurez alcanzado.

e. La validación del instrumento para evaluar la madurez de la gestión de riesgos.

Implementation of a Risk Management Plan in a Hospital Operating Room [30]

Guo (2015) presenta un plan que permite gestionar los riesgos de la sala de operaciones de uno de los hospitales más grande de Beijin – China. Para lograr este propósito se aplicó el proceso de gestión de riesgos descrito en AS / NZS 4360 a las funciones realizadas en el quirófano, y después de consultar con la administración de la sala de operaciones sobre sus componentes individuales, se presenta el plan para dicho quirófano, el cual consiste de los siguientes pasos:

– Establecer el ambiente

– Establecer el ámbito estratégico.

– Estableciendo el ámbito organizacional.

– Estableciendo el principio de gestión de riesgos.

– Establecer un sistema de responsabilidad de gestión de riesgos, así como un sistema de recompensas y castigos.

– Establecer sistemas estandarizados para la evaluación e identificación de riesgos.

– Identificación, análisis y evaluación de riesgos

– Eliminación de riesgos

– Establecer un mecanismo de comunicación y consulta

– Establecer un mecanismo de monitoreo y evaluación

La combinación de las normas de gestión con los procedimiento e instrucciones del hospital identifican 9 tipos distintos de riesgos:

– Riesgo de gestión

– Riesgo ambiental

– Riesgo de seguridad del paciente

– Riesgo de Tecnología

– Riesgo de los recursos humanos

– Riesgo de infección

– Riesgo de seguridad ocupacional

– Riesgo legal

– Riesgo de reputación

Los cuales se dividen en 4 niveles según su probabilidad de ocurrencia y la gravedad de sus consecuencias:

– Riesgo bajo

– Riesgo moderado

– Riesgo alto

– Riesgo extremo

Así como 3 categorías que consisten en:

– Aceptable

– Reducible

– Inaceptable

Los pasos mencionados, permite la elaboración de un marco de gestión de riesgos para la sala de operaciones del mencionado hospital.

Modelo de gestión de seguridad de la información para el E-Gobierno [3]

Mercado (2016) Propone un modelo de gestión a manera de un SGSI, con énfasis en gobierno electrónico, utiliza una estructura y aspectos organizacionales los cuales permiten la implementación y gestión de acuerdo con las fases establecidas, así como la identificación del nivel de madurez. Se contempla el monitoreo y seguimiento a fin de validar los niveles de seguridad propuestos por medio de la verificación de los controles e índices establecidos.

El modelo permite la identificación de 05 niveles de madurez, implementa 114 controles de acuerdo a estos niveles, que van en un rango de 0 a 5 niveles siendo 30 el inicial y 114 el nivel 5; asimismo establece la obligatoriedad de 10 documentos para los 05 niveles.

Para la implementación del modelo, propone una secuencia de 04 fases con 06 indicadores, a fin de estimar el grado de cumplimiento de los mismos (Ver Figura 4).

El modelo presentado contempla tanto los procesos de análisis, así como de evaluación de riesgos y contribuye al cumplimiento de la ISO/IEC 27001, contribuyendo al SGSI, enfocándose en gestionar los procesos pertenecientes a actividades de E-Gobierno

El estudio no considera la agregación de nuevos elementos que cambien el escenario o afecten los procesos propios del Gobierno Electrónico y una de sus recomendaciones es definir nuevos modelos para empresas soportadas en tecnologías de Cloud Computing.

Introducing OSSF: A Framework for Online Service Cybersecurity Risk Management [31]

La investigación contribuye con la elaboración de un nuevo marco de gestión de servicios en línea. Comprende un modelo de amenazas y un modelo de riesgo, los cuales pueden personalizarse a las características propias de los servicios y entornos del ciberespacio.

Para el desarrollo del marco propuesto se utilizó la metodología de Investigación de la Ciencia del Diseño publicada por Peffers et al. (2007). el cual establece un artefacto consistente en un proceso de seis actividades:

– Identificación y motivación del problema.

– Definir los objetivos para la solución.

– Diseño y desarrollo del artefacto.

– Demostración que comprende el uso del artefacto para resolver una o más instancias del problema.

– Observación, evaluación y medición de la operatividad del artefacto.

– Comunicación del problema, su importancia y el artefacto propuesto.

Port Risk Management in Container Terminals [32]

La investigación emplea la Evaluación Formal de Seguridad - Formal Safety Assessment (FSA) que es un proceso proactivo introducido por la Organización Marítima Internacional (OMI).

La FSA debe usarse como una herramienta en el proceso de reglamentación, es "una forma de garantizar que se tomen medidas antes de que ocurra un desastre". La FSA preferiblemente aborda una categoría específica de nave o área de navegación, pero también se puede aplicar a un problema específico de seguridad marítima para identificar opciones de reducción de riesgos efectivas en función de los costos.

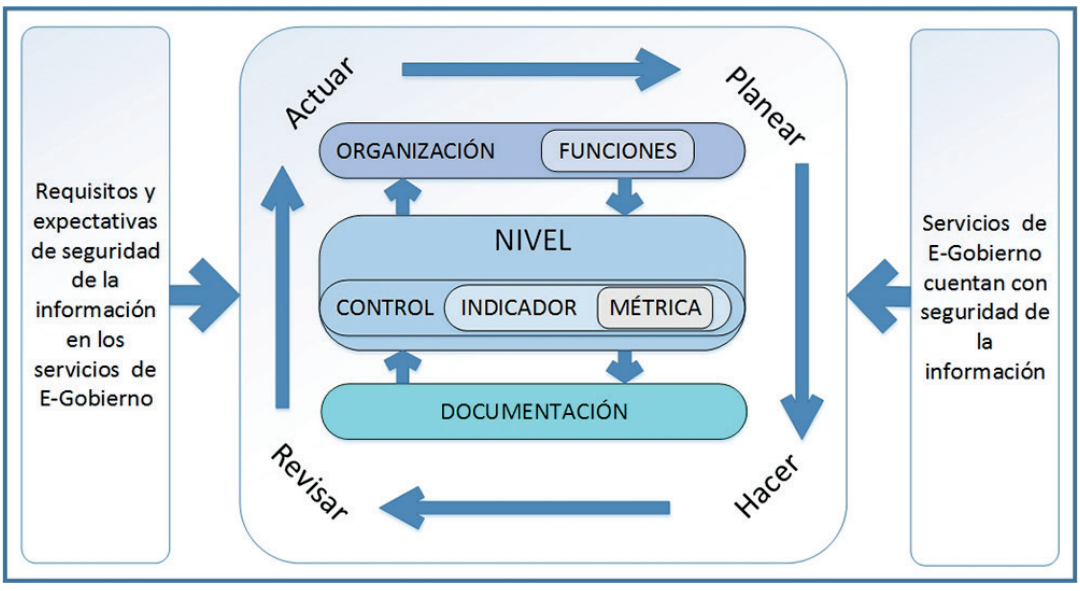

Figura 4. Modelo de gestión de SI para el E-Gobierno [3]

La técnica de identificación de riesgos es una combinación de la metodología HAZOP y SWIFT que utiliza la literatura existente y la experiencia de los profesionales para enfocarse en los riesgos asociados con el sistema especializado de puertos y terminales de contenedores. La evaluación del riesgo se realiza de manera cuantitativa y cualitativamente mediante el uso de una matriz de riesgos en la que las filas representan la severidad creciente de las consecuencias de un riesgo liberado y las columnas representan la creciente probabilidad o frecuencia de estas consecuencias. La matriz indica las combinaciones de probabilidad y consecuencia, y genera tres regiones distintas: Riesgo aceptable, Medidas de reducción y Riesgos Inaceptables.

La metodología propuesta de evaluación de riesgos portuarios, construye su estructura y funcionalidad de acuerdo con la Evaluación de seguridad formal (FSA) y se adapta mediante la utilización de la opinión experta del puerto y la literatura existente para adaptar su aplicabilidad dentro del dominio del puerto.

Effects of Risk Management Practice on the Success of IT Project [24]

La investigación es orientada en medir el grado en que una adecuada gestión de riesgos, logra impactar en proyectos de TI exitosos, incluye una revisión de la literatura, cuestionarios y análisis estadísticos, tanto descriptivos como inferenciales. Se resalta la forma en la que se emplea el cuestionario, el cual fue adoptado como un medio para recopilar datos confiables y cuantificables. La población objetivo consistió en gerentes de proyecto, gerentes de TI y analistas de TI de empresas de TI en Tailandia y la muestra se obtuvo del método de muestreo de conveniencia.

Se tomó como a 200 personas a quienes se realizó cuestionarios de investigación

Los cuestionarios fueron categorizados en 3 partes:

Primera parte: hubo 2 preguntas sobre los tipos y tamaños de la organización y fueron preguntas de la lista de verificación.

Segunda parte: 12 preguntas sobre las prácticas de gestión de riesgos de la siguiente manera: identificación, análisis, planificación, monitoreo y control de riesgos.

Tercera parte: 10 preguntas sobre el rendimiento del proceso que involucraron el presupuesto, tiempo y el rendimiento del producto que involucraron los requisitos del proyecto.

El estudio incluye un marco de investigación, que se desarrolla para explorar el efecto de los factores organizacionales y las actividades relacionadas al manejo de riesgos, y cómo influyen en el éxito de los proyectos de TI, como se presenta en la Figura 5. El modelo implica la utilización de dos variables independientes y una variable dependiente. Las variables independientes son factores organizacionales y prácticas de gestión de riesgos. La variable dependiente es el éxito del proyecto de TI que incluye las dimensiones de rendimiento particulares de la organización.

Figura 5. Marco de investigación desarrollado [24]

Implementación de la administración de riesgos en el sistema de control interno del Ministerio de Justicia y Derechos Humanos de Perú (*MINJUSDH*) [33]

El estudio está orientado al sector Público (MINJUSDH) y considera el establecimiento de lineamientos y acciones que permitan la implementación de la gestión de riesgos con respecto a las entidades públicas, lo cual considera fundamental para el sistema de Control Interno de dicha institución, resalta la rotación del personal directivo como un desafío para la implementación del proceso de administración del riesgo.

El estudio indica que una adecuada gestión de riesgos sobrepasa el solo hecho de implementar de una matriz de riesgos y propone la implementación de un modelo bajo tres elementos fundamentales: (Figura 6)

– Elemento Gestión del Conocimiento para la Gestión Integral de Riesgos – GIR

– Elemento Estructura Organizativa Adecuada para la Implementación de la GIR

– Elemento Comité de Control Interno.

Figura 6. Implementación de la Administración de Riesgos [33]

Los procesos de implementación requieren la implementación de manera progresiva, considerando el

impacto que pueda tener en la organización. Considera la resistencia al cambio como elemento importante a considerar por tratarse de una entidad del estado, siendo en éste sector más fuerte.

Este modelo puede ayudar a otras instituciones del estado a fin de lograr la adecuada implementación de la gestión de riesgos y sirva de soporte a la puesta en marcha de su sistema de control interno, coadyuvando a que las instituciones públicas puedan realizar una administración eficaz y luchar contra la corrupción.

Gestión de Riesgos de Tecnologías de la Información de las empresas de Nephila Networks [34]

La investigación se enfoca en estimar la eficiencia de la gobernanza respecto a los riesgos de TI. Se tiene como como uno de los objetivos principales medir el nivel de eficiencia del tratamiento de los riesgos de TI, para lo cual se tomó como población 21 empresas que fueron catalogadas como empresas de servicio y comerciales.

Llontop (2018) plantea su investigación considerando 3 dimensiones particulares:

– Proceso de gobernanza del riesgo.
– Concientización sobre riesgos.
– Implantación eficaz de TI.

El modelo que propone, considera las tres dimensiones definidas anteriormente y plantea un conjunto de controles contemplados en 4 fases:

– Análisis de riesgos.
– Clasificación de riesgos.
– Implementación de controles.
– Evaluación de controles.

Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas [35]

El estudio considera los escenarios en el que se circunscriben muchas Pymes, lo cual no hacen factible la aplicación de soluciones de SI, por no estar consideradas dentro de su presupuesto y por ser prioritario, (en función del grado de producción) para dichas organizaciones la implementación de estas soluciones. El presente estudio desarrolla un modelo enfocado en dichas Pymes, realizando una armonización de una metodología con una norma de gestión de riesgos.

El modelo que propone ayuda a identificar los activos de información con que cuenta una organización, así como los riesgos inherentes a estos, cuantificando el valor de los riesgos presentados y permitiendo entender las causas de las vulnerabilidades y su riesgo residual en función de los controles establecidos.

El modelo desarrollado contempla las tres fases de la metodología OCTAVE-S:

– Elaboración de perfil de amenazas.
– Identificación de vulnerabilidades en la infraestructura.
– Planes de seguridad.

Los mismos que son complementados con los procesos pertenecientes a la norma ISO 27005, esto genera un modelo desarrollado por fases, a manera de diagrama, el cual resulta de fácil comprensión y facilita la implementación de una adecuada gestión de riesgos, según las circunstancias particulares de las Pymes, la Figura 7 muestra las fases centrales que comprenden el modelo presentado.

A novel security media cloud framework [36]

La investigación se enfoca en las amenazas de seguridad a las que se enfrentan los servicios brindados en la nube, se parte de la premisa que dichos desafíos provienen principalmente de dos aspectos: los problemas de seguridad de datos y los riesgos de seguridad causados por la computación en la nube.

El estudio de la literatura tiene como objetivo tomar los aspectos de seguridad en la nube ya cubiertos y complementar los aspectos no cubiertos como la seguridad de almacenamiento y control de acceso. Se desarrolla Modelo de amenaza en Diagrama de Flujo de Datos (DFD) y en Diagrama de Flujo de Proceso (DFP) El modelo indica que, al margen de la arquitectura del operador, las amenazas de robo y fuga se producirá en el proceso de prestación de servicios a los usuarios.

Como propuesta de mejora de la seguridad de la plataforma de computación en la nube, se presenta un modelo que consta de dos partes: Un marco de medios seguros en la nube y un protocolo de control de acceso.

El desarrollo metodológico implica un mecanismo de encriptación para fortalecer la seguridad. El estudio concluye que un medio seguro de computación en la nube deberá cumplir tres requisitos fundamentales:

– Entorno de nube seguro.
– Seguridad en el almacenamiento de contenido.
– Control de acceso seguro.

Information security governance in big data environments: A systematic mapping [37]

La investigación brinda un modelo útil a profesionales de seguridad de TI y especialistas en sistemas de información para cubrir entornos de Big Data. Para conocer los aspectos de interrelación del Big Data con el gobierno de TI, se realiza un mapeo sistemático y una clasificación de los entornos en los que se desarrolla.

Moghadama et al. (2018) proponen un importante aporte, llamado "método de mapeo sistemático" que se presenta en la figura 8, el cual es una técnica consistente en pasos sistemáticos del proceso de mapping con el propósito de brindar una visión global del tema a investigar.

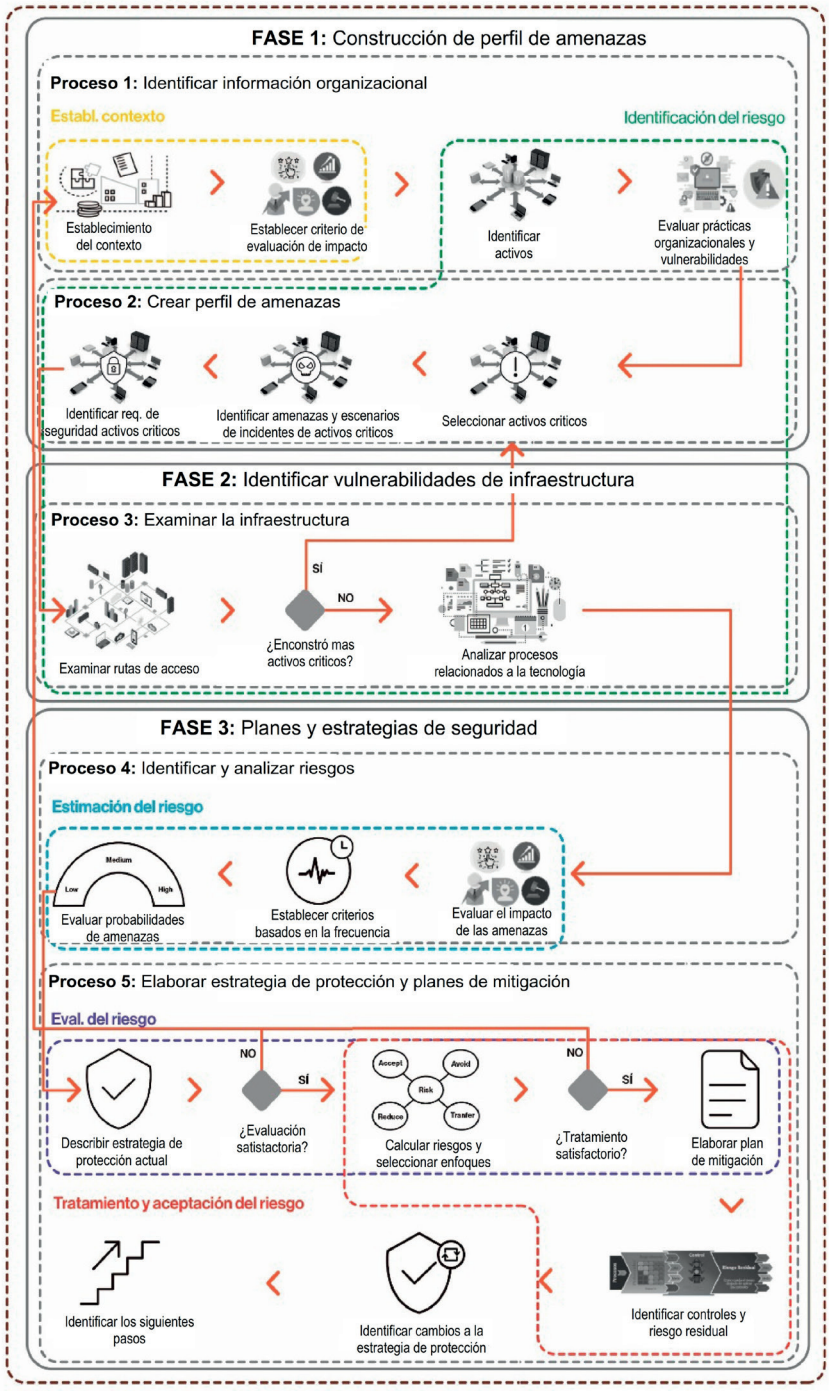

Figura 7. Modelo de Gestión de Riesgos orientado a Pymes [35]

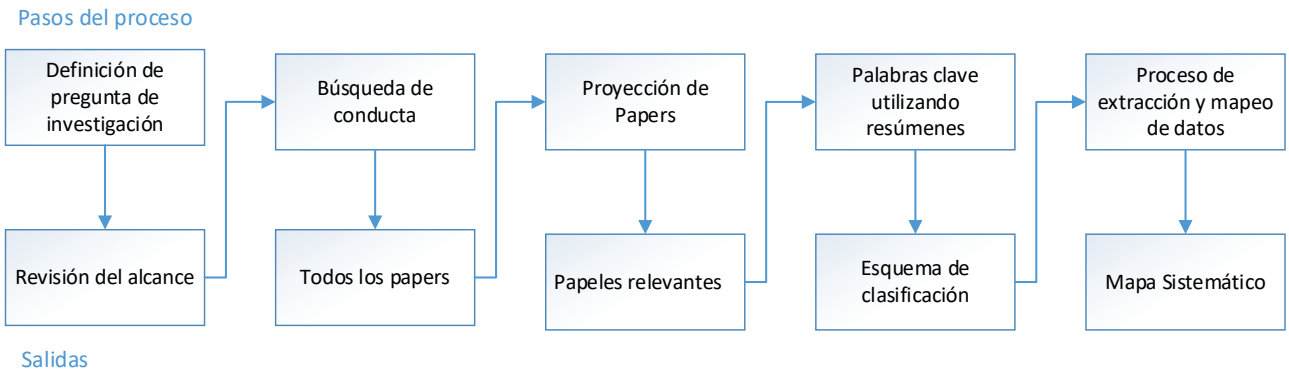

Figura 8. Diagrama de Mapeo Sistemático [37]

Este estudio abarca aspectos de la gobernanza de la SI en Big Data, realizando una revisión de la literatura al respecto. Analiza las aristas de riesgos encontrados en la literatura. Realiza una identificación de los problemas de gobierno de TI, así como de las herramientas, modelos y marcos existentes al respecto.

Mediante un enfoque sistemático se brinda una visión general de la gobernanza en entornos de Big Data. Considera que es necesario un monitoreo permanente con respecto a los procesos para lograr un adecuado gobierno de SI.

El estudio muestra la carencia de investigaciones respecto a la regulación y cumplimiento de la gobernanza de SI sobre todo en entornos de Big Data. así como la ausencia de modelos y marcos integrales y específicos en esta área.

4. Analisis de Tecnicas Revisadas

De acuerdo a la literatura revisada se identifican diversos elementos, procesos y actividades comunes durante el proceso de desarrollo de modelos de gestión de riesgos, los cuales son presentados a continuación, como una guía referencial en el desarrollo de los mismos, teniendo una orientación a la seguridad de la información.

4.1. Desarrollo de Modelos de Gestión de Riesgos de Seguridad de la Información. (MGRSI)

Un modelo de gestión de riesgo, contribuye a la organización en la identificación de sus activos de información con que cuente, así mismo conocer los riesgos inherentes a ellos. Además, permite establecer métricas que permitan medir cuantitativamente el valor del riesgo, conocer las vulnerabilidades, así como establecer controles necesarios que permitan proteger dichos activos de ataques o amenazas de seguridad y establecer controles que permitan hacer frente a los riesgos que se presenten.

El desarrollo de los modelos personalizados de gestión de riesgo, se apoya en normas y/o metodologías de gestión, como: la ISO 31000, ISO 27005, Magerit, COSO, etc. Los modelos de gestión de riesgos analizados se caracterizan por tener algunos procesos comunes como:

- Establecimiento del contexto.
- Definición de alcance.
- Identificación de activos.
- Identificación, análisis y evaluación de riesgos.
- Declaración de Aplicabilidad.
- Tratamiento de riesgos.
- Revisión del cumplimiento.
- Medición (Medir eficacia de controles)
- Acciones correctivas.
- Registro e informe.
- Monitoreo, seguimiento y revisión.
- Comunicación y consulta.

4.2. Procesos del Modelos

A continuación, se describen los procesos identificados que formarían parte del desarrollo de un MGRSI.

4.2.1. Establecimiento del contexto

Una adecuada gestión de riesgos toma como una línea base, la determinación y definición de los objetivos de la organización. [38] Por lo que en esta fase se definen los criterios básicos a fin de dar cumplimento a dichos objetivos. Es necesario considerar que la gestión del riesgo debe ser capaz de integrarse con el contexto de la organización, tan interno como externo. Esto conlleva definir las condiciones internas como externas que establecerá el marco de gestión de riesgo.

En el ámbito interno se considera:

- La cultura organizacional.
- Recursos de la organización.
- Procesos y objetivos organizacionales.

En el ámbito externo es necesario considerar aspectos sociales, políticos, económicos, legislativos entre otros. Teniendo en cuenta la interacción de estos elementos con la organización, se establece la Política de Seguridad, la cual registrará con claridad los objetivos perseguidos respecto a la gestión del riesgo, criterios de evaluación de riesgo, métodos a utilizar en la evaluación del riesgo. [7]

4.2.2. Definición del alcance

Se debe establecer claramente los límites y el grado de aplicabilidad del MGRSI con el propósito de establecer su alcance. [6]

Al realizar este proceso se debe de considerar: aspectos externos e internos, partes interesadas y los requisitos de las, interfaces y dependencias entre actividades, sean o no de la organización. Por requisito de la norma ISO/IEC 27001, se debe documentar dicho alcance. [6]

4.2.3. Identificación de activos

Se considera activos de información a todo componente, funcionalidad o recurso que tenga valor para la organización, [6] los cuales permitan almacenar en cualquier medida información perteneciente a los procesos organizacionales y contribuyan a que la organización alcance sus objetivos, los mismos que están expuestos a distintos riesgos de seguridad.

La identificación de los activos genera un inventario, el cual permite clasificarlos a fin de brindar mayor o menor protección, dependiendo del grado de criticidad para la organización, esto se logra identificando claramente sus características y rol en los procesos. [39]

4.2.4. Identificación de Riesgos

La identificación de riesgos se realiza con posterioridad a la identificación de los activos, en el que se han de conocer las amenazas y vulnerabilidades a las que éstas están expuestas y que pueden explotarse a fin de causar daño. Esta identificación de los riesgos puede obtenerse por medio de entrevistas a los propietarios de los activos, usuario, expertos, etc.

4.2.5. Análisis de riesgos

El propósito del análisis del riesgo, es el de determinar una apreciación y priorización de cada uno de los riesgos, en función al conocimiento obtenido durante el proceso previo de identificación, con el propósito de determinar el nivel de riesgo y las actividades a implementar como medidas de respuesta. [40]

Esta etapa proporcionará información sobre los peligros y riesgos presentes en los procesos y servicios que presta la organización con respecto al tratamiento de información que realiza, sobre los cuales se tiene influencia y puedan controlarse, con la finalidad de prevenir daños; comprende la identificación, selección, aprobación e implementación de controles a establecer para eliminar o disminuir los riesgos evaluados a niveles aceptables por la organización. Estas acciones nos llevan a:

– Reducir la ocurrencia de amenazas.

– Limitar el impacto de las amenazas.

– Reducir o eliminar vulnerabilidades detectadas.

– Posibilitar la recuperación del impacto producido o gestionar la transferencia del riesgo.

4.2.6. Estimación de riesgos

Implica la clasificación de los riesgos en función del impacto hacia la organización, para lo cual la organización podrá considerar acciones como:

Evitar: Impedir la materialización del riesgo.

Reducir: Cuando no es posible evitar el riesgo, se considera reducirlo hasta que pueda ser aceptable.

Transferir/Compartir: Se considera la transferencia de los riesgos a aseguradoras, proveedores, etc.

Aceptar: Aceptación de los riesgos de manera clara y objetiva, siempre que satisfaga la política y los criterios establecidos por la organización.

La tabla 3 presenta una estimación de valor, donde los riesgos se miden en términos de su impacto y probabilidad de ocurrencia, realizando una asignación de valores a fin de poder estimarlos adecuadamente:

Tabla 3. *Medición de impacto y probabilidad*

Probabilidad/ Impacto	Valorización
Muy Alto	5
Alto	4
Moderado	3
Bajo	2
Muy Bajo	1

Fuente: Elaboración propia

Para la valoración de riesgos se toman como base dos variables: el impacto que produzca en caso se materialice, así como la probabilidad de ocurrencia.

4.2.6.1. Probabilidad de ocurrencia

Se define considerando los criterios descritos en la tabla 4.

Tabla 4. *Probabilidad de ocurrencia*

Niveles de Probabilidad		Descripción
5	**Muy alta**	Riesgo cuya materialización es recurrente (Casi seguro).
4	**Alta**	Riesgo que puede materializarse de manera habitual (Probable).
3	**Moderada**	Riesgo que se presenta de forma casual o accidental (Posible).
2	**Baja**	Riesgo que puede presentarse de manera eventual (Raro).
1	**Muy baja**	Riesgo cuya probabilidad de materializarse es mínima (Improbable).

Fuente: Elaboración propia

4.2.6.2. Impacto

La valoración del impacto se realiza sobre los principios del SGSI:

Confidencialidad: Mide cómo impactaría a la organización, la pérdida de confidencialidad de los activos de información, considerando el supuesto escenario que sean conocidos por personal no autorizado.

Integridad: Mide cómo impactaría la pérdida de integridad, considerando la alteración o manipulación de los métodos de procesamiento que pueda reflejar inexactitud o un estado incompleto de los activos de información.

Disponibilidad: Mide el impacto que tendría la pérdida de disponibilidad, considerando el escenario en que los usuarios requieran acceder a los activos de información y no pudieran, pese a estar autorizados.

El impacto se representa de acuerdo a los niveles expresados en la Tabla 5.

Tabla 5. *Valoración del Impacto*

NIVEL	CONCEPTO	DESCRIPCIÓN	SEGURIDAD DE LA INFORMACIÓN
1	**Muy Bajo**	Suscitado el evento, las consecuencias serían mínimas.	Influye en una actividad del proceso.
2	**Bajo**	Suscitado el evento, presentaría bajo efecto o impacto.	Compromete a una persona, grupo de personas o actividades del proceso.
3	**Moderado**	Suscitado el evento, ocasionaría medianos efectos o consecuencias respecto a la organización.	Compromete a un conjunto de datos personales o al mismo proceso.
4	**Alto**	Suscitado el evento tendría altos efectos o consecuencias respecto a la organización.	Compromete a varios conjuntos de datos personales o procesos.
5	**Muy Alto**	Suscitado el evento tendría desastrosos efectos o consecuencias respecto a la organización.	Compromete a toda la organización. Implicando aún la suspensión de sus actividades.

Fuente: Elaboración propia

4.2.6.3. Niveles de Riesgo

Con base en la estimación del impacto y su probabilidad de ocurrencia, que cada riesgo represente para la organización, se establecen los niveles de riesgos, según se aprecia en la Tabla 6 (donde R = Riesgo).

Tabla 6. *Nivel de Riesgo*

NIVEL DE RIESGO	VALOR	ACCIÓN PROPUESTA
Riesgo Extremo	[R >16]	Evitar el riesgo por medio de medidas orientadas a reducir la probabilidad de ocurrencia, y/o disminuir el impacto, considerar acciones orientadas a compartir el riesgo.
Riesgo Alto	[9 < R ≤16]	Evitar o mitigar el riesgo por medio de recursos adecuados que conduzcan a un estado moderado, considerar acciones orientadas a compartir el riesgo.
Riesgo Moderado	[4 < R ≤ 9]	Limitar el impacto del riesgo con medidas prontas y apropiadas a fin de disminuir el nivel de riesgo.
Riesgo Bajo	[2 < R ≤ 4]	El evento tendrá efectos e impactos menores que pueden ser asumidos, se realiza acciones de mitigación con actividades ya definidas tanto detectivas como preventivas.
Riesgo Muy Bajo	[R ≤ 2]	Riesgo Aceptable. No se requiere ninguna acción

Fuente: Elaboración propia

De acuerdo a la evaluación que se realice, los riesgos se distribuyen en la matriz de calor presentada en la figura 9.

4.2.7. Declaración de Aplicabilidad

Declaración documentada (Statement of Applicability) tiene como propósito mantener y describir un registro y control de las medidas de seguridad establecidas que sean relevantes y aplicables a la organización con respecto al SGSI. [6] Los controles y objetivos de control se fundamentan en función de:

– Los resultados y conclusiones de los procesos de evaluación y tratamiento.

– Los requisitos reglamentarios.

– Los compromisos contractuales.

– Las exigencias comerciales.

4.2.8. Tratamiento del riesgo

Consiste en la selección y aplicación de las medidas adecuadas, teniendo el propósito de minimizar el riesgo a fin de evitar daños asociados al factor de riesgo o aprovechar las ventajas presentadas. [5]

Se debe establecer los parámetros apropiados para definir el proceso de tratamiento, dependiendo del tipo de riesgo, a fin de considerar el tipo de tratamiento que se dará. Los planes de acción resultantes se aterrizan en hojas de ruta para aproximar el riesgo a un estado que pueda ser aceptable, aquellos a los que no aplique dicha estrategia, deberán ser articulados por medio de planes de continuidad, considerando que no serían viables la aplicación de medidas preventivas.

4.2.9. Revisión del cumplimiento

Las amenazas planteadas a los activos de los sistemas de información no son estáticas; están cambiando constantemente dentro de un entorno muy dinámico e interrelacionado con otros factores implícitos o no a la organización. Esto exige una revisión y una publicación constante de las políticas, metodologías y procedimientos de a seguir, y la seguridad de que el personal de operaciones los está utilizando. [41] Estas consideraciones implican escenarios en el que surjan cambios normativos, procedimentales o la irrupción de nuevas tecnologías, las cuales deben de ser consideradas para validarlas en el modelo de gestión.

4.2.10. Medición de eficacia de controles

Este control está orientado a determinar el nivel de eficacia, eficiencia y efectividad de los componentes de implementación y gestión definidos por el modelo propuesto o desarrollado. [42]

Tiene como objetivos:

– Evaluar Efectividad de los controles implementados.

– Evaluar la eficiencia del modelo internamente.

– Servir de aporte al plan de análisis y tratamiento de riesgos.

Para la evaluación de la efectividad del control, se recurre a la evolución del escenario de riesgo, para lo cual los riesgos que se consideren significativos se les diseña indicadores claves de riesgos, que permitirá realizar el seguimiento de la evolución de los riesgos más significativos.

4.2.11. Acciones correctivas

Las acciones correctivas arreglan la brecha existente entre la expectativa y la práctica. Estos esfuerzos correctivos deben de estar documentados a fin de respaldar iniciativas de mejora continua, Se debe de considerar el uso de un registro continuo a fin de identificar, ejecutar, rastrear y reevaluar para garantizar que se lleva a cabo la intención de la acción correctiva, debe de considerarse la interacción con otras políticas de la organización, recursos disponibles, y una revisión periódica tanto de las políticas establecidas como de propio método de trabajo. [41]

Esta etapa comprende la aplicación de acciones correctivas y preventivas identificadas en la Revisión de cumplimiento y la medición de la eficacia de los controles.

4.2.12. Registro e informe

El programa de implementación considera los niveles de riesgo asignados para los diferentes activos y las medidas de protección, salvaguardas o actividades a realizar, y en función del impacto que representa la amenaza establece planes de acción para la implementación de las mismas, en las que se considerará recursos, tiempo, materiales, etc. Todas estas actividades deben de ser registradas adecuadamente y ser informadas a las partes interesadas.

4.2.13. Monitoreo, seguimiento y revisión

Determina la efectividad de las actividades realizadas, se debe de realizar periódicamente utilizando distintas estrategias como: revisión de alta dirección, auditorías internas y externas, monitoreo de controles puntuales, medición del desempeño, reporte de gestión, rendición de cuentas, etc.

Se debe de tener claro los conceptos de la gestión de riesgos, en la Figura 10 se muestra una descripción general de los conceptos utilizando el método de la corbata de lazo descrito por Hopkin, [43] el cual permite conocer las relaciones entre los eventos, sus detonantes y consecuencias, describiendo el escenario de riesgo a fin de establecer un marco que permita registrar el programa a implementar y su correspondiente informe.

4.2.14. Comunicación y consulta

Este proceso involucra a todos los demás procesos del MGRSI. Es imprescindible puesto que permite asegurar el entendimiento de las diferentes partes que interactúan en la gestión de riesgo.

Las partes interesadas deberá comunicar respecto a sus funciones y responsabilidades, así como los resultados de sus actividades, debiendo esto ser comunicado a la alta dirección a fin de contribuir con la toma de decisiones.

4.3. Comparación de elementos identificados

Teniendo en consideración los procesos identificados como elementos de un modelo de gestión de riesgos, se realiza una comparación con los diversos modelos estudiados para estimar similitudes con respecto a los mismos consignando (N) si el elemento no es considerado en el modelo planteado, (W) si existe una similitud débil, (P) si

PROBABILIDAD	IMPACTO				
	Muy Baja	Baja	Moderada	Alta	Muy Alta
Muy alta	5	10	15	20	25
Alta	4	8	12	16	20
Moderada	3	6	9	12	15
Baja	2	4	6	8	10
Muy Baja	1	2	3	4	5

Figura 9. Matriz de calor – Fuente: elaboración propia

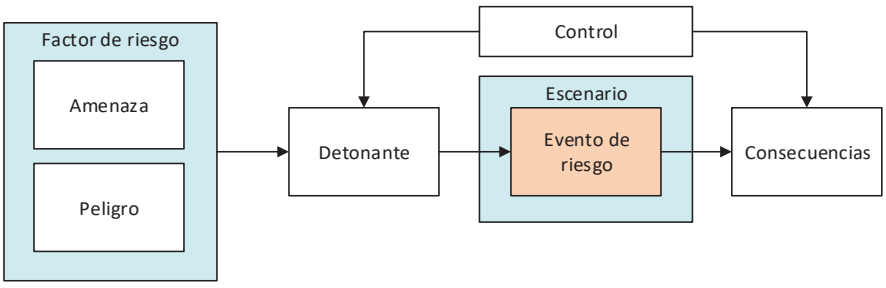

Figura 10. Programa de implementación [43]

se encuentra una similitud parcial y (S) si existe una fuerte relación del elemento en el modelo planteado.

Tabla 7. *Comparación de elementos por modelos descritos*

	Establecimiento del contexto	Definición de alcance	Identificación de activos	Identificación de riesgos	Análisis de riesgos	Estimación del riesgo	Declaración de Aplicabilidad	Tratamiento del riesgo	Revisión del cumplimiento	Medición de eficacia de controles	Acciones correctivas	Registro e informe	Monitoreo y revisión.	Comunicación y consulta
[3]	P	S	S	S	S	S	S	S	W	P	S	S	S	S
[15]	P	P	S	S	S	S	W	P	S	W	S	P	S	P
[18]	S	S	S	S	S	S	P	S	S	P	S	S	S	S
[19]	S	P	W	S	S	S	S	S	S	P	S	S	S	S
[20]	S	S	S	S	S	S	P	S	S	S	S	S	S	S
[21]	S	P	P	S	S	S	S	S	S	S	S	S	S	S
[22]	S	P	S	S	S	S	S	S	S	P	S	S	S	S
[24]	N	P	P	S	S	S	W	S	N	S	S	P	S	S
[27]	S	S	S	S	S	S	P	S	S	S	S	S	S	S
[28]	S	S	S	S	S	S	N	W	N	N	P	S	S	P
[29]	W	W	P	S	S	S	S	P	S	N	W	W	P	S
[30]	S	S	W	S	S	S	P	S	W	N	S	S	S	S
[31]	S	S	S	S	S	S	W	S	W	S	S	P	S	S
[32]	S	S	P	S	S	S	P	S	P	P	S	S	S	S
[33]	S	S	W	S	S	S	S	S	P	S	S	S	S	S
[34]	S	S	S	S	S	S	P	S	W	S	S	S	S	S
[35]	S	S	S	S	S	S	P	S	S	P	S	S	S	S
[36]	S	S	S	S	S	S	P	S	W	N	S	S	S	S

Fuente: Elaboración propia

Realizando el respectivo tratamiento y análisis del grado de coincidencia, se tiene la tabla 8 que indica el porcentaje de similitud por elementos descritos, comprendidos en los modelos estudiados.

Tabla 8. *Puntuación por elementos*

	Establecimiento del contexto	Definición de alcance	Identificación de activos	Identificación de riesgos	Análisis de riesgos	Estimación del riesgo	Declaración de Aplicabilidad	Tratamiento del riesgo	Revisión del cumplimiento	Medición de eficacia de controles	Acciones correctivas	Registro e informe	Monitoreo y revisión.	Comunicación y consulta
S	78%	67%	61%	100%	100%	100%	33%	83%	50%	39%	89%	78%	94%	89%
P	11%	28%	22%	0%	0%	0%	44%	11%	11%	33%	6%	17%	6%	11%
W	6%	6%	17%	0%	0%	0%	17%	6%	28%	6%	6%	6%	0%	0%
N	6%	0%	0%	0%	0%	0%	6%	0%	11%	22%	0%	0%	0%	0%

Fuente: Elaboración propia

La tabla 9 muestra un resumen global de las similitudes encontradas en los distintos modelos estudiados considerando el criterio de similitud, donde se observa que se presenta una similitud parcial y fuerte de los elementos equivalente a un 90%, similitudes débiles 7% y no coincidencias 3%.

Tabla 9. *Resumen Similitud de elementos*

Criterio	Porcentaje de relación
Not related (N)	**3%**
Weakly related (W)	**7%**
Partially related (P)	**14%**
Strongly related (S)	**76%**

Fuente: Elaboración propia

5. Conclusiones

El presente trabajo presenta un estado del arte respecto a modelos de gestión de riesgos orientado a la seguridad de la información, también describe los conceptos que forman la base de distintos marcos de gestión de riesgos. Se presenta una descripción de los diferentes aspectos de los modelos actuales y de acuerdo a ello se concluye que:

La implementación de modelos de gestión de riesgos, alineados a los requerimientos particulares de una organización, influyen en la reducción de costos, tiempos y hacen más predecibles los procesos de una organización, esto ayuda a la alta dirección a tomar mejores decisiones, a comunicarse y a resolver sus riesgos de manera más efectiva.

No se debería simplemente copiar y aplicar una norma existente y usarlo como práctica estándar, ya que se tiene que considerar la adaptabilidad que pueda tener en relación a la organización, debiendo ser aplicable a las situaciones específicas que se encuentran. Las diferentes organizaciones se enfrentan a diferentes tipos de riesgos y deben adoptar diferentes enfoques cuando tratan de eliminarlos o controlarlos.

Los procesos a realizar para la elaboración de un modelo de gestión de riesgo, implica explorar los factores organizacionales y las prácticas de administración de riesgos que afectan el logro de los objetivos que estiman como estratégicos. El propósito de gestionar los riesgos es desarrollar un análisis detallado de la organización, sus operaciones, activos, procesos y sus interrelaciones existentes a fin de establecer una lista completa de riesgos, lo cual implica identificar, analizar y brindar alternativas de tratamiento a riesgos reales y potenciales.

Las técnicas más empleadas al realizar el proceso de armonización de distintos modelos de gestión son el mapping y matching. Los cuales permiten proponer modelos híbridos que permitan un control personalizado de los riesgos de acuerdo a las características particulares de una organización y sus activos que pretenda resguardar.

De acuerdo al análisis de similitud de elementos comprendidos en los distintos modelos estudiados, se tiene que los procesos relacionados a la identificación, análisis y estimación del riesgo se encuentran fuertemente relacionados en todos los modelos estudiados (100%). Como un factor clave en este escenario se evidencia la tendencia en la aplicación de la norma ISO 31000, lo cual también influye en los altos porcentajes (superiores al 83%) con respecto a los procesos de: "tratamiento de riesgo", "monitoreo", "comunicación y consulta".

En este contexto el elemento que posee una menor cantidad de coincidencias es la "medición de eficacia de los controles", (39%). La ausencia de este elemento repercutirá en un tratamiento ineficiente del riesgo y a su vez afecta negativamente las estimaciones y consideraciones que se plantee con respecto al riesgo residual.

Los elementos descritos presentan un nivel de relación fuerte (S) en un 76% y de manera parcial (P) en un 14%, por lo que se puede concluir que los modelos revisados utilizan claramente dichos elementos hasta en un 90%.

La tendencia con respecto a la gestión de riesgos, va hacia la disminución de las intervenciones humanas, esto irá en incremento conforme las regulaciones sean más complejas y los controles de cumplimiento tiendan a ser más exigentes. Aquellos procesos que no puedan ser automatizados requerirán de un mayor nivel de control, monitoreo y seguimiento, a fin de disminuir los niveles de error. Las innovaciones tecnológicas contribuirán en la toma de decisiones en aspectos de gestión de riesgos, permitirán, por medio de la utilización de grandes cantidades de información como Big Data y el uso de "machine learning", desarrollar herramientas que brinden información de carácter predictivo y cada vez más preciso, utilizando la identificación de patrones de comportamientos a partir de conjuntos de datos, sin que medie la intervención humana en el proceso de aprendizaje de los mismos, lo cual permitirá incrementar los niveles de seguridad de la información.

6. Referencias

[1] E. F. Mejía Peñafiel, «La ingeniería de requisitos una base fundamental para el desarrollo de proyectos de ti en la web,» *Revista Científica y Tecnológica UPSE,* vol. III, nº 1, pp. 71-78, 2015.

[2] R. G. C. a. V. H. M. G. Piraquive, «Analysis and Improvement of the Management,» *IEEE Latin America Transactions,* 2015.

[3] B. P. L. A. a. M. Z. Domínguez, «A systematic review of code generation proposals from state machine specifications,» *Information and Software Technology 54,* p. 1045–1066, 2012.

[4] IBM, «IBM Rational Rose,» 20 Agosto 2018. [En línea]. Available: http://www-01.ibm.com/software/awdtools/ developer/rose/.

[5] Tigris.org, «Open Source Software Engineering Tools,» 25 Setiembre 2018. [En línea]. Available: http://argouml.tigris.org.

[6] J. Resig, «https://jquery.com,» 29 05 2019. [En línea].

[7] PrimeFaces, «https://www.primefaces.org/,» 23 09 2019. [En línea].

[8] JBOSS, «http://richfaces.jboss.org,» 23 09 2019. [En línea].

[9] W. Michael, «Vaadin,» 05 11 2019. [En línea]. Available: https://vaadin.com/. [Último acceso: 2019 12 23].

[10] «Eclipse Luna,» 21 Abril 2018. [En línea]. Available: www.eclipse.org/downloads/packages/eclipse-modeling-tools/lunasr2.

[11] A. S. Foundation, Oracle Corporation y Sun Microsystems, «NetBeans,» 1 12 2019. [En línea]. Available: https://netbeans.org/. [Último acceso: 23 12 2019].

[12] MKLab, «http://staruml.io/,» 29 05 2019. [En línea].

[13] C. P. J. G. C. F. P. L. J. M. F. M. J. C. M. Alejandro, Fundamentos de programación, Madrid: Thomson, 2007.

[14] A. Manoli, «Generating operation specifications from UML class diagrams: A model transformation approach,» *Data & Knowledge Engineering, 70,* p. 365–389, 2011.

[15] J. Bennett, «Aspect-oriented model-driven skeleton code generation: A graph-based transformation approach,» *Science of Computer Programming 75,* p. 689_725, 2010.

[16] M. Pinto, «Deriving detailed design models from an aspect-oriented ADL using MDD",» *The Journal of Systems and Software, 85,* p. 525– 545, 2012.

[17] M. Rincón, «Generación Automática de Código a Partir de Máquinas de Estado Finito,» *Computación y Sistemas Vol. 14 No. 4,* pp. 405-421, 2011.

[18] «Papyrus,» 30 Octubre 2018. [En línea]. Available: http://www.papyrusuml.org/.

[19] P. Clemente, « Managing crosscutting concerns in component based systems using a model driven development approach,,» *The Journal of Systems and Software 84 ,* p. 1032–1053, 2011.

[20] F. P. Basso, «Automated design of multi-layered web information systems,» *Journal of Systems and Software, vol. 117,* pp. 612-637, 2016.

[21] I. Garrigós, «Specification of personalization in web application design,» *nformation and Software Technology,* p. 991–1010, 2010.

[22] F. A. Vasquez, «Programación por Capas,» *Revista del Departamento Académica Universidad Ricado Palma,* vol. 1, pp. 13-30, 2010.

[23] R. S. Pressman, Ingenierıa de software: un enfoque practico. 7ta edicion, ISBN 970–10–5473–3, Mexico: INTERAMERICANA, 2010.

[24] Santiago Domingo Moquillaza Henríquez, Hugo Vega Huerta, «Programación en N capas,» *Revista de Investigación de Sistemas e Informática,* vol. 7, nº 2, pp. 57-67, 2010.

[25] R. Hat, «http://www.hibernate.org/,» 30 09 2019. [En línea].

[26] S. Microsystems, «JSF,» 04 Febrero 2016. [En línea]. Available: https://javaee.github.io/javaserverfaces-spec/.

[27] «PHP,» 30 06 2018. [En línea]. Available: www.php.net.

[28] A. Vega Fajardo, «Generación Codigo,» 30 Octubre 2018. [En línea]. Available: www.speeddatasoftware.com/speed/gca.html.

[29] E. Mamas, «Towards PortableSource Code Representation Using XML,» *7th WCRE'2000,* 2000.

[30] T. Thuma, «FeatureIDE: An Extensible Framework for,» *Science of Computer Programming,* 2012.