MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a Empresas Navieras.

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Fresia Yanina HOLGUÍN GARCÍA.

Bajo la dirección de:
Lohana Mariella LEMA MORETA.

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Marzo del 2018

Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a Empresas Navieras.

Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI; focused on Shipping Companies.

Fresia Yanina HOLGUÍN GARCÍA[1]
Lohana Mariella LEMA MORETA[2]

Resumen

El presente artículo tiene como objetivo proponer un Modelo de Madurez para el Análisis de Riesgos de los Activos de Información en Empresas Navieras, que brinde oportunidades de mejora a nivel tecnológico y consecuentemente de negocio, con base en las mejores prácticas de las metodologías MAGERIT, OCTAVE y MEHARI. El modelo propuesto se fundamenta en una revisión literaria de los principales conceptos de riesgo; para su diseño se establecieron como niveles de madurez los definidos en la estructura del Capability Maturity Model Integration (CMMI); además, para incorporar las mejores prácticas seleccionadas se definió un Mapa de Control que guía su cumplimiento por niveles. El modelo resultante ha sido validado por un grupo de expertos mediante la técnica Delphi, con la finalidad de obtener una valoración cuantitativa de su aplicabilidad en las Entidades Navieras. Como resultado principal y en base a una escala Likert de cinco puntos, se obtuvo que el modelo es muy aplicable (valoración 5) para estas empresas, y se estima que al utilizarlo pueden alcanzar un nivel de madurez Definido (nivel 3 de 5), llegando a tener un proceso de análisis de riesgo formalizado y con técnicas proactivas.

Palabras clave: Modelo de Madurez, Riesgo, MAGERIT, OCTAVE, MEHARI.

Abstract

The aim of this essay is the proposal of a Maturity Model for the risk analysis of information assets in shipping companies, which provides opportunities for technological and consequently business improvement, based on the best practices of MAGERIT, OCTAVE and MEHARI methodologies. The proposed model is based on literature review about main risk concepts; for its design those defined in the Capability Maturity Model Integration (CMMI) structure were established as maturity levels; in addition, a control map was defined to guide compliance by levels to incorporate the selected best practices. The resulting model has been validated by a group of experts using the Delphi technique, in order to obtain a quantitative assessment of its applicability in the shipping companies. As a main result and based on a Likert scale of five points, it was obtained that the model is very applicable (valuation 5) for these companies, and it is estimated that by using it they can reach a defined level of maturity (level 3 of 5), arriving to have a formalized risk analysis process and with proactive techniques.

Key words Maturity Model, risk, MAGERIT, OCTAVE, MEHARI.

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail fholguin@uees.edu.ec.
[2] Magíster en Ingeniería del Software. Docente de la Universidad Espíritu Santo- Ecuador. E-mail lohanalema@uees.edu.ec

INTRODUCCIÓN

Actualmente la adopción de las Tecnologías de Información y la Comunicación (TIC), así como la implantación de los Sistemas de Información (SI), representan un factor crítico para el éxito de toda organización; sin embargo, para lograrlo se requiere de una adecuada alineación estratégica a los procesos del negocio, de lo contrario se vería mermada la eficiencia y efectividad a nivel operacional (Dong, Liu, y Yin, 2008). Dentro de este contexto también se puede palpar que la innovación tecnológica conlleva problemas ligados al aumento de entropía de los activos de información, tales como: vulnerabilidades, amenazas y ataques informáticos (Hernández y Mejía, 2015).

Aunado a lo anterior, la expansión descontrolada del Internet, así como el crecimiento de las redes corporativas (intranets y extranets), entre otros factores; propician la coexistencia de escenarios favorables para la actuación de personas inescrupulosas que, apoyadas en el anonimato, intentan acceder a la información privada de las organizaciones; por tal motivo, la correcta identificación y evaluación de los riesgos se ha convertido en un elemento crucial en la gestión de TI (Ramírez, 2012).

En este ámbito, es deber de las empresas establecer mecanismos que les permitan identificar las indeterminaciones que afectan sus actividades y procesos; así como también, analizar los controles existentes para disminuir la posibilidad de que un riesgo potencial se materialice en una pérdida cierta; y finalmente, adoptar medidas para reducir o controlar el riesgo en aquellas áreas donde se observa que se está por encima de los límites tolerables (Chu, Wei, & Chang, 2013).

En virtud a lo expuesto, surgieron estándares, normas, metodologías y guías para llevar a cabo análisis que prevengan, controlen y reduzcan los riesgos asociados a la violación o vulnerabilidad de la información (Gómez, Pérez, Donoso y Herrera, 2010). Una manera de evaluar en toda su magnitud la situación organizacional en el manejo del riesgo respecto a una situación ideal, es a través de los modelos de madurez orientados a la seguridad de la información, los cuales se sustentan en el conocimiento de los procesos, logrando así la toma de decisiones más acertada (Jugdev & Thomas, 2002).

Si bien es cierto, los modelos de madurez fueron creados para la industria del software, en la actualidad su área de aplicación es muy diversa, siendo utilizados en la gestión de proyectos, desarrollo de procesos, cadena de suministro, entre otros (Röglinger & Pöppelbuß, 2011). En el ámbito de la seguridad informática, un modelo de madurez describe un camino de mejoramiento evolutivo, que abarca desde los procesos inconsistentes hasta los más desarrollados de una empresa, convirtiéndose en un mapa que orienta a la organización en la implementación de buenas prácticas e identifica claramente las áreas donde la entidad debe enfocarse para mejorar (Becker, Niehaves, Poppelbus, & Simons, 2010).

Por otra parte, dentro de los distintos tipos de empresas que existen a nivel mundial, es preciso distinguir las organizaciones del sector de transporte marítimo denominadas *Agencias Navieras,* las cuales desempeñan un papel clave en la documentación, logística, estiba, desestiba y demás operaciones portuarias que requiere una embarcación cuando atraca en un puerto. Su operación se apoya en distintos activos tecnológicos de información; sin embargo, la identificación y categorización de este tipo de entidades de acuerdo a su fortaleza y nivel de riesgo de su ambiente tecnológico se considera un vacío conceptual no atendido según se manifiesta en un estudio realizado por Llop et al. (2013).

Este artículo tiene como objetivo proponer un *Modelo de Madurez para el Análisis de Riesgos de los Activos de Información en las Empresas Navieras*, que se convierta en un medio de evaluación alineado a la realidad de estas organizaciones y brinde oportunidades de mejora a nivel tecnológico y consecuentemente

de negocio, con base en las mejores prácticas de las metodologías MAGERIT, OCTAVE y MEHARI; donde *MAGERIT* considera que el crecimiento de la tecnología en las organizaciones se da de forma exponencial y por lo tanto es necesario minimizar los riesgos asociados a los sistemas garantizando su autenticidad, confidencialidad, integridad y trazabilidad (Carvajal, 2013); que, *OCTAVE*, equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnologías para que a partir de éstos los entes empresariales tomen decisiones basados en los principios de seguridad (CERT, 2013); y finalmente, que *MEHARI* proporciona un conjunto de herramientas para realizar un análisis de riesgo cuantitativo y cualitativo (CLUSIF, 2010).

Para alcanzar el objetivo antes planteado se realizará una revisión bibliográfica del proceso de análisis de riesgo, las particularidades de las metodologías MAGERIT, OCTAVE y MEHARI; y se profundizará el concepto de niveles madurez haciendo énfasis al modelo CMMI. Además, y como parte de la metodología propuesta se construirá un modelo con tres elementos: *Niveles de Madurez, Categorías a Evaluar y Mapa de Control*; los mismos que tienen como fundamento las mejores prácticas de las metodologías revisadas, y para estimar su validez se aplicará la técnica Delphi, por lo cual se escogerán siete profesionales con experticia laboral en entornos navieros.

Este articulo está estructurado en cinco secciones: en la primera, denominada *Introducción*, se expone la problemática, justificación y objetivos; la segunda instancia titulada *Marco Teórico* aborda la revisión y síntesis de bibliografía relacionada a la temática; la tercera parte denominada *Metodología* presenta los métodos utilizados para el desarrollo de la propuesta del modelo de madurez; en la cuarta sección titulada *Análisis de Resultados* se detallan las inferencias obtenidas; finalmente en la sección de *Conclusiones* se puntualizan las aportaciones de la presente investigación y se proponen trabajos futuros.

MARCO TEÓRICO

La revisión de literatura de este articulo comprende definiciones de análisis de riesgos en relación a TI, también se especifican las etapas que permiten llevar a cabo su ejecución en un entorno organizacional. Así mismo, se detallan las características distintivas de las metodologías: MAGERIT, OCTAVE y MEHARI; por ello se hace mención a las fases que aguardan cada una de éstas. Además, se amplía el concepto de Modelo de Madurez, y se identifican las propiedades que deben considerarse durante su construcción.

Análisis de Riesgo

Areitio (2008) define el análisis de riesgo como un proceso exhaustivo que tiene como finalidad identificar los peligros que atentan a la seguridad, establecer el impacto de su materialización y determinar las áreas que requieren salvaguardas. Así mismo, Aguilera (2010) señala que un análisis de riesgo conlleva conocer todos los activos de información que componen un sistema para estipular su grado de vulnerabilidad y el impacto que un ataque causaría; lo cual será el sustento para seleccionar las medidas de protección más oportunas. En cambio, INCIBE (2015) considera que el análisis de riesgo es una aproximación metódica para cuantificar el riesgo, y posibilita desde el resguardo de los activos de información de una organización hasta la capacidad de cumplir sus objetivos más primordiales.

En este contexto, Curiman y Toth (2004) aseveran que el análisis de riesgo no es un proceso aislado respecto a otras iniciativas conducentes a asegurar un nivel óptimo de seguridad, al contrario, éstas conformarían una línea base que permitirá identificar con rapidez las áreas más vulnerables logrando también que la implantación de las salvaguardas sea acorde a las necesidades requeridas por el entorno.

Según ENISA (2006) el llevar a cabo un correcto análisis de riesgo propicia que toda entidad pueda asegurar la continuidad

operacional, manejar adecuadamente las amenazas críticas, justificar la mejora continua de la seguridad de la información y minimizar el impacto en relación a la pérdida de dinero, tiempo y mano de obra. También, Echenique (2012) agrega que existen seis elementos claves dentro del análisis de riesgo:

1.- Probabilidad: estimación de la posibilidad que se produzca una amenaza real (Canal, 2004).

2.- A*menazas:* acciones que pueden ocasionar consecuencias negativas en una empresa, y cuya naturaleza puede ser: física (desastres ambientales, falla de cableado, entre otros) o lógica (virus, accesos no autorizados a la base de datos, entre otros) (Tarazona, 2012).

3.- Vulnerabilidades: condiciones inherentes en los activos o presentes en el entorno que facilitan que una amenaza se materialice siendo su origen variado; por ejemplo: antivirus desactualizado, errores en la implementación de una herramienta, falta de mantenimiento, entre otras (Voutssas, 2010).

***4.- Activos*:** recursos que pertenecen a un sistema de información o están relacionados al mismo; se clasifican en: datos, software, hardware, redes, instalaciones, personal, servicios y soporte (Aguilera, 2010).

5.- Impacto: es el daño que causa o puede causar sobre un activo la materialización de una amenaza. Su tipificación puede variar, pero generalmente se valora con respecto al grado de afectación de los principios básicos de seguridad: confidencialidad, integridad y disponibilidad (Eterovic y Pagliari, 2011).

6.- Riesgo: Posibilidad que una amenaza se materialice causando efectos positivos o negativos (Gupta, & Xu, 2010).

Gómez, Farías y Mendoza (2003) señalan que durante la ejecución del análisis de riesgo es recomendable desarrollar los pasos establecidos por las metodologías existentes, y según INCIBE (2017) éstas contemplan fases comunes:

Identificar los activos: Durante esta etapa se clasifican los activos que requieren mayor protección, y también se identifican sus características y el rol desempeñado (MINTIC, 2016).

Valorar los activos identificados: Permite definir el costo de recuperar un activo cuando un fallo se ha suscitado, esta valoración puede realizarse de forma cuantitativa (utilizando cantidades numéricas, valores exactos) y cualitativa (se emplea una escala de niveles, por ejemplo: alto, medio y bajo) (MINTIC, 2016).

Determinar las amenazas a las que están expuestos los activos: En esta fase se identifican las amenazas naturales (terremotos, inundaciones, entre otras) o las provocadas deliberadamente (intrusión, espionaje, fraude, entre otras) (Bracho, Rincón y Acurero, 2010).

Estimar el impacto de la amenaza: Permite determinar los efectos perjudiciales que puede provocar la materialización de una amenaza sobre los activos, y para ello considera todas las dimensiones que pueden ser afectadas (Bracho, Rincón y Acurero, 2010).

Determinación del riesgo: En este periodo es posible calcular el riesgo, el cual se estima de forma cuantitativa (se multiplica la probabilidad por el impacto); o cualitativa (la estimación se basa en matrices con escalas) (Fernández, Moya y Piattini, 2003).

Molina (2007) manifiesta que, una vez llevadas a cabo las fases antes descritas, se obtendrá un mapa de los riesgos a los que está expuesta una organización y luego se deberá proceder a su gestión o tratamiento.

Según Aguilera (2010) la gestión o tratamiento de riesgo es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas en el análisis de riesgo. Así mismo, el Ministerio de Haciendas y Administración

Pública del Gobierno de España (2012) asevera que la gestión de riesgo es un proceso para seleccionar e implantar las medidas de seguridad más idóneas, de tal manera que se logre prevenir, impedir, reducir o controlar los riesgos. En este mismo ámbito, Molina (2007) señala que la gestión de riesgo se lleva a cabo a través de cuatro estrategias: transferir el riesgo a un tercero, eliminar el riesgo, asumir el riesgo o implantar medidas para mitigarlo.

Por otra parte, Peláez (2005) indica que existen varias metodologías para el análisis de riesgos, las cuales, aunque se orientan al mismo objetivo tienen características propias. También, Peltier (2005) pone en evidencia que las metodologías existentes difieren esencialmente en la manera de estimar la probabilidad de ocurrencia de una amenaza y en la forma de determinar el impacto en la organización. Alemán y Rodríguez (2014) agregan que las metodologías más sobresalientes en este dominio son: OCTAVE, MAGERIT, MEHARI, NIST SP 800:30, Coras, Cramm y Ebios; sin embargo, en este artículo se abarcará OCTAVE, MAGERIT Y MEHARI debido a que su proceso de análisis de riesgo es homólogo, y porque las metodologías excluidas requieren un costo de licencia que las convierte en poco atractivas para su implementación.

OCTAVE

Alberts & Dorofee (2002) señalan que OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) es una metodología desarrollada en el año 2001 por el CERT/CC, en la cual la tecnología es examinada en relación a las prácticas de seguridad y la toma de decisiones respecto a la protección de información, se basa en los riesgos de confidencialidad, integridad y disponibilidad a los que pueden estar sometidos los bienes con información crítica. En el mismo ámbito, Januszkiewicz & Marek (2006) añaden que el objetivo de OCTAVE es identificar los requisitos de seguridad de información cuantificando el riesgo sobre el negocio, de tal manera que se puede establecer una mejor relación costo/beneficio.

Según Alberts, Dorofee, Stevens & Woody (2003), OCTAVE es autodirigido, pero requiere de un equipo interdisciplinario (conformado por el personal del sector operativo y del departamento de TI), que trabaje enfocado a las distintas necesidades de protección y equilibre los aspectos de: riesgos operativos, prácticas de seguridad y tecnología. Así mismo, CERT (2013) indica que para la ejecución de OCTAVE se cuenta con tres fases claramente definidas:

Fase 1, Visión Operativa: Determina lo que es importante para la organización (activos relacionados con la información) y las estrategias/medidas que se están utilizando para proteger esos activos (CERT, 2013).

Fase 2, Visión Tecnológica: Examina los principales componentes operacionales y estipula sus debilidades, las cuales pueden dar lugar a una acción no autorizada contra los activos críticos (CERT, 2013).

Fase 3, Desarrollo de Estrategias y Planes: En esta etapa se crean estrategias y planes para abordar los riesgos de los activos críticos, basándose en la información obtenida de los pasos previos (CERT, 2013).

La Figura 1 muestra un esquema del proceso antes expuesto.

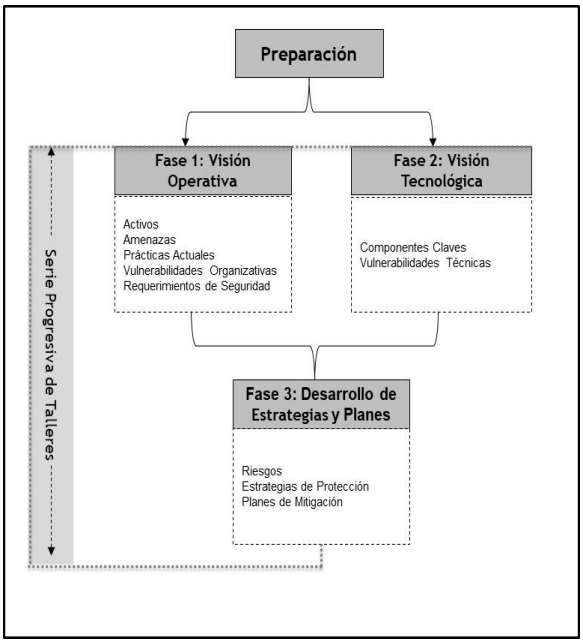

Figura 1: Fases del método OCTAVE.
Fuente: (Alberts, Dorofee, Stevens & Woody, 2003).

Hasta la presente fecha esta metodología consta de los métodos: OCTAVE, OCTAVE – S, y OCTAVE ALLEGRO; los cuales se basan en los criterios del estándar con un enfoque en la práctica y evaluación de la seguridad fundamentada en la información de riesgo de la entidad objeto de análisis (dicho enfoque es el resultado del conocimiento de los empleados así como las prácticas y procesos relacionados a la seguridad de la información que se llevan a cabo dentro de la empresa) (Alberts, Dorofee, Stevens & Woody, 2003).

Método OCTAVE: Fue desarrollado para organizaciones de trecientos o más empleados, considerando la jerarquía de múltiples capas, así como la infraestructura que suelen tener este tipo de empresas. Durante su desarrollo se examinan los lineamientos organizacionales y tecnológicos, se crea una visión clara de la organización, y se definen sus necesidades de seguridad; por ello este método se enfoca en: identificar los elementos críticos y las amenazas de los activos, establecer las vulnerabilidades (organizativas y tecnológicas), y desarrollar una estrategia basada en las prácticas y planes de mitigación de riesgos (Alberts & Dorofee, 2002).

Método OCTAVE-S: Fue concebido para las pequeñas organizaciones (con un personal de entre veinte a ochenta empleados), y a pesar de ser un método más simplificado produce el mismo tipo de resultados que OCTAVE**.** Para llevar a cabo su ejecución se requiere un equipo conformado por tres o hasta cinco personas, las cuales deben conocer a profundidad el sentido organizacional de la empresa pues se encargarán de recopilar información sobre los elementos significativos, los requisitos de seguridad, las amenazas y las estrategias de protección. Debido a que las entidades de este tipo generalmente externalizan servicios TI este método solo incluye una exploración limitada de la infraestructura informática (Januszkiewicz & Marek, 2006).

Método OCTAVE ALLEGRO: Es una variante simplificada del método de OCTAVE, sin embargo, debido a que su enfoque principal son los activos de la información, la identificación de otros importantes recursos se realiza en función de los activos de información a la que están conectados; lo cual elimina una posible confusión sobre el alcance de la evaluación (Caralli, Stevens, Young & Wilson, 2007).

A diferencia de los métodos anteriormente descritos, OCTAVE ALLEGRO cuenta con cuatro fases:

Fase 1, Establecer Dirección: Se desarrollan los criterios de medición de riesgos utilizando las directrices de la organización (Caralli, Stevens, Young & Wilson, 2007).

Fase 2, Perfilar Activos: Se crea un perfil de los activos críticos de información estableciendo sus límites e identificando sus necesidades de seguridad (Caralli, Stevens, Young & Wilson, 2007).

Fase 3, Identificar Amenazas: Se definen las amenazas de cada activo según el contexto (Caralli, Stevens, Young & Wilson, 2007).

Fase 4, Identificar y Mitigar los Riesgos: Se determinan y analizan los riesgos para los

activos de información y se desarrollan los planes de mitigación (Caralli, Stevens, Young & Wilson, 2007).

En la Figura 2 se bosquejan las fases del método OCTAVE ALLEGRO:

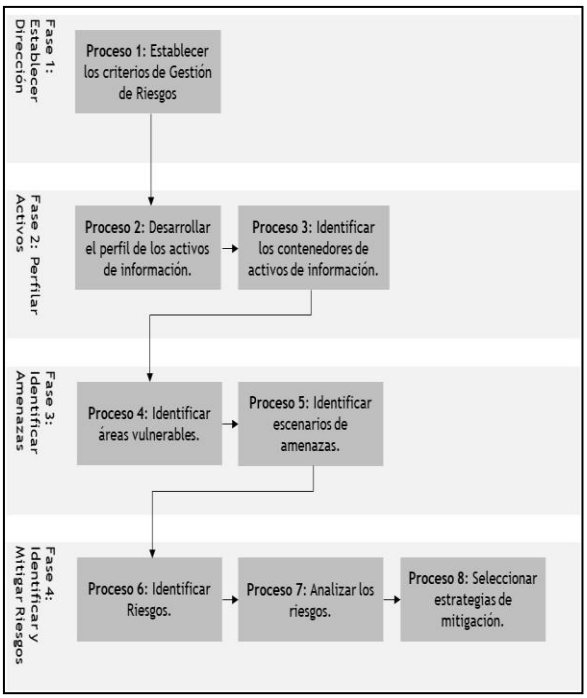

Figura 2: Fases del método OCTAVE ALLEGRO.
Fuente: (Caralli, Stevens, Young & Wilson, 2007).

Por otra parte, es ineludible indicar que la metodología OCTAVE es adaptable a todo tipo de organización debido a que se basa en los riesgos, la capacidad de recuperación y la experiencia con la que cuenta la empresa respecto a procesos similares (Espinoza, Martínez y Armador, 2014).

MAGERIT

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) es una metodología elaborada por el Consejo Superior de Administración Electrónica de España en respuesta a la percepción de que el gobierno dependía cada vez más de la tecnología de la información para conseguir sus objetivos de servicio, sin embargo, en la actualidad es de carácter público siendo utilizada por organizaciones de todo el mundo (Sylim, Hori & Sakurai, 2009).

Según el Ministerio de Haciendas y Administración Pública del Gobierno de España (2012) MAGERIT es una aproximación metódica del análisis de riesgos que no da cabida a la improvisación o arbitrariedad de quien la ejecute. Así mismo, Eterovic y Pagliari (2011) consideran que esta metodología permite conocer el estado de seguridad de los sistemas de información desde el punto de vista de los activos (se consideran todos los elementos), lo cual dará como resultado una profunda mitigación de vulnerabilidades.

Nagata, Amagasa & Kigawa (2009) señalan que MAGERIT tiene como objetivos: crear conciencia de la existencia de riesgos y la importancia de tratarlos a tiempo; proporcionar un método sistemático para analizar los riesgos garantizando la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad; diseñar estrategias para mantener los riesgos controlados; y preparar a la empresa para los procesos de auditorías, certificaciones y acreditaciones.

Es preciso señalar que MAGERIT está compuesto por tres libros que orientan su implementación, el primero de ellos (Método) es una guía detallada de como ejecutar el análisis de riesgo, el segundo (Catálogo de Elementos) expone un inventario con elementos específicos en el ámbito de riesgos (tipos de activos, amenazas típicas sobre los sistemas de información, criterios de valoración de activos, entre otros), y finalmente el tercero (Guía de Técnicas) es una compilación de prácticas para llevar a cabo proyectos de análisis y gestión de riesgos (Ministerio de Haciendas y Administración Pública del Gobierno de España, 2012).

MAGERIT propone la realización de cinco pasos para efectuar el análisis de riesgos, los cuales se detallan en la Figura 3.

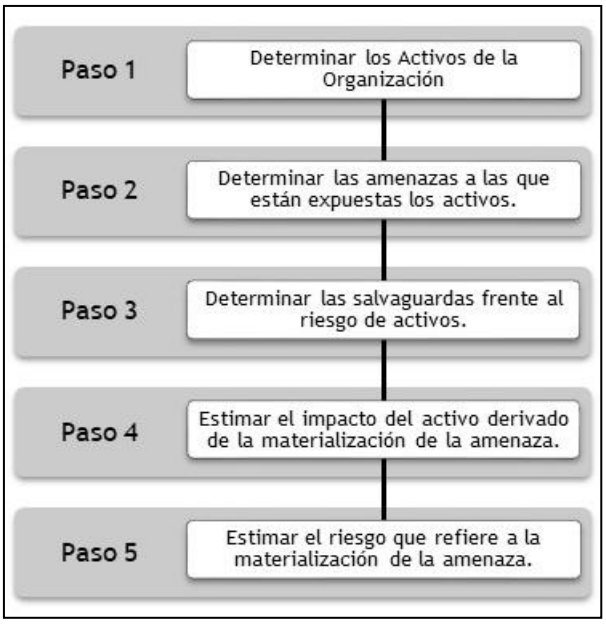

Figura 3: Pasos para el Análisis de Riesgos de MAGERIT. **Fuente:** (Ministerio de Haciendas y Administración Pública del Gobierno de España, 2012).

Mientras que para la gestión de riesgo MAGERIT propone las etapas que se evidencian en la Figura 4.

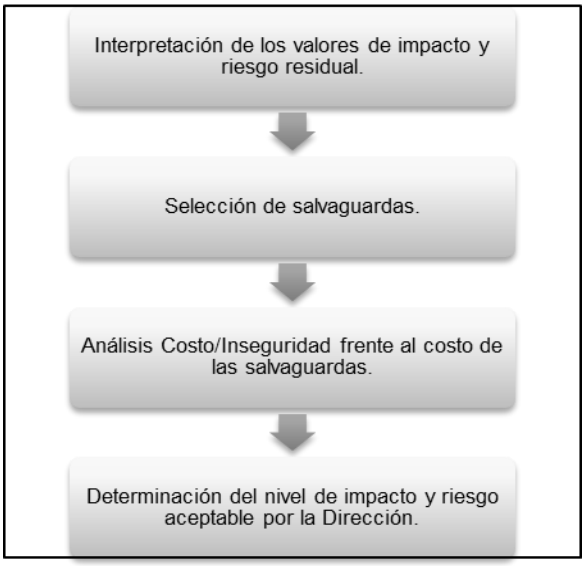

Figura 4: Pasos para la Gestión de Riesgos de MAGERIT. **Fuente:** (Ministerio de Haciendas y Administración Pública del Gobierno de España, 2012).

MEHARI

MEHARI, también conocido como un método de análisis de riesgo armonizado, es una metodología desarrollada en el año 1995 por CLUSIF (CLUb de la Sécurité de l'Information Français) con la finalidad de que los responsables de la seguridad informática evalúen cuantitativamente o cualitativamente (según sea necesario) los principales factores de riesgos que puede percibir una organización según su contexto, y para ello se requiere que la entidad establezca previamente una política de seguridad y mantenimiento de riesgos a un nivel convenido, la misma que servirá de referencia para que el acople de los objetivos estratégicos existentes sea acorde a los nuevos métodos de funcionamiento de la empresa (Alemán y Rodríguez , 2014).

Según CLUSIF (2010b) MEHARI proporciona un método para la evaluación y gestión de riesgos, orientado al dominio de la seguridad de la información según los requerimientos de la norma ISO/IEC 27005, y se basa en tres criterios: confidencialidad, integridad y disponibilidad. Así mismo, CLUSIF (2010a) manifiesta que la practicidad de MEHARI genera un análisis directo de situaciones de riesgos en diferentes escenarios, y también proporciona un conjunto de herramientas para la gestión de la seguridad que son adaptables a los distintos niveles de madurez organizacional.

MEHARI está estructurado por tres módulos: el primero tiene como finalidad el análisis de riesgos, el segundo está orientando a la evaluación de seguridad (con énfasis al análisis de vulnerabilidades) y el tercero permite el análisis de amenazas; cabe señalar que la ejecución de los mismos consentirá el diseño e implantación de los planes de acción que fomentaran la seguridad de la información (Alemán y Rodríguez, 2014).

El proceso de evaluación, tratamiento y gestión del riesgo de MEHARI, se exponen en la Figura 5.

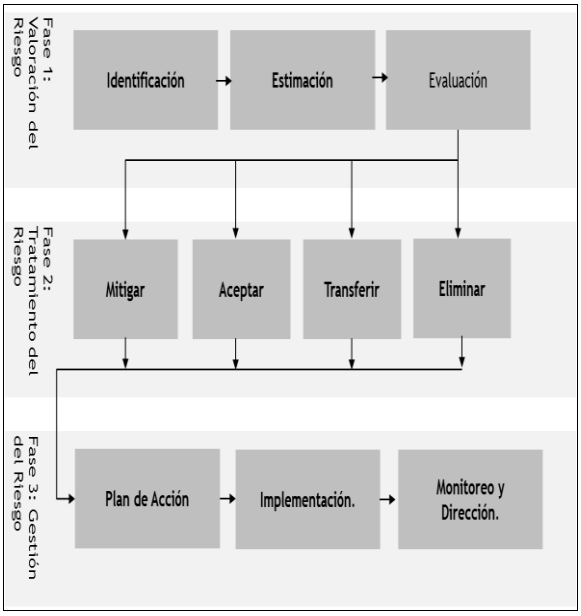

Figura 5: Proceso de evaluación, tratamiento y gestión del Riesgo de MEHARI.
Fuente: (CLUSIF, 2010b).

Modelo de Madurez

Rosemann & De Bruin (2005) definen el término *madurez* como una medida para evaluar la capacidad de una organización respecto a una determinada disciplina. En cambio, Mettler (2009) afirma que la madurez es un proceso evolutivo en la demostración de una habilidad específica.

Partiendo de estas definiciones OPM3 (2003) establece que un modelo de madurez es un esquema con niveles jerárquicos, que en esencia permite a una organización comprender su situación actual y orientarla a la consecución de un nivel más elevado lo cual requiere la implementación de mejores prácticas o rutas de mejora. Analógicamente, Galarza y Uriona (2012) indican que un modelo de madurez determina los procesos organizacionales que se deben optimizar para alcanzar la excelencia en la disciplina sobre la cual trabajan, y es por ello que éste describe desde los procesos inmaduros y ad hoc (ausencia de estándares), hasta procesos maduros y disciplinados.

Según Mettler (2009) los mapas de mejora que proponen los modelos de madurez apoyan la progresión escalonada con respecto a la capacidad de la organización, por lo cual son el camino idóneo para cumplir con las características requeridas por un nivel de madurez específico.

En este mismo ámbito, Klimko (2001) señala que de forma general los modelos de madurez tienen como propiedades: un número limitado de niveles (generalmente de cuatro a seis), cada nivel consta de requisitos determinados que deben ser alcanzados, y los niveles de madurez están clasificados de forma secuencial siendo el último un nivel de perfección.

Por otra parte, considerando la importancia de evaluar la capacidad de una organización respecto a la posibilidad para cumplir con los objetivos de seguridad de la información se han originado varios modelos de madurez, sin embargo, es el CMMI (Capability Maturity Model Integrated) el utilizado con mayor preponderancia como marco de referencia para el desarrollo de nuevos modelos (Matrane, Talea & Okar, 2014).

Según Crawford (2002) el CMMI está orientado a la industria del software y contiene una cantidad de áreas definidas por proceso, las cuales cubren conceptos básicos que son indispensables para la mejora de los mismos. También Kerzner (2000) señala que este modelo clasifica a las organizaciones en cinco niveles de madurez basados en el grado de sofisticación de sus prácticas de ingeniería, los cuales son: inicial, repetible, definido, administrado y optimizado. En la Figura 6 se esquematizan estos niveles.

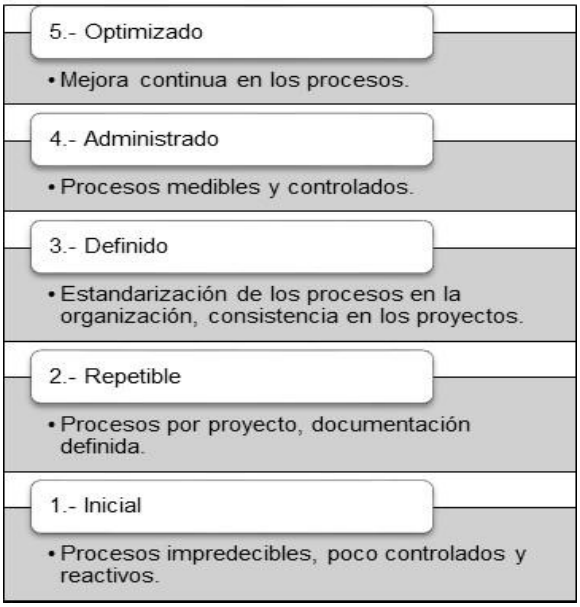

Figura 6: Niveles de Madurez CMMI.
Fuente: (Crawford, 2002).

Finalmente, es preciso señalar que en el CMMI los niveles de madurez son medidos por el logro de metas y prácticas genéricas/especificas asociados a cada área de un proceso (Crawford, 2002).

Consideraciones Finales

El *Marco Teórico* demuestra que el Análisis de Riesgo es un proceso metódico y de vital importancia para alcanzar un óptimo desempeño de las TI, y aunque existen varias metodologías orientadas a este fin, cada una posee características propias que ayudan a las organizaciones a tener un mejor control sobre los activos, su valor y minimizar las amenazas que puedan impactarlas.

Así mismo, la evidencia bibliográfica establece que las metodologías objeto de análisis: MAGERIT, OCTAVE y MEHARI cuentan con una estructura claramente definida, documentada y adaptable a todo tipo de empresa; sus fases de análisis de riesgo son semejantes, permiten identificar los activos y sus riesgos para que a partir de ello se puedan tomar decisiones y hacer mejoras en los procesos internos organizacionales; están enmarcadas a los tres principios de seguridad de la información (integridad, confidencialidad y disponibilidad), y admiten después de su implementación la realización de un plan de actividades que puede ser detallado, monitoreado y controlado periódicamente. En virtud a las características antes expuestas se considera que las metodologías seleccionadas son adecuadas para el desarrollo del modelo de madurez de las empresas navieras.

También, la literatura sustenta que los Modelos de Madurez son caminos de evolución lógica que admiten identificar futuros objetivos de mejora a través de la implementación de buenas prácticas, de allí la relevancia que sean utilizados en las entidades (sin distinción de su naturaleza) como herramienta de evaluación y rendimiento.

La siguiente sección del artículo detallará los métodos utilizados en la construcción del Modelo de Madurez para el Análisis de Riesgo considerando las necesidades de las empresas navieras y las mejores estrategias de las metodologías antes señaladas.

METODOLOGÍA.

El enfoque de la investigación es de origen *Cualitativo* porque se utilizará la teoría como fundamento en la elaboración del Modelo de Madurez para el Análisis de Riesgos de los Activos de Información, en lugar de implementar una fundamentación empírica; mientras que el alcance es *Descriptivo,* debido a que se identificará la contribución del modelo en las empresas navieras a través de la profundización de información sobre un contexto en particular, de tal manera que se logre una descripción de sus características.

Por otra parte, el desarrollo de la investigación se llevará a cabo en cinco fases:

1. Revisión de trabajos relacionados al modelo de madurez CMMI y las metodologías MAGERIT, OCTAVE y MEHARI.

2. Análisis de las Empresas Navieras en contexto a las Tecnologías de Información.
3. Construcción del Modelo de Madurez para el Análisis de Riesgos de los Activos de Información para las Empresas Navieras basado en los resultados obtenidos del paso 1 y 2.
4. Validación del modelo propuesto.
5. Presentación de resultados.

Para establecer las necesidades de las Agencias Navieras en relación al análisis de riesgo se utilizó como población las 17 entidades constituidas legalmente en el Ecuador (Autoridad Portuaria de Manta, 2016), de las cuales siete se encuentran en la ciudad de Manta, cinco en Guayaquil, tres en Esmeraldas, una en La Libertad y una en Galápagos. Considerando que el mayor número de empresas se encuentran radicadas en Manta y poseen una amplia trayectoria en el mercado se tomó como muestra los sietes entidades de esta urbe. Los informantes claves fueron el personal del Departamentos de TI de la muestra obtenida, a quienes se les formuló como técnica de recolección de información la entrevista.

ANÁLISIS DE RESULTADOS

1.- Revisión de trabajos relacionados al Modelo de Madurez CMMI y las Metodologías MAGERIT, OCTAVE y MEHARI.

Maggiore (2014) definió un *Modelo de Madurez para la Seguridad de Información* utilizando CMMI, pues éste admitió la integración de la madurez de los procesos de gestión de riesgos con los relacionados a la gestión de controles en dependencia al plan de tratamiento de riesgos. El autor contrastó a través de la bibliografía los modelos de madurez desarrollados por COBIT y Gartner llegando a discernir que utilizan algunos términos y características del modelo CMMI, sin embargo, la estructura (áreas de proceso, metas y prácticas genéricas, metas y prácticas específicas) de éste último son más concisas en la definición de los niveles de madurez. Además, argumenta que CMMI permitió que su propuesta incluya prácticas efectivas, repetibles, duraderas e inherentes a los procesos organizativos; así como la transición de un aprendizaje individual a un aprendizaje organizacional basado en la mejora continua y las experiencias adquiridas. Las prácticas planteadas en el modelo están articuladas a los estándares ISO/IEC 27001, ISO/IEC 27005 y ISO/IEC 27002; y la efectividad de la propuesta se evaluó en cinco escenarios distintos los cuales concluyeron con éxito.

Analógicamente, Mayer y Lemes (2008) crearon un *Modelo de Madurez para Evaluar los Procesos de Gestión de Riesgos en Seguridad de la Información* considerando como referencia el CMMI, debido a que una de sus principales fortalezas es la posibilidad de representar el modelo por etapas o de manera continua; siendo esta última opción la más idónea para establecer que cada actividad o buena práctica para la gestión de riesgo pueda alcanzar un nivel de madurez independientemente del nivel alcanzado por las demás actividades, con lo que la empresa logra verificar en cuál de las actividades necesita enfocarse más. El modelo utiliza la Norma ISO/IEC 27005 y su diseño está fundamentado en la experiencia (empírico).

Por otra parte, Sotelo, Torres y Rivera (2012) desarrollaron un *Proceso Práctico de Análisis de Riesgos de Activos de Información* utilizando como eje de su temática la metodología MAGERIT porque los subprocesos planteados en el análisis de riesgos eran satisfactorios para el desarrollo de las acciones de seguridad que requiere la gestión del riesgo de los activos de información, pero los autores le agregaron un proceso de Análisis de Impacto del Negocio (BIA) para definir el impacto de la no disponibilidad de los servicios tecnológicos de la información. El proceso propuesto fue implementado en una entidad pública donde los resultados fueron satisfactorios.

En cambio, Amador (2014) definió una propuesta denominada *Gestión de Riesgo con base a la ISO 27005 adaptando OCTAVE-S,* en la cual manifiesta que este método provee un

instrumento para identificar ágilmente las amenazas más relevantes en los activos de información proporcionando a su vez una estimación cualitativa de la probabilidad e impacto; lo cual ayuda a definir las estrategias de protección y controles para el tratamiento del riesgo. La propuesta se evaluó en un centro de estudios universitario privado con lo cual se logró una reducción significativa del riesgo luego de la implantación de los respectivos controles sugeridos en el tratamiento.

Además, Maldonado (2013) en su trabajo *Gestión de Riesgos Informáticos para la Protección de los Sistemas de Información en la Cooperativa de Ahorro y Crédito Campesina COOPAC,* combina las prácticas de las metodologías MAGERIT, OCTAVE y MEHARI para evaluar las distintas situaciones de riesgo en la institución financiera COOPAC; el autor establece que pudo alinear estos métodos pues todos permiten analizar y administrar los riesgos en diferentes niveles considerando la magnitud del impacto y proporcionando información adecuada en la toma decisiones; por tal motivo hizo énfasis en que las prácticas escogidas satisfagan los pilares de: planificación de la reducción de riesgos, planificación de la prevención de incidentes, visualización y detección de las debilidades existentes en los sistemas de información, ayuda en la toma de las mejores decisiones en materia de seguridad de la información. Además, el autor demostró con practicidad la eficiencia y validez de su propuesta.

A través de los trabajos anteriormente expuestos queda evidenciado que el modelo CMMI puede ser utilizado en combinación con otros estándares, además que las metodologías MAGERIT y *OCTAVE-S* han generado resultados exitosos en el análisis y gestión de riesgos en instituciones públicas como privadas. En la investigación de Maldonado (2013) se demostró que la alineación de las metodologías MAGERIT, OCTAVE y MEHARI es factible y a la vez puede ser adaptable a un contexto en particular (en este estudio fueron las instituciones financieras), por lo que es útil establecer pilares como guía para la selección de las mejores prácticas.

2.- Análisis de las Empresas Navieras en contexto a las Tecnologías de Información

Los servicios portuarios han intensificado el uso de las tecnologías de información debido a que el incremento de las capacidades de transporte demanda información inmediata sobre la ubicación y status exacto de la carga; así como de todos los aspectos institucionales y logísticos que circundan la operativa portuaria (Mundo Marítimo, 2010). Frente a ese tipo de exigencias todos los sectores de los puertos y la industria naviera han viabilizado la adquisición de nuevos sistemas y canales de comunicación que posibiliten la eficiencia de sus operaciones. Las Agencias Navieras forman parte de este contexto por lo que necesitan entrelazar las TI al servicio brindado independiente de su tipo (servicios regulares, servicios sin trayecto fijo, servicios industriales y petroleros) (Beato, 2012).

Por consiguiente, para definir sus necesidades en relación al análisis de riesgo de los activos de información se utilizó como técnica de recolección de información la entrevista; la misma que se realizó a la muestra establecida (siete Agencias Navieras del país) y se escogió a siete empleados (un empleado de TI por entidad) que cumplieran actividades de infraestructura y seguridad. Es preciso señalar, que dos de las entidades escogidas pertenecen al grupo de grandes empresas, cuentan con una media de treinta y tres años en el mercado y su Área de TI la conforman seis personas; mientras que las otras cinco agencias son medianas empresas, tienen un promedio de diecisiete años de trayectoria y sus Departamentos de TI poseen una media de tres empleados. Las preguntas formuladas fueron:

- ¿Considera que existe una Metodología adecuada para realizar un Análisis de Riesgo en las Entidades Navieras?

- ¿Cuáles son los principales problemas que afronta el Departamento de TI durante el proceso de Análisis de Riesgos?
- ¿Considera usted que un Modelo de Madurez que determine el status actual en relación al Análisis de Riesgos de los Activos de Información, sería una herramienta útil en el Departamento de TI?

La información obtenida en las entrevistas y que se exponen en el Anexo 1 ha permitido concluir que las Agencias Navieras tienden a expandirse a nuevas áreas geográficas, lo cual requiere maximizar el uso de la tecnología para crear redes mundiales de puertos y así ofrecer niveles consistentes de servicios; pero esto genera un desconocimiento en la categorización del riesgo que pueden tolerar según la madurez de los procesos que se ejecutan en la actualidad, además que estos nuevos retos implican una capacitación permanente de todo el personal para poder evitar brechas en conocimientos. También, los cambios de jefes en el área de TI suelen ser un obstáculo en el diseño e implantación de estrategias unificadas y perdurables, lo cual se acrecienta con una política de seguridad ambigua.

Partiendo de las inferencias antes descritas y considerando que Applegate, McFarlan, & Austin (2002) señalan que en un negocio correctamente estructurado deben existir políticas, procesos e indicadores; que estén alineados a una adecuada identificación y tratamiento de riesgos; se han establecidos dos lineamientos para el desarrollo del modelo: estrategias claves el proceso de análisis de riesgo, y estrategias conexas al negocio en relación al riesgo tecnológico.

3.- Construcción del Modelo de Madurez para el Análisis de Riesgos de los Activos de Información para las Empresas Navieras

La construcción del modelo prototipo se basa en los resultados obtenidos de las fases anteriores; y debe responder a las siguientes interrogantes:

- ¿Se adapta a los requerimientos de las Agencias Navieras?
- ¿Las buenas prácticas sugeridas se enmarcan en las metodologías MAGERIT, OCTAVE y MEHARI?
- ¿El modelo abarca las fases esenciales del análisis de riesgo?

Para definir el modelo se han desarrollado los siguientes elementos:

- Propuesta: Niveles de Madurez.
- Propuesta: Categorías a Evaluar y Mejores Prácticas.
- Propuesta: Mapa de Control.

Propuesta: Niveles de Madurez

El modelo de madurez propuesto consta de cinco niveles secuenciales que abarcan desde un nivel ad hoc hasta un nivel sofisticado; y para su elaboración se analizaron las directrices del CMMI en relación al grado de practicidad de los procesos que conllevan el análisis de riesgos. En la Figura 7 se detallan los niveles de madurez con sus características.

Figura 7: Niveles de Madurez del Modelo Propuesto con base al CMMI.
Fuente: (Elaboración propia, 2017).

Propuesta: Categorías a Evaluar y Mejores Prácticas

El modelo propuesto define once *Categorías a Evaluar,* de los cuales A, B, C y D corresponden a estrategias relacionadas al negocio y al riesgo tecnológico, y las categorías restantes comprenden los aspectos claves que se requieren en el proceso de análisis de riesgo. Además, por cada categoría se han establecido mejores prácticas en contexto a las metodologías MAGERIT, OCTAVE y MEHARI. En la Tabla 1 se evidencian los entes antes señalados.

Tabla 1: Propuesta de Categorías a Evaluar y Mejores Prácticas con base en las metodologías MAGERIT, OCTAVE y MEHARI.

	Categorías a Evaluar	Mejores Prácticas	MAGERIT	OCTAVE	MEHARI
El Negocio y el Riesgo Tecnológico	**A. Política de Riesgo**	**A.1.-** Existe una política formal de riesgo aprobada por la autoridad responsable y que transciende a pesar de cambios de personal en la alta dirección.			
		A.2.- La política ha sido comunicada a toda la entidad.			
		A.3.- La política de riesgo es revisada y actualizada para incluir los cambios del entorno interno y externo.			
		A.4.- La política incluye una definición de la cantidad de riesgo (apetito de riesgo) que la entidad puede aceptar, y puede estar descrita en términos cuantitativos o cualitativos.			
	B.- Responsabilidad	**B.1.-** La entidad posee un departamento de TI con un equipo de análisis de riesgo.			
		B.2.- Los roles del equipo de análisis de riesgo están claramente definidos, asignados y documentados. Por ejemplo: El personal verifica que las prácticas de respuestas al riesgo sean acordes a la política establecida, coordina los planes de acción así como también la consistencia y exactitud del proceso, aprueba el apetito de riesgo en la entidad.			
	C.- Compromiso de la Alta Dirección	**C.1.-** La alta dirección es un apoyo activo para el equipo de análisis de riesgo, así por ejemplo: verifica que la política sea compatible con las necesidades de la empresa, evalúa la efectividad del proceso (revisión periódica de los informes del equipo de análisis riesgo) y está dispuesto a participar del mismo si es necesario.			
		C.2.- La alta dirección garantiza los recursos necesarios para llevar a cabo el análisis de riesgo, así como la formación y entrenamiento del personal.			
	D.- Comunicación y Formación	**D.1.-** La empresa posee un personal altamente calificado en el departamento de TI, por ello se promueve su capacitación permanente.			
		D.2.- Existen programas de capacitación formalizada para establecer una cultura de riesgo y asegurar que el personal de la entidad entiende la política de riesgo.			
		D.3.- Se informa periódicamente y de forma inmediata a la alta dirección la consolidación de un riesgo.			
	Identificar los Activos / ***Valorar los Activos Identificados*** — **E.- Determinación y Valoración de los Activos de Información**	**E.1.-** Los activos/recursos TI han sido clasificados según una perspectiva de: servicios, datos/información, aplicaciones, equipos informáticos, redes de comunicación, soporte de información, equipamiento auxiliar, instalaciones y personal.			
		E.2.- Se cuenta con un perfil que describe características únicas, cualidades, dependencia (medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior) y valor de los activos de información.			

Fases del Análisis de Riesgos			**E.3.-** Existe una escala de valoración definida, por ejemplo: de tipo logarítmica (la misma tiene como objetivo hacer una valoración cualitativa respondiendo a valoraciones subjetivas por parte del personal de la organización).	■	■	■
	Determinar las amenazas a las que están expuestos los activos	**F.- Identificación y estimación de Amenazas**	**F.1.-** La empresa analiza exhaustivamente las amenazas externas e internas a los que pueden verse afectados los activos de información.	■	■	■
			F.2.- Por cada amenaza identificada se ha definido la dimensión de disponibilidad, integridad, y confidencialidad; que puede resultar afectada en el activo de información.	■	■	■
	Estimar el impacto de la amenaza	**G.- Estimación de Impacto**	**G.1.-** Se ha establecido una escala de impacto considerando la gravedad de las consecuencias de la materialización de una amenaza; por ejemplo: reputación, pérdida de clientes, costos operativos, pérdida de ingresos, pérdidas financieras, horas de trabajo del personal, pérdidas significadas de vida y seguridad.		■	
			G.2.- Se ha ponderado el impacto acumulado tomando en cuenta la degradación causada por la amenaza, y el impacto repercutido teniendo en cuenta el valor propio del activo y las amenazas a los que está expuesto.	■		
	Determinación del riesgo	**H.- Evaluación del Riesgo**	**H.1.-** Se ha definido el riesgo acumulado considerando la degradación causada y la frecuencia de la amenaza; y se ha definido el riesgo repercutido calculando el daño en los activos explícitamente valorados.	■		
			H.2.- Los riesgos son clasificados a partir de una escala que considera la probabilidad e impacto, con la finalidad de priorizar los más significativos.	■	■	■
	Plan de Acción	**I.- Respuesta a los Riesgos**	**I.1.-** Se determina una respuesta por cada riesgo identificado (la cual es producto de una socialización y consenso) considerando su probabilidad e impacto.	■	■	■
			I.2.- Cada respuesta al riesgo está perfectamente desplegada, configurada, mantenida y recaerá en una de estas categorías: *Mitigar,* contiene una o varias estrategias de mitigación, las cuales describen los controles a implantar y los recursos requeridos; *Aceptar,* no deben acarrear graves consecuencias a la organización; *Transferir,* deberán estar incluidos en el plan financiero de la empresa; *Eliminar,* constan de medidas estructurales para lograr su consecución.	■	■	■
			I.3.- Se ha definido el riesgo residual que permanecerá cuando una respuesta al riesgo se implemente.	■	■	■
	Monitoreo y Dirección	**J.- Actividades de Control**	**J.1.-** Se definen indicadores de desempeño sobre la respuesta a los riesgos para determinar su validez.	■		■
			J.2.- Los efectos de las respuestas a los riesgos se miden frente al apetito de riesgo.		■	
			J.3.- Se evalúa el riesgo residual una vez aplicada la respuesta al riesgo.	■	■	■
		K.- Mejora Continua del Análisis de Riesgo	**K.1.-** Exhaustiva recopilación de información para el seguimiento, revisión y aprendizaje en torno al análisis de riesgo.	■		■
			K.2.- La presencia de nuevos riesgos se identifica sistemáticamente de manera oportuna y proactiva.	■	■	■

Fuente: (Elaboración propia, 2017).

Leyenda:

■ Metodología(s) en las que se basa la Mejor Práctica. □ La Mejor Práctica no se basa en esta metodología.

Propuesta: Mapa de Control

El Mapa de Control propuesto expone las Categorías a Evaluar con las Mejores Prácticas que se sugieren estén implementadas según el nivel de madurez (se utilizaron los resultados obtenidos en la Figura 7 y Tabla 1). En la Tabla 2 se detalla el Mapa de Control.

Tabla 2: Mapa de Control propuesto.

Categorías a Evaluar	Nivel 1: Inicial	Nivel 2: Repetible	Nivel 3: Definido	Nivel 4: Administrado	Nivel 5: Optimizado
A. Política de Riesgo	No se esperan prácticas formales.		A1, A2	A3, A4	
B.- Responsabilidad		B1	B2		
C.- Compromiso de la Alta Dirección			C1	C2	
D.- Comunicación y Formación			D1	D2, D3	
E.- Determinación y Valoración de los Activos de Información		E1	E2, E3		
F.- Identificación y estimación de Amenazas			F1	F2	
G.- Estimación de Impacto			G1	G2	
H.- Evaluación del Riesgo			H1, H2		
I.- Respuesta a los Riesgos			I1, I2	I3	
J.- Actividades de Control				J1	J2, J3
K.- Mejora Continua del Análisis de Riesgo					K1, K2

Fuente: (Elaboración propia, 2017).

4.- Validación del Modelo Propuesto.

Como método de validación del marco metodológico propuesto se utilizó Delphi, debido a que las *Mejores Prácticas* seleccionadas son el resultado de la revisión de literatura y era preciso verificar la aplicabilidad en las empresas navieras considerando la experticia de profesionales del sector.

Según Gordon (1994) el método Delphi puede ser utilizado como un debate controlado que busca obtener el consenso de varios especialistas y evitar un criterio unipersonal. Analógicamente, Reguant y Torrado (2016) señalan que otra forma de emplear el método Delphi es a través de la elaboración de un cuestionario con la finalidad que sea validado por un grupo de expertos en un área específica, cuyo tamaño suele oscilar entre 6 a 30 participantes; los profesionales escogidos deberán reunir características de: trayectoria académica, méritos especiales, experiencia profesional destacada o rasgos por los que resalten en el tema de estudio.

Partiendo de estas definiciones, en este artículo se utilizó Delphi según la forma señalada por Reguant y Torrado (2016), de tal manera que se logre establecer en base al juicio de expertos el nivel de aceptación y factibilidad con respecto al entorno naviero de: los niveles de madurez, criterios a evaluar, buenas prácticas y la pertinencia de cada mejor práctica por nivel de madurez.

Respecto al perfil de los profesionales en primera instancia se convocó a diez especialistas, sin embargo, solo 7 aceptaron evaluar el Modelo de Madurez. Los expertos escogidos eran hombres ecuatorianos entre 30 a 60 años de edad, debido a que se trató de captar heterogeneidad en cuanto a años de experiencia laboral. De este grupo, el 42,85% tenía más de 25 años laborando en entidades navieras y en sus perfiles destacaba la existencia de títulos como: Magister en Gestión de Tecnologías y Magister en Ciencias de la Computación. Así mismo, el 28,57% indicó una trayectoria de 21- 25 años en el sector, con el título de Magister en Informática de Gestión y Nuevas Tecnologías, y contaban con certificaciones CISCO CNNA, DBA ESPOL y Auditor Interno ISO 27001. Además, el 14,29% señaló una experticia de 16-20 años y tenía el título de Magister en Análisis de Datos. Finalmente, el 14.29% de los profesionales poseían entre 5 – 10 años de experiencia en el área naviera con una certificación MIT EMTECH. Cabe señalar que todos los expertos han llevado a cabo procesos de análisis de riesgos en estas entidades.

Por otra parte, el cuestionario fue elaborado en la herramienta Formularios de Google, estuvo habilitado por 5 días (del 26 al 30 de diciembre del 2017) y el tiempo para su desarrollo se estimaba en una hora. Su estructura la conformaban seis secciones:

- La primera sección describía la definición de *Modelo de Madurez* y el objetivo de la investigación.
- La segunda parte estaba orientada a recopilar información relacionada al perfil del encuestado.
- La tercera sección explicaba los 5 niveles de madurez definidos y se solicitó a los participantes valorar su aplicabilidad en las agencias navieras para lo cual se elaboró la Tabla 3 que permitía puntuar el nivel de aprobación según una escala Likert cuyo rango oscilaba del 1 al 5.

Tabla 3: Escala de aplicabilidad.

Nivel	Escala	Descripción
Totalmente en Desacuerdo	1	Ningún nivel de madurez es aplicable en las agencias navieras.
En desacuerdo	2	Un nivel de madurez es aplicable en las agencias navieras.
Ni de acuerdo ni en desacuerdo	3	Dos o tres niveles de madurez son aplicables en las agencias navieras.
De acuerdo	4	Cuatro niveles de madurez son aplicables en las agencias navieras.
Totalmente de Acuerdo	5	Todos los niveles de madurez son aplicables en las agencias navieras.

Fuente: (Elaboración propia, 2017).

- La cuarta parte exponía las once *Categorías a Evaluar* y se pidió a los expertos valorar su importancia para el Análisis de Riesgo en las empresas navieras; por ello se definió una escala Likert del 1 al 5, la cual se expone en la Tabla 4.

Tabla 4: Escala de importancia.

Nivel	Escala	Descripción
Sin Importancia	1	La *Categoría a Evaluar* es prescindible, no causa repercusión en el Análisis de Riesgo.
De poca Importancia	2	La *Categoría a Evaluar* podría aplicarse pero su utilización no influye mayormente en el Análisis de Riesgo.
Moderadamente Importante	3	La *Categoría a Evaluar* debe aplicarse, su utilización repercute en el Análisis de Riesgo.
Importante	4	La *Categoría a Evaluar* debe aplicarse, su utilización causa gran repercusión en el Análisis de Riesgo.
Muy Importante	5	La *Categoría a Evaluar* es imprescindible en el Análisis de Riesgo y conlleva a un mejor desempeño del mismo.

Fuente: (Elaboración propia, 2017).

- La quinta sección detallaba las 28 mejores prácticas identificadas a partir de la revisión bibliográfica y se solicitó a los participantes determinar su aplicabilidad para el Análisis de Riesgo en las empresas navieras utilizando una escala Likert con un rango de 1 al 5, la cual se evidencia en la Tabla 5.

Tabla 5: Escala de aplicabilidad.

Nivel	Escala	Descripción
Totalmente en Desacuerdo	1	La *Buena Práctica* es prescindible, no causa repercusión en el Análisis de Riesgo
En desacuerdo	2	La *Buena Práctica* podría aplicarse pero su utilización no influye mayormente en el Análisis de Riesgo.
Ni de acuerdo ni en desacuerdo	3	La *Buena Práctica* debe aplicarse, su utilización repercute en el Análisis de Riesgo.
De acuerdo	4	La *Buena Práctica* debe aplicarse, su utilización causa gran repercusión en el Análisis de Riesgo.
Totalmente de Acuerdo	5	La *Buena Práctica* es imprescindible en el Análisis de Riesgo y conlleva a un mejor desempeño del mismo.

Fuente: (Elaboración propia, 2017).

- Finalmente, en la sexta parte se pidió a los expertos definir la pertinencia de cada buena práctica a un determinado Nivel de Madurez, con la finalidad de comparar y mejorar el diseño planteado en el Mapa de Control.

5.- Presentación de Resultados

Una vez finalizado el periodo en que podía ser respondido el cuestionario, se procedió a su deshabilitación para dar inicio al análisis de resultados.

En lo que respecta a la sección *Aplicabilidad de los Niveles de Madurez propuestos para el Análisis de Riesgos de los Activos de Información en las Empresas Navieras*, los profesionales señalaron estar *Totalmente de Acuerdo* en la aplicabilidad con un 86%, mientras que el 14% indicó *De Acuerdo*. En la Figura 8 se esquematizan estas inferencias.

Figura 8: Niveles de Madurez y su Aplicabilidad en las Entidades Navieras.
Fuente: (Encuesta a **E**xpertos, 2017).

En relación a la sección del cuestionario *Importancia de las Categorías a Evaluar para el Modelo de Madurez en las Entidades Navieras* se puede apreciar que las *Categorías* relacionadas a las *Fases del Análisis de Riesgos* tienen un nivel de importancia promedio de 4,8; mientras que las categorías

que abarcan *El Negocio y el Riesgo Tecnológico* alcanzaron una calificación promedio de 4,75.

Además, de las categorías que engloban las *Fases del Análisis de Riesgo* la menor puntuada es *Mejora Continua del Análisis de Riesgo* con una calificación de 4,86; mientras que las otras categorías (E, F, G, H, I y J) alcanzaron una valoración de 5.

Respecto a las categorías que abarcan *El Negocio y el Riesgo Tecnológico* las que obtuvieron menor calificación con un promedio de 4,71 fueron: *Responsabilidad, Compromiso de la Alta Dirección, y Comunicación y Formación;* y se considera como Muy Importante con un promedio de 5 la categoría de *Política de Riesgo.*

En la Figura 9 y 10 se sintetizan los resultados antes descritos.

Figura 9: Importancia de las Categorías a Evaluar para el Análisis de Riesgo de las Entidades Navieras en Relación al Negocio y el Riesgo Tecnológico.
Fuente: (Consulta a Expertos, 2017).

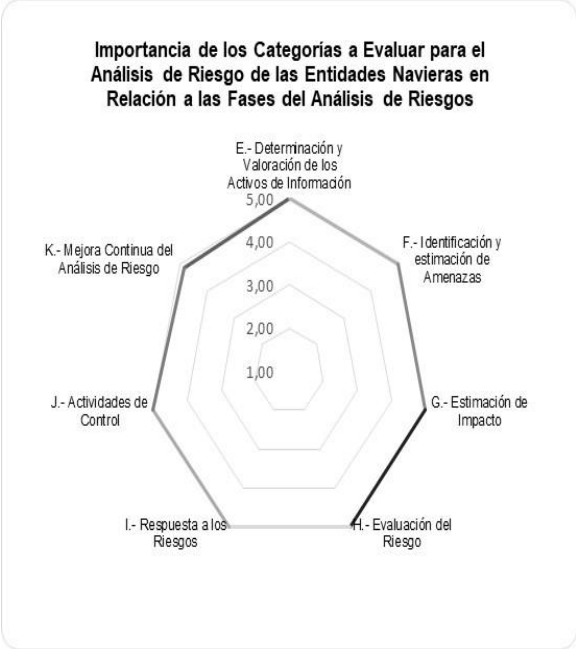

Figura 10: Importancia de las Categorías a Evaluar para el Análisis de Riesgo de las Entidades Navieras en relación a las Fases del Análisis de Riesgos.
Fuente: (Consulta a Expertos, 2017).

En la sección del cuestionario *Aplicabilidad en las Agencias Navieras de las Mejores Prácticas de las Metodologías MAGERIT, OCTAVE y MEHARI* se obtiene como resultados en las Categorías que engloban a El Negocio y el Riesgo Tecnológico los siguientes aspectos:

De la categoría *Política de Riesgo* la mejor práctica evaluada es la A.1 con una aplicabilidad de 4,86, la cual señala que *Existe una política formal de riesgo aprobada por la autoridad responsable y que transciende a pesar de cambios de personal en la alta dirección.* Mientras que, la práctica menor calificada con un puntaje de 4,57 es la A.4 que establece *La política incluye una definición de la cantidad de riesgo (apetito de riesgo) que la entidad puede aceptar, y puede estar descrita en términos cuantitativos o cualitativos.*

En la categoría *Responsabilidad,* la práctica mejor calificada es la B.2 con una valoración de 4,71 la cual señala *Los roles del equipo de análisis de riesgo están claramente definidos, asignados y documentados.* Pero, la práctica menor valorada es la B.1 que indica *La entidad*

posee un departamento de TI con un equipo de análisis de riesgo, siendo su puntaje de 3,71.

Para la categoría C*ompromiso de la Alta Dirección* los expertos consideraron que las prácticas C.1 y C.2 tenian el mismo nivel de aplicabilidad, siendo su puntaje de 4,86.

Respecto a la categoría *Comunicación y Formación,* la mejor práctica evaluada fue D.2 con una valoración de 4,71, la misma que indica *Existen programas de capacitación formalizada para establecer una cultura de riesgo y asegurar que el personal de la entidad entiende la política de riesgo.* Mientras que, la práctica D.3 obtuvo el menor puntaje con una ponderación de 4, la cual señala *Se informa periódicamente y de forma inmediata a la alta dirección la consolidación de un riesgo.*

En la Figura 11 se consolidan los resultados de las buenas prácticas relacionados a las categorias A, B, C y D.

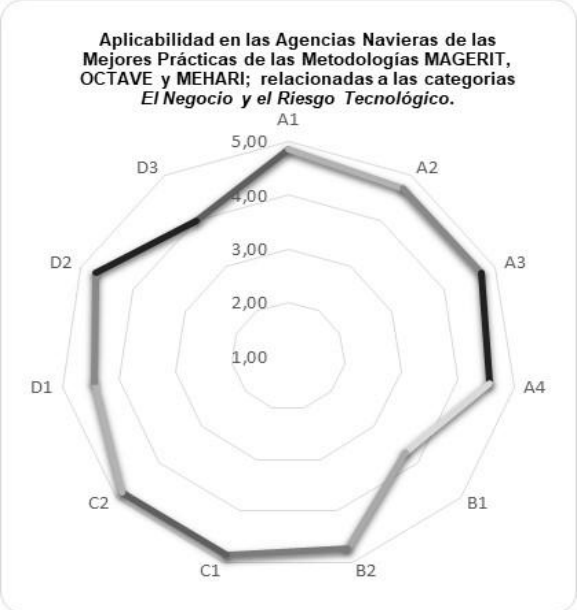

Figura 11: Aplicabilidad en las Agencias Navieras de las Mejores Prácticas de las metodologías MAGERIT, OCTAVE y MEHARI; relacionadas a las Categorías *El Negocio y el Riesgo Tecnológico.*
Fuente: (Consulta a Expertos, 2017).

Así mismo, de las categorías que abarcan las *Fases de Analisis de Riesgo* se obtuvieron los siguientes resultados:

En la categoría *Determinación y Valoración de los Activos de Información* la mejor práctica evaluada fue la E.1 con una valoración de 4,71 la cual indica *Los activos/recursos TI han sido clasificados en base a una perspectiva;* y la práctica que obtuvo una menor calificación fue E.2 con un puntaje de 4,43 y señala *Se cuenta con un perfil que describe características únicas, cualidades, dependencia y valor de los activos de información.*

Para la categoría *Identificación y estimación de Amenazas* se le otorgó a la práctica F.2 una aplicabilidad de 5, y esta indica *Por cada amenaza identificada se ha definido la dimensión de disponibilidad, integridad, y confidencialidad; que puede resultar afectada en el activo de información.* Mientras que la práctica F.1 fue valorada con 4,86 y señala que *La empresa analiza exhaustivamente las amenazas externas e internas a los que pueden verse afectados los activos de información.*

De la categoría *Estimación de Impacto* se determinó que la práctica G.1 es aplicable con una calificación de 4,86 y denota que *Se ha establecido una escala de impacto considerando la gravedad de las consecuencias de la materialización de una amenaza.* En este mismo ámbito la práctica G.2 tuvo un puntaje de 4,57 y establece que *Se ha ponderado el impacto acumulado tomando en cuenta la degradación causada por la amenaza, y el impacto repercutido teniendo en cuenta el valor propio del activo y las amenazas a los que está expuesto.*

En la categoría *Evaluación del Riesgo* los profesionales establecieron estar de acuerdo que la práctica H.2 es aplicable con un puntaje de 4,86; e indica *Los riesgos son clasificados a partir de una escala que considera la probabilidad e impacto, con la finalidad de priorizar los más significativos.* Además, la práctica H.1 tuvo una valoración de 4,57 y puntualiza *Se ha definido el riesgo acumulado considerando la degradación causada y la frecuencia de la amenaza; y se ha definido el*

riesgo repercutido calculando el daño en los activos explícitamente valorados.

Respecto a la categoría *Respuesta a los Riesgos* los expertos consideraron que las prácticas I.1 e I.2 tenian el mismo nivel de aplicabilidad, siendo su puntaje de 5. Mientras que la práctica I.3 fue calificada con una valoración de 4,71.

Para la categoría *Actividades de Control* se ponderaron las prácticas J.1, J.2 y J.3 con 4,57. Mientras que para la categoría *Mejora Continua del Análisis de Riesgo* se valoró la práctica K.2 con un puntaje de 5 la misma que señala *La presencia de nuevos riesgos se identifican sistemáticamente de manera oportuna y proactiva;* y en este mismo contexto se determinó que la práctica K.1 tenía una aplicabilidad de 4,71 que establece *Exhaustiva recopilación de información para el seguimiento, revisión y aprendizaje en torno al análisis de riesgo.*

En la Figura 12 se consolidan los resultados de las buenas prácticas relacionados a las categorías E, F, G, H, I, J y K.

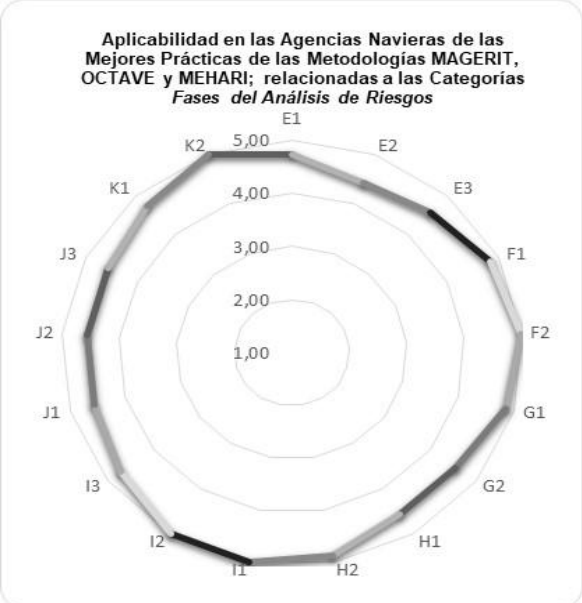

Figura 12: Aplicabilidad en las Agencias Navieras de las Mejores Prácticas de las Metodologías MAGERIT, OCTAVE y MEHARI; relacionadas a las categorías *Fases del Análisis de Riesgo.*
Fuente: (**C**onsulta a Expertos, 2017).

Si comparamos el promedio de las mejores prácticas relacionadas a las categorías de *El Negocio y el Riesgo Tecnológico* en contraposición a las que engloban el *Análisis de Riesgo de los Activos de Información*; se puede deducir que estas últimas obtuvieron un mejor promedio (4,71), lo cual concuerda con el alto nivel de importancia que le dieron los profesionales en la sección del cuestionario *Importancia de las Categorías en el Modelo de Madurez en las Entidades Navieras,* antes detallado.

También, se puede señalar que las prácticas mejor valoradas y que alcanzaron una puntuación de cinco fueron: F.2, del criterio *Identificación y estimación de Amenazas;* I.1 e I.2, del criterio *Respuesta a los Riesgos*; y K.2 del criterio *Monitoreo y Ejecución*; las cuales son afines a las tres metodologías. Sin embargo, la menor puntuada es la B.1 del criterio *Responsabilidad,* con una aplicabilidad de 3,71 y pertenece a la metodología MAGERIT. Cabe indicar que ninguna práctica escogida recibió una calificación de 1 o 2 según la escala.

Por otra parte, la aplicabilidad promedio de todas las prácticas expuestas es de 4,67. Además, por metodologías se obtuvo que las prácticas de OCTAVE tienen un promedio valoración de 4,73; las prácticas de MEHARI 4,80; y las de MAGERIT un puntaje de 4,67.

Finalmente, en la Sección que solicitaba *Definir la Pertinencia de cada Buena Práctica a un determinado Nivel de Madurez* se obtuvieron como resultados los siguientes aspectos:

El 100% de los expertos consideraron que las prácticas A.1 y A.2 deberían constar en el tercer nivel de madurez. Además, el 71.43% de los encuestados ubicaron las prácticas A.3 y A.4 en el cuarto nivel de madurez y el 28.57% sugirieron el quinto nivel.

Así mismo, el 100% de los expertos situaron la práctica B.1 en el tercer nivel de madurez; y en

relación a la práctica B.2 el 71.43% de los encuestados valuaron su correspondencia al tercer nivel mientras el 28.57% restante la correlacionaron en el cuarto nivel de madurez.

Respecto a las prácticas C.1 y C.2 el 57.14% de los profesionales consultados las situaron en el cuarto nivel de madurez y en contraparte el 42,86% las emplazaron al tercer nivel.

En relación a las prácticas D.1 y D.3 el 71.43% de los encuestados señalaron su correspondencia al cuarto nivel de madurez y el 28.57% al tercer nivel. Por otra parte, la práctica D.2 fue catalogada por el 71.43% de los profesionales como pertinente en el tercer nivel de madurez y el 28.57% restante la ubicaron en el cuarto nivel.

Además, la práctica F.1 con un 85.71% fue considerada por los expertos para el tercer nivel de madurez y el 14.29% la calificaron para el cuarto nivel. Así mismo, la práctica F.2 con un 57.14% fue ubicada por los profesionales en el tercer nivel de madurez y el 42.86% la valuaron en el cuarto nivel.

El 71.43% de los expertos consideraron que la práctica G.1 debe ubicarse en el tercer nivel de madurez y en contraparte el 28.57% la situaron en el cuarto nivel. De la práctica G.2 el 57.14% de los encuestados la relacionaron al tercer nivel de madurez y el 42.86% la emplazaron al cuarto nivel.

En las prácticas H.1 y H.2 el 57.14% de los profesionales las correlacionaron al tercer nivel de madurez, en cambio el 42.86% las situaron en el cuarto nivel.

En relación a la mejor práctica I.1 el 57.14% de los encuestados la precisaron para el tercer nivel madurez y el 42.86% la ubicaron en el cuarto nivel. La práctica I.2 fue catalogada para el tercer nivel de madurez por un 71.43% de los profesionales mientras que el 28.57% señalaron el cuarto nivel. Además, la buena práctica I.3 fue situada en el cuarto nivel de madurez por el 100% de los expertos.

Respecto a la práctica J.1 el 100% de los profesionales precisaron el cuarto nivel de madurez, y las prácticas J.2 y J.3 también fueron ubicadas en el cuarto nivel, pero por el 71.43% de los profesionales en contraposición al 28.57% que las emplazaron al quinto nivel.

Por otra parte, las prácticas K.1 y K.2 fueron correlacionadas al quinto nivel de madurez por el 100% de los encuestados.

Al comparar los resultados obtenidos con el *Mapa de Control Propuesto* (Tabla 2) se puede discernir que existen diferencias en la pertinencia de las mejores prácticas: los profesionales no situaron ninguna buena práctica en el segundo nivel de madurez, mientras que en la propuesta se planteaban dos; en el tercer nivel de madurez los expertos sugieren dieciséis mejores prácticas, pero en la propuesta se establecieron trece; en el cuarto nivel de madurez los encuestados correlacionaron diez prácticas y en el diseño se proyectaban nueve; finalmente en el quinto nivel de madurez ellos ubicaron dos mejores prácticas, sin embargo, en la propuesta se sugerían cuatro. Por ello, basándose en estas apreciaciones, la propuesta de Mapa de Control se replantea en la Tabla 6.

Tabla 6: Propuesta de Mapa de Control (reestructurado en base a los resultados obtenidos en la encuesta).

Categorías a Evaluar	Nivel 1: Inicial	Nivel 2: Repetible	Nivel 3: Definido	Nivel 4: Administrado	Nivel 5: Optimizado
A. Política de Riesgo	No se esperan prácticas formales.	Las prácticas son reactivas.	A1, A2	A3, A4	
B.- Responsabilidad			B1, B2		
C.- Compromiso de la Alta Dirección				C1, C2	
D.- Comunicación y Formación			D2	D1, D3	
E.- Determinación y Valoración de los Activos de Información			E1, E2, E3		
F.- Identificación y estimación de Amenazas			F1, F2		
G.- Estimación de Impacto			G1, G2		
H.- Evaluación del Riesgo			H1, H2		
I.- Respuesta a los Riesgos			I1, I2	I3	
J.- Actividades de Control				J1, J2,J3	
K.- Mejora Continua del Análisis de Riesgo					K1, K2

Fuente: (Encuesta a **E**xpertos, 2017).

En base a los resultados antes descritos, y relacionando la puntuación promedio de aplicabilidad otorgado por los expertos a las mejores prácticas agrupadas por niveles de madurez (siguiendo el Mapa de Control, las prácticas mejor evaluadas se encuentran en el nivel 3 y son: F.2, I.1 e I.2); se proyecta que aplicando este modelo las empresas navieras pueden alcanzar progresivamente un nivel de madurez *Definido,* lo cual representa la existencia de un enfoque formal de análisis de riesgo en el que consta una política de riesgo aprobada por una autoridad responsable, la distinción y organización de los activos de información, el análisis de las amenazas internas y externas que pueden verse afectados los activos, una respuesta por cada riesgo identificado, entre otras buenas prácticas.

CONCLUSIONES

Un modelo de madurez es un camino de mejoramiento evolutivo que orienta a una organización a la consecución de la excelencia en un ámbito en particular, siendo necesario la implementación de prácticas específicas; y considerando que el CMMI es un modelo pionero de la ingeniería, su estructura permitió definir las especificaciones en los niveles del modelo planteado.

Las metodologías MAGERIT, OCTAVE y MEHARI se fundamentan en lineamientos prácticos claramente definidos, documentados y compatibles lo que permitió llevar a cabo un escogimiento basado en las estrategias primordiales que requieren las fases del análisis de riesgos asociados a los activos de información, evitando las ambigüedades de estos estándares.

El Modelo planteado es el resultado de integrar los niveles de madurez con las mejores prácticas de las metodologías antes descritas; lo cual fue posible a través de la Propuesta de un Mapa de Control, el mismo que orienta su consecución paulatina. No obstante, las especificaciones de requerimientos pueden ser halladas en la documentación formal de las metodologías.

El Modelo desarrollado se enfoca en establecer una categorización del grado de madurez alcanzado en las empresas navieras de acuerdo a las prácticas de análisis de riesgo adoptadas, lo cual les permitirá detectar sus falencias actuales y priorizar las categorías que deben mejorar o adquirir para avanzar a un nivel superior (hasta obtener el nivel Optimizado); por consecuencia se logrará una mejor eficiencia en el manejo de riesgos de los activos de información.

La Propuesta del Modelo de Madurez se validó a través del método Delphi, el cual permitió determinar con valiosos datos cuantitativos la aplicabilidad del diseño; además, esta técnica admitió que los expertos pudieran establecer la correlación de cada buena práctica a un nivel de madurez especifico.

Durante la validación del modelo propuesto se pudo apreciar una tendencia favorable de aceptación de las Niveles Madurez Sugeridos, las Categorías a Evaluar y las Mejoras Prácticas Seleccionadas; sin embargo, existieron diferencias respecto a la pertinencia de las buenas prácticas por nivel de madurez que se exponen en el Mapa de Control, siendo necesaria su reestructuración en base a la percepción de los expertos.

En términos generales se considera que el modelo propuesto es adaptable a las empresas navieras, además se estima en relación al promedio de aplicabilidad otorgado por los expertos a las mejores prácticas agrupadas por niveles de madurez que su aplicación conlleve la consecución de un nivel de madurez *Definido,* logrando de esta manera que el Análisis de Riesgo este formalizado y con estrategias proactivas.

Dentro de las limitaciones de esta investigación se encuentra que el Modelo Propuesto

resultante es conceptual, por lo tanto, su validez es teórica. Además, ciertos expertos convocados han laborado en entidades de otros sectores, lo cual pudo haber influido en las respuestas dadas.

En un futuro, siguiendo esta línea investigativa se sugiere la implementación y prueba del Modelo en una entidad naviera real, cuyos resultados permitirán medir la eficiencia de las Categorías a Evaluar definidas, así como la pertinencia de las Mejores Prácticas según el nivel de madurez; lo cual puede ser contrastado con los resultados obtenidos en este artículo. También, en un siguiente momento este modelo puede ser ampliado para incluir en el diseño la Gestión de Riesgo de tal manera, que se evalúe si la madurez es acorde con el nivel de riesgo aceptado por la empresa.

REFERENCIAS BIBLIOGRÁFICAS

Aguilera, P. (2010). Seguridad Informática. Madrid, España: Editex

Alberts, C. & Dorofee, A. (2002). Managing Information Security Risks: The OCTAVE Approach. Boston, USA: Addison-Wesley

Alberts, C., Dorofee, A., Stevens, J. & Woody, C. (2003). Introduction to the OCTAVE® Approach. Recuperado de https://www.itgovernance.co.uk/files/Octave.pdf

Alemán, H., y Rodríguez, C. (2014). Metodologías para el análisis de riesgo en los SGSI. Revista Especializada en Ingeniería, 9, 73-86. Recuperado de http://oaji.net/articles/2017/5082-1501187567.pdf

Amador, S. (2014). *Gestión de Riesgo con base a la ISO 27005 adaptando OCTAVE-S* (Tesis de Maestría). Universidad Internacional de la Rioja, Logroño, España.

A.P.M. (2016). *Agencias Navieras.* Recuperado de http://www.puertodemanta.gob.ec/clientes/agencias-navieras

Asesoría Económica & Marketing. (2009). *Calculadora de Muestras.* Recuperado de http://www.corporacionaem.com/tools/calc_muestras.php

Areitio, J. (2008). Seguridad de la Información. Redes, Informática y Sistemas de Información. Madrid, España: Paraninfo.

Beato, N. (2012). *Las Navieras*. Recuperado de https://acento.com.do/2012/opinion/203028-las-navieras/

Becker, J., Niehaves, B., Poppelbus, J., & Simons, A. (2010). Maturity Models in IS Research. *ECIS, 42*, 1-12. Recuperado de https://webdocs.uni.li/public/04046167.PDF

Bracho, D., Rincón, C. y Acurero, A. (2010). Modelo para la cuantificación del riesgo telemático en una organización. *Enl@ce Revista Venezolana de Información, Tecnología y Conocimiento, 7*(2), 63-81. Recuperado de http://www.redalyc.org/html/823/82315410005/

Canal, V. (2006). *Seguridad de la información, Expectativas, Riesgos y Técnicas de Protección*. Ciudad de México, México: Editorial LIMUSA.

Carcay, M. (2013). IT Risk Management: A Capability Maturity Model Perspective. *The Electronic Journal Information Systems Evaluation, 16 (1),* 3-13. Recuperado de www.ejise.com/issue/download.html?idArticle=858

Carvajal, A. (2013). *Análisis y Gestión de Riesgos, base fundamental del SGSI. Caso Metodología MAGERIT.* Recuperado de http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/17-ElAnalisisRiesgosBaseSistemaGestionSeguridadInformacionCasoMagerit.pdf

Caralli, R., Stevens, J., Young, L. & Wilson, W. (2007). *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process.* Recuperado de https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf

CERT. (2013). *OCTAVE*. Recuperado de http://www.cert.org/resilience/products-services/octave/

Chu, Y., Wei, Y. & Chang, W. (2013). A risk recommendation approach for information security risk assessment. *IEICE*, *10*, 1-3. Recuperado de http://i-scover.ieice.org/proceedings/APNOMS/2013/pdf/P3-10-116166.pdf

CLUSIF. (2010a). *MEHARI.* Recuperado de https://clusif.fr/publications/mehari-2010-guide-de-lanalyse-des-enjeux-et-de-la-classification/

CLUSIF. (2010b). *MEHARI: Risk analysis and treatment Guide.* Recuperado de

http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-Risk-Analysis-and-Treatment-Guide.pdf

Crawford, J. (2002). Project management maturity model: Providing a proven path to project management excellence. New York: Marcel Dekker.

Curiman, F. y Toth, G. (2004). *Análisis de riesgos. Técnicas, metodologías y herramientas para el desarrollo de un Análisis de Riesgos.* Recuperado de https://es.scribd.com/document/96314331/Analisis-de-Riesgos-Curiman-Toth

Dong, X. HYPERLINK "https://scholars.cityu.edu.hk/en/persons/ben-liu (5a21b34d-2e3e-4adb-b5d5-0f40b2c2782d).html", Liu, Q., & Yin, D. (2008). Business Performance, Business Strategy, and Information System Strategic Alignment: An Empirical Study on Chinese Firms. HYPERLINK "https://scholars.cityu.edu.hk/en/journals/tsinghua-science-and-technology (f49ed3f9-99ea-47be-bf1d-b1e38a4f10b7)/publications.html" Tsinghua *Science and Technology, 13*(3), 348-354. DOI: 10.1016/S1007-0214(08)70056-7

Echenique, J. (2012). *Auditoría Informática.* Ciudad de México, México: McGraw-Hill

ENISA. (2006). *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools.* Recuperado de https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

Espinoza, D., Martínez, J., y Amador, S. (2014). Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC 27005 de 2011, proponiendo una adaptación de la metodología OCTAVE-S. Caso de estudio: Proceso de Inscripciones y Admisiones en la división de Admisión Registro y Control Académico (Darca) De La Universidad Del Cauca. *Ing. USBMed, 5*(2), 1-11. Recuperado de http://web.usbmed.edu.co/usbmed/fing/v5n2/pdf/Articulo_Gestion_Riesgo_Seguridad_Informacion

Eterovic, J. y Pagliari, G. (2011). Metodología de Análisis de Riesgos Informáticos. *Cyta, 10*(1), 1-5. Recuperado de http://www.cyta.com.ar/ta1001/v10n1a3.htm

Fernández, E., Moya, R. y Piattini, M. (2003). *Seguridad de las Tecnologías de Información: La Construcción de la Confianza para una sociedad conectada*. Madrid, España: AENOR.

Galarza, J. y Uriona, C. (2012). Modelos de Madurez en los Datos de una Organización; Caso de Estudio Universidad Católica Boliviana "San Pablo" Cochabamba. *ACTA NOVA, 5*(4), 462-476. Recuperado de *www.scielo.org.bo/pdf/ran/v5n4/v5n4_a03.pdf*

Gómez, L., Farías, M., y Mendoza, M. (2003). *Importancia del Análisis de Riesgo de Seguridad.* Recuperado de http://seguridad.internet2.ulsa.mx/congresos/2003/cudi2/impariesgo.pdf.

Gómez, R., Pérez, D., Donoso, Y., y Herrera, A. (2010). Metodología y Gobierno de la Gestión de Riesgos de Tecnologías de la Información. *Revista de Ingeniería Universidad de los Andes,* (31), 109-118. Recuperado de http://www.scielo.org.co/pdf/ring/n31/n31a12.pdf

Gupta, S., & Xu, H. (2010). Examining the Relative Influence of Risk and Control on Intention to Adopt Risky Technologies. *Journal of technology management & innovation*, *5*(4), 22-37. DOI: https://dx.doi.org/10.4067/S0718-27242010000400003

Hernández, A, y Mejía, J. (2015). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *ReCIBE. Revista electrónica de Computación, Informática Biomédica y Electrónica, 4*(1), 1-18. Recuperado de http://www.org.redalyc.org/articulo.oa?id=512251501005

INCIBE. (2015). *Gestión de Riesgos.* Recuperado de https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf

INCIBE. (2017). HYPERLINK "https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo" *Análisis de riesgos en 6 pasos.* Recuperado de https://www.incibe.es/protege-tu-empresa/blog/analisis-riesgos-pasos-sencillo

Januszkiewicz, P. & Marek, P. T*he OCTAVE methodology as a risk analysis tool for business resources.* Recuperado de http://www.proceedings2006.imcsit.org/pliks/160.pdf

Jugdev, K. & Thomas, J. (2002). Project management maturity models: The silver bullets of competitive advantage. *Project Management Journal, 33*(4), 4–14. Recuperado de https://dspace.ucalgary.ca/bitstream/1880/44250/1/2002%20PMJ%20PM%20maturity%20models.pdf

Kerzner, H. (2000). Gestión de Proyectos: Un enfoque sistemático para la planificación, programación y control, John Wiley and Sons, New York.

Klimko, G. (2001). *Knowledge management and maturity models: Building common understanding.* Paper presented at Proceedings of the 2nd European Conference on Knowledge Management, Bled, Slovenia.

Llop, M., Escamilla, M., Furió, S., Galdón, M., García, L., García, J. Lara, J. y Navarro, C. (2013). Tendencias TIC en puertos. Valencia, España: Fundación Valenciaport

Maggiore, M. (2014). *Modelo de Evaluación de Madurez para la Gestión de la Seguridad de la Información* (Tesis de Maestría). Universidad de Buenos Aires, Buenos Aires, Argentina.

Maldonado, D. (2013). *Gestión de Riesgos Informáticos para la Protección de los Sistemas de Información en la Cooperativa de Ahorro y Crédito Campesina COOPAC* (Tesis de Maestría). Universidad Regional Autónoma de Los Andes, Ambato, Ecuador.

Matrane, O., Talea, M. & Okar, C. (2014). Towards A New Maturity Model for Information System. I*nternational Journal of Computer Science Issues, 12*(3), 268-275. Recuperado de https://www.ijcsi.org/papers/IJCSI-12-3-268-275.pdf

Mayer, J. y Lemes, L. (2008). *M*odelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação. *VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais.* Simposio llevado a cabo en São Leopoldo, Brasil.

Mettler, T. (2009). A design science research perspective on maturity models in Information Systems. Recuperado de https://www.alexandria.unisg.ch/214531/1/20090512%2520Maturity%2520Model%2520Design.pdf

Ministerio de Hacienda y Administración Pública del Gobierno de España. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Recuperado de https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html

MINTIC. (2016). *Guía para la Gestión y Clasificación de los Activos de Información.* Recuperado de https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Molina, D. (2007). *Modelo Económico para la Administración de Riesgos – Madurando a "Security 2.0".* Recuperado de http://cito.gov.jm/files/summit2009presentations/Security%202%200%20Presentation%20Dan%20Molina%20%20Infotech%20%20McAfee%20%20Thurs%2021%20May%202009.pdf

Mundo Marítimo (2010). *Las TIC en el desarrollo portuario latinoamericano*. Recuperado de http://www.mundomaritimo.cl/noticias/las-tics-en-el-desarrollo-portuario-latinoamericano

Nagata, K., Amagasa, M. & Kigawa, Y. (2009). *Method to select Effective Risk Mitigation Controls Using Fuzzy Outranking*. Recuperado de http://ieeexplore.ieee.org/document/5364934/

OPM3. (2003). *Organizational project management maturity model.* Recuperado de http://faculty.kfupm.edu.sa/MGM/bubshait/project%20management/PDF/opm3KF.pdf

Peláez, J., (2005). *Herramientas para el Desarrollo del Software.* Recuperado de: http://www.lcc.uma.es/~jignacio/index_archivos/TEMA5.pdf.

Peltier, T. (2005). *Information Security Risk Analysis*. USA: 2005.

Ramírez, A. (2012). Riesgo Tecnológico y su impacto para las Organizaciones Parte II Gobierno de TI y Riesgos. *Revista Seguridad, 15,* 23-26. Recuperado de https://revista.seguridad.unam.mx/sites/default/files/revistas/pdf/SeguridadNum15.pdf

Reguant, M. y Torrado, M. (2016). El método Delphi. *REIRE*, *9*(1), 87-102. DOI: 10.1344/reire2016.9.1916

Rosemann, M. & De Bruin, T. (2005). *Towards a business process management maturity model.* Recuperado de https://eprints.qut.edu.au/25194/1/25194_rosemann_2006001488.pdf

Röglinger, M. & Pöppelbuß, J. (2011). What makes a useful maturity model? A framework for general design principles for maturity models and its demonstration in business process management. *FIM, 28*, 1-13. Recuperado de http://fim-rc.de/Paperbibliothek/Veroeffentlicht/327/wi-327.pdf

Sotelo, M., Torres, J. y Rivera, J. (Octubre de 2012). Un proceso práctico de análisis de riesgos de activos de información. *IV Congreso Internacional de Computación y Telecomunicaciones COMTEL*. Congreso llevado a cabo en Lima, Perú.

Sylim, A., Hori, Y. & Sakurai, K. (2009). C*omparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide*. Recuperado de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.165.6972&rep=rep1&type=pdf

Tarazona, C. (2012). *Amenazas informáticas y seguridad de la información.* Recuperado de http://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915

Voutssas, J. (2010). Preservación documental digital y seguridad informática. *Investigación bibliotecológica*, *24*(50), 127-155. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008&lng=es&tlng=es

ANEXO 1: Compendio de Respuestas de las Entrevistas.

Entrevistado 1:

1. **¿Considera que existe una Metodología adecuada para realizar un Análisis de Riesgo en las Entidades Navieras?**
   Las metodologías existentes están orientadas a todo tipo de empresa, no existe una específica para las navieras. Por ello, en ocasiones se adoptan prácticas indistintas de las metodologías actuales.

2. **¿Cuáles son los principales problemas que afronta el Departamento de TI durante el proceso de Análisis de Riesgos?**
   Existen algunos problemas, pero el principal es que la empresa tiende a crecer en tecnología anualmente debido a que se incrementan los requerimientos de los Armadores Pesqueros en lo que respecta a información. Por lo tanto, se restructuran los servicios y ello requiere modificar las medidas de seguridad que deben responder adecuadamente a los riesgos del entorno.

3. **¿Considera usted que un Modelo de Madurez que determine el status actual en relación al Análisis de Riesgos de los activos de información sería una herramienta útil en el Departamento de TI?**
   Un Modelo de Madurez aportaría en gran magnitud en el proceso de Análisis de Riesgo, porque permitiría enfocarnos en un nivel específico para lograr un crecimiento posterior.

Entrevistado 2:

1. **¿Considera que existe una Metodología adecuada para realizar un Análisis de Riesgo en las Entidades Navieras?**
   No existe una metodología específica, sin embargo, se ha utilizado MAGERIT y los resultados han permitido palpar brechas de riesgos.

2. **¿Cuáles son los principales problemas que afronta el Departamento de TI durante el proceso de Análisis de Riesgos?**
   Considero que los cambios de líderes en Departamento TI es uno de los grandes problemas que se ha afrontado en los procesos de Análisis de Riesgo, debido a que cada Jefe tiene sus lineamientos, políticas y preferencias en el manejo de riesgo; lo que ha originado inestabilidad, retrasos y desacuerdos en las medidas implantadas.

3. **¿Considera usted que un Modelo de Madurez que determine el status actual en relación al Análisis de Riesgos de los activos de información sería una herramienta útil en el Departamento de TI?**
   Un Modelo de Madurez nos permitiría definir una ruta a seguir, por ello considero que sería un aporte fundamental en el Análisis de Riesgo.

Entrevistado 3:

1. **¿Considera que existe una Metodología adecuada para realizar un Análisis de Riesgo en las Entidades Navieras?**
   Para las entidades navieras no se ha desarrollado una Metodología de Análisis de Riesgo, sin embargo, las existentes pueden adoptarse a este entorno, pero se requiere una revisión del tamaño de la empresa para definir la más adecuada.

2. **¿Cuáles son los principales problemas que afronta el Departamento de TI durante el proceso de Análisis de Riesgos?**

Cuando se ha desarrollado el proceso de Análisis de Riesgo un problema que se ha suscitado reiterativamente es la no continuidad, es decir no existe un control progresivo de los riesgos a los que pueden estar expuestos los nuevos procesos implantados que hacen uso de las TI, lo cual está relacionado a la estimación de riesgo, apetito, y consecuencias de ocurrencias.

3. **¿Considera usted que un Modelo de Madurez que determine el status actual en relación al Análisis de Riesgos de los activos de información sería una herramienta útil en el Departamento de TI?**
   Sería una herramienta muy útil, porque permitiría establecer un mayor control del proceso de análisis y gestión de riesgos.

Entrevistado 4:

1. **¿Considera que existe una Metodología adecuada para realizar un Análisis de Riesgo en las Entidades Navieras?**
   Cada una de las metodologías existentes tienen rasgos que pueden ser utilizados en las Entidades Navieras, sin embargo, en esta entidad consideramos que OCTAVE satisface muchos de los requerimientos en lo que respecta al análisis de riesgos.

2. **¿Cuáles son los principales problemas que afronta el Departamento de TI durante el proceso de Análisis Riesgos?**
   El apoyo de la alta dirección en ocasiones ha sido un problema en este proceso, debido a que al incrementarse los requerimientos de TI es preciso evaluar su resistencia a riesgo y a pesar de exponer esta necesidad se cree que es muy repetitivo, que esta evaluación debe realizarse con menos frecuencia.

3. **¿Considera usted que un Modelo de Madurez que determine el status actual en relación al Análisis de Riesgos de los activos de información sería una herramienta útil en el Departamento de TI?**
   Considero que una propuesta de este tipo mejoraría este proceso debido a que nos enfocaríamos a realizar prácticas específicas según el nivel actual en que la empresa se ubique.

Entrevistado 5:

1. **¿Considera que existe una Metodología adecuada para realizar un Análisis de Riesgo en las Entidades Navieras?**
   No existe una Metodología diseñada para las Empresas Navieras, sin embargo, se suele trabajar con aquella que contenga pasos eficaces y estratégicos. Según mi criterio esta metodología es MAGERIT.

2. **¿Cuáles son los principales problemas que afronta el Departamento de TI durante el proceso de Análisis de Riesgos?**
   La apertura de una nueva sucursal en este año nos ha hecho revalorizar y reestructurar las medidas de seguridad por ello fue necesario un análisis de riesgo en la que tuvimos como dificultad el cambio de Jefe de TI y cambio de política, lo cual retrasó notoriamente este proceso.

3. **¿Considera usted que un Modelo de Madurez que determine el status actual en relación al Análisis de Riesgos de los activos de información sería una herramienta útil en el Departamento de TI?**
   Toda herramienta que contribuya al mejoramiento de un proceso como el Análisis de Riesgo es de gran utilidad, más aún cuando ésta permitirá visualizar la excelencia en la gestión de riesgo a través del cumplimiento de diferentes etapas.

ANEXO 2: Tabulación de Resultados a Expertos

Tabla 7: Perfil de los Encuestados

Características	Categorización	Frecuencia
Experiencia Laboral	5- 10 años	1
	11-15 años	0
	16-20 años	1
	21-25 años	2
	Más de 25 años	3
Cargo	Alta Dirección	3
	Asistentes de TI	4
Ubicación	Manta	6
	Guayaquil	1
Nivel de Estudios	Tercer Nivel	0
	Cuarto Nivel	7
Certificaciones Obtenidas	Auditor Interno ISO 27001	1
	CISCO CNNA	3
	Certificación Superior DBA ESPOL	1
	MIT EMTECH.	1

Fuente: (**C**onsulta a Expertos, 2017).

Tabla 8: Niveles de Madurez y su Aplicabilidad en las Entidades Navieras.

Nivel	Escala	Frecuencia
Totalmente en Desacuerdo	1	0
En desacuerdo	2	0
Ni de acuerdo ni en desacuerdo	3	0
De acuerdo	4	1
Totalmente de Acuerdo	5	6

Fuente: (**C**onsulta a Expertos, 2017).

Tabla 9: Importancia de las Categorías a Evaluar para el Análisis de Riesgos en las Entidades Navieras.

Categoría a Evaluar	Importancia					Frecuencia	Valoración Obtenida
	1	2	3	4	5		
A.- Política de Riesgo	0	0	0	1	6	7	**4,86**
B.- Responsabilidad (Se cuenta con un Departamento de TI)	0	0	0	2	5	7	**4,71**
C.- Compromiso de la Alta Dirección	0	0	0	2	5	7	**4,71**
D.- Comunicación y Formación	0	0	0	2	5	7	**4,71**
E.- Determinación y Valoración de los Activos de Información	0	0	0	0	7	7	**5,00**
F.- Identificación y estimación de Amenazas	0	0	0	0	7	7	**5,00**
G.- Estimación de Impacto	0	0	0	0	7	7	**5,00**
H.- Evaluación del Riesgo	0	0	0	0	7	7	**5,00**
I.- Respuesta a los Riesgos	0	0	0	0	7	7	**5,00**
J.- Actividades de Control	0	0	0	0	7	7	**5,00**
K.- Mejora Continua del Análisis de Riesgo	0	0	0	1	6	7	**4,86**

Fuente: (**C**onsulta a Expertos, 2017).

Tabla 10: Aplicabilidad de las Mejores Prácticas en base a las Metodologías MAGERIT, OCTAVE y MEHARI en Empresas Navieras.

Buena Práctica	Aplicabilidad					Frecuencia	Valoración Obtenida
	1	2	3	4	5		
A.1.- Existe una política formal de riesgo aprobada por la autoridad responsable y que transciende a pesar de cambios de personal en la alta dirección.	0	0	0	1	6	7	**4,86**
A.2.- La política ha sido comunicada a toda la entidad.	0	0	0	2	5	7	**4,71**
A.3.- La política de riesgo es revisada y actualizada para incluir los cambios del entorno interno y externo.	0	0	0	2	5	7	**4,71**
A.4.- La política incluye una definición de la cantidad de riesgo (apetito de riesgo) que la entidad puede aceptar, y puede estar descrita en términos cuantitativos o cualitativos.	0	0	1	1	5	7	**4,57**
B.1.- La entidad posee un departamento de TI con un equipo de análisis de riesgo.	0	0	3	3	1	7	**3,71**
B.2.- Los roles del equipo de análisis de riesgo están claramente definidos, asignados y documentados. Por ejemplo: El personal verifica que las prácticas de respuestas al riesgo sean acordes a la política establecida, coordina los planes de acción así como también la consistencia y exactitud del proceso, aprueba el apetito de riesgo en la entidad.	0	0	0	2	5	7	**4,71**
C.1.- La alta dirección es un apoyo activo para el equipo de análisis de riesgo, así por ejemplo: verifica que la política sea compatible con las necesidades de la empresa, evalúa la efectividad del proceso (revisión periódica de los informes del equipo de análisis riesgo) y	0	0	0	1	6	7	**4,86**

está dispuesto a participar del mismo si es necesario.							
C.2.- La alta dirección garantiza los recursos necesarios para llevar a cabo el análisis de riesgo, así como la formación y entrenamiento del personal.	0	0	0	1	6	7	**4,86**
D.1.- La empresa posee un personal altamente calificado en el departamento de TI, por ello se promueve su capacitación permanente.	0	0	1	2	4	7	**4,43**
D.2.- Existen programas de capacitación formalizada para establecer una cultura de riesgo y asegurar que el personal de la entidad entiende la política de riesgo.	0	0	0	2	5	7	**4,71**
D.3.- Se informa periódicamente y de forma inmediata a la alta dirección la consolidación de un riesgo.	0	0	2	3	2	7	**4,00**
E.1.- Los activos/recursos TI han sido clasificados según una perspectiva de: servicios, datos/información, aplicaciones, equipos informáticos, redes de comunicación, soporte de información, equipamiento auxiliar, instalaciones y personal.	0	0	0	2	5	7	**4,71**
E.2.- Se cuenta con un perfil que describe características únicas, cualidades, dependencia (medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior) y valor de los activos de información.	0	0	1	2	4	7	**4,43**
E.3.- Existe una escala de valoración definida, por ejemplo: de tipo logarítmica (la misma tiene como objetivo hacer una valoración cualitativa respondiendo a valoraciones subjetivas por parte del personal de la organización).	0	0	1	1	5	7	**4,57**
F.1.- La empresa analiza exhaustivamente las amenazas externas e internas a los que pueden verse afectados los activos de información.	0	0	0	1	6	7	**4,86**
F.2.- Por cada amenaza identificada se ha definido la dimensión de disponibilidad, integridad, y confidencialidad; que puede resultar afectada en el activo de información.	0	0	0	0	7	7	**5,00**
G.1.- Se ha establecido una escala de impacto considerando la gravedad de las consecuencias de la materialización de una amenaza; por ejemplo: reputación, pérdida de clientes, costos operativos, pérdida de ingresos, pérdidas financieras, horas de trabajo del personal, pérdidas significadas de vida y seguridad.	0	0	0	1	6	7	**4,86**
G.2.- Se ha ponderado el impacto acumulado tomando en cuenta la degradación causada por la amenaza, y el impacto repercutido teniendo en cuenta el valor propio del activo y las amenazas a los que está expuesto	0	0	1	1	5	7	**4,57**
H.1.- Se ha definido el riesgo acumulado considerando la degradación causada y la frecuencia de la amenaza; y se ha definido el riesgo repercutido calculando el daño en los activos explícitamente valorados.	0	0	1	1	5	7	**4,57**
H.2.- Los riesgos son clasificados a partir de una escala que considera la probabilidad e impacto, con la finalidad de priorizar los más significativos.	0	0	0	1	6	7	**4,86**

I.1.- Se determina una respuesta por cada riesgo identificado (la cual es producto de una socialización y consenso) considerando su probabilidad e impacto.	0	0	0	0	7	7	**5,00**
I.2.- Cada respuesta al riesgo está perfectamente desplegada, configurada, mantenida y recaerá en una de estas categorías: *Mitigar,* contiene una o varias estrategias de mitigación, las cuales describen los controles a implantar y los recursos requeridos; *Aceptar,* no deben acarrear graves consecuencias a la organización; *Transferir,* deberán estar incluidos en el plan financiero de la empresa; *Eliminar,* constan de medidas estructurales para lograr su consecución.	0	0	0	0	7	7	**5,00**
I.3.- Se ha definido el riesgo residual que permanecerá cuando una respuesta al riesgo se implemente.	0	0	0	2	5	7	**4,71**
J.1.- Se definen indicadores de desempeño sobre la respuesta a los riesgos para determinar su validez.	0	0	1	1	5	7	**4,57**
J.2.- Los efectos de las respuestas a los riesgos se miden frente al apetito de riesgo.	0	0	1	1	5	7	**4,57**
J.3.- Se evalúa el riesgo residual una vez aplicada la respuesta al riesgo.	0	0	1	1	5	7	**4,57**
K.1.- Exhaustiva recopilación de información para el seguimiento, revisión y aprendizaje en torno al análisis de riesgo.	0	0	0	2	5	7	**4,71**
K.2.- La presencia de nuevos riesgos se identifica sistemáticamente de manera oportuna y proactiva.	0	0	0	0	7	7	**5,00**

Fuente: (**C**onsulta a Expertos, 2017).

Tabla 11: Pertinencia de las Mejores Prácticas a un Nivel de Madurez para las Empresas Navieras.

Buena Práctica	Nivel de Madurez					Frecuencia	Nivel de Madurez Obtenido
	1	2	3	4	5		
A.1.- Existe una política formal de riesgo aprobada por la autoridad responsable y que transciende a pesar de cambios de personal en la alta dirección.	0	0	7	0	0	7	**3,00**
A.2.- La política ha sido comunicada a toda la entidad.	0	0	7	0	0	7	**3,00**
A.3.- La política de riesgo es revisada y actualizada para incluir los cambios del entorno interno y externo.	0	0	0	5	2	7	**4,29**
A.4.- La política incluye una definición de la cantidad de riesgo (apetito de riesgo) que la entidad puede aceptar, y puede estar descrita en términos cuantitativos o cualitativos.	0	0	0	7	0	7	**4,00**
B.1.- La entidad posee un departamento de TI con un equipo de análisis de riesgo.	0	0	7	0	0	7	**3,00**
B.2.- Los roles del equipo de análisis de riesgo están claramente definidos, asignados y documentados. Por ejemplo: El personal verifica que las prácticas de respuestas al riesgo sean acordes a la política establecida, coordina los planes de acción así como también la consistencia y exactitud del proceso, aprueba el apetito de riesgo en la entidad.	0	0	5	2	0	7	**3,29**

C.1.- La alta dirección es un apoyo activo para el equipo de análisis de riesgo, así por ejemplo: verifica que la política sea compatible con las necesidades de la empresa, evalúa la efectividad del proceso (revisión periódica de los informes del equipo de análisis riesgo) y está dispuesto a participar del mismo si es necesario.	0	0	3	4	0	7	**3,57**
C.2.- La alta dirección garantiza los recursos necesarios para llevar a cabo el análisis de riesgo, así como la formación y entrenamiento del personal.	0	0	3	4	0	7	**3,57**
D.1.- La empresa posee un personal altamente calificado en el departamento de TI, por ello se promueve su capacitación permanente.	0	0	2	5	0	7	**3,71**
D.2.- Existen programas de capacitación formalizada para establecer una cultura de riesgo y asegurar que el personal de la entidad entiende la política de riesgo.	0	0	5	2	0	7	**3,29**
D.3.- Se informa periódicamente y de forma inmediata a la alta dirección la consolidación de un riesgo.	0	0	2	5	0	7	**3,71**
E.1.- Los activos/recursos TI han sido clasificados según una perspectiva de: servicios, datos/información, aplicaciones, equipos informáticos, redes de comunicación, soporte de información, equipamiento auxiliar, instalaciones y personal.	0	0	7	0	0	7	**3,00**
E.2.- Se cuenta con un perfil que describe características únicas, cualidades, dependencia (medida en que un activo superior se vería afectado por un incidente de seguridad en un activo inferior) y valor de los activos de información.	0	0	7	0	0	7	**3,00**
E.3.- Existe una escala de valoración definida, por ejemplo: de tipo logarítmica (la misma tiene como objetivo hacer una valoración cualitativa respondiendo a valoraciones subjetivas por parte del personal de la organización).	0	0	5	2	0	7	**3,29**
F.1.- La empresa analiza exhaustivamente las amenazas externas e internas a los que pueden verse afectados los activos de información.	0	0	6	1	0	7	**3,14**
F.2.- Por cada amenaza identificada se ha definido la dimensión de disponibilidad, integridad, y confidencialidad; que puede resultar afectada en el activo de información.	0	0	4	3	0	7	**3,43**
G.1.- Se ha establecido una escala de impacto considerando la gravedad de las consecuencias de la materialización de una amenaza; por ejemplo: reputación, pérdida de clientes, costos operativos, pérdida de ingresos, pérdidas financieras, horas de trabajo del personal, pérdidas significadas de vida y seguridad.	0	0	5	2	0	7	**3,29**
G.2.- Se ha ponderado el impacto acumulado tomando en cuenta la degradación causada por la amenaza, y el impacto repercutido teniendo en cuenta el valor propio del activo y las amenazas a los que está expuesto	0	0	4	3	0	7	**3,43**
H.1.- Se ha definido el riesgo acumulado considerando la degradación causada y la frecuencia de la amenaza; y se ha definido el riesgo repercutido calculando el daño en los activos explícitamente valorados.	0	0	4	3	0	7	**3,43**

H.2.- Los riesgos son clasificados a partir de una escala que considera la probabilidad e impacto, con la finalidad de priorizar los más significativos.	0	0	4	3	0	7	**3,43**
I.1.- Se determina una respuesta por cada riesgo identificado (la cual es producto de una socialización y consenso) considerando su probabilidad e impacto.	0	0	4	3	0	7	**3,43**
I.2.- Cada respuesta al riesgo está perfectamente desplegada, configurada, mantenida y recaerá en una de estas categorías: *Mitigar,* contiene una o varias estrategias de mitigación, las cuales describen los controles a implantar y los recursos requeridos; *Aceptar,* no deben acarrear graves consecuencias a la organización; *Transferir,* deberán estar incluidos en el plan financiero de la empresa; *Eliminar,* constan de medidas estructurales para lograr su consecución.	0	0	5	2	0	7	**3,29**
I.3.- Se ha definido el riesgo residual que permanecerá cuando una respuesta al riesgo se implemente.	0	0	0	7	0	7	**4,00**
J.1.- Se definen indicadores de desempeño sobre la respuesta a los riesgos para determinar su validez.	0	0	0	7	0	7	**4,00**
J.2.- Los efectos de las respuestas a los riesgos se miden frente al apetito de riesgo.	0	0	0	5	2	7	**4,29**
J.3.- Se evalúa el riesgo residual una vez aplicada la respuesta al riesgo.	0	0	0	5	2	7	**4,29**
K.1.- Exhaustiva recopilación de información para el seguimiento, revisión y aprendizaje en torno al análisis de riesgo.	0	0	0	0	7	7	**5,00**
K.2.- La presencia de nuevos riesgos se identifica sistemáticamente de manera oportuna y proactiva.	0	0	0	0	7	7	**5,00**

Fuente: (**C**onsulta a Expertos, 2017).