risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Revista Ibérica de Sistemas y Tecnologías de Información

Recebido/Submission: 25/11/2018
Aceitação/Acceptance: 14/01/2019

Modelo para Medir la Madurez del Análisis de Riesgo de los Activos de Información en el contexto de las Empresas Navieras

Fresia Yanina Holguín García[1], Lohana Mariella Lema Moreta[2]

fholguin@uees.edu.ec, lohanalema@uees.edu.ec

[1] Universidad Espíritu Santo, Samborondón, Ecuador.

[2] Universidad Espíritu Santo, Samborondón, Ecuador.

DOI: 10.17013/risti.31.1–17

Resumen: El avance tecnológico ha contribuido al incremento de eventos disruptivos de diferente naturaleza en las empresas que podrían producir pérdida de información; por tal motivo, es vital realizar análisis de riesgos adecuado. Considerando que las empresas navieras no están exentas de amenazas, ataques o vulnerabilidades, este artículo propone un Modelo para Medir la Madurez del Análisis de Riesgos de los Activos de Información en éste contexto empresarial. Para cumplir esto, se ejecutaron tres actividades. En la primera, se analizó y seleccionó MAGERIT, OCTAVE y MEHARI como metodologías de análisis de riesgos considerando su uso en otras iniciativas de construcción de modelos de madurez. Luego, se realizaron entrevistas a siete empresas navieras a fin de conocer su postura frente a la problemática planteada. Finalmente, podemos determinar que la construcción de esta propuesta conlleva la ejecución de un proceso de análisis de riesgo formalizado y con técnicas proactivas acorde al contexto empresarial establecido.

Palabras-clave: modelo de madurez; análisis de riesgo; empresas navieras.

Model for Measuring the Maturity of the Risk Analysis of Information Assets in the context of Shipping Companies

Abstract: Technological progress has contributed to the increase of disruptive events of different nature in companies that could produce loss of information; for this reason, it is vital to carry out adequate risk analysis. Considering that shipping companies are not exempt from threats, attacks or vulnerabilities, this article proposes a Model to Measure the Maturity of Risk Analysis of Information Assets in this business context. To accomplish this, three activities were executed. In the first, MAGERIT, OCTAVE and MEHARI were analyzed and selected as risk analysis methodologies considering their use in other maturity modeling initiatives. Afterwards, seven shipping companies were interviewed in order to know their position regarding the proposed problem. Finally, we can determine that the construction of this proposal involves the execution of a formalized risk analysis process and proactive techniques according to the established business context.

Keywords*:* maturity model; risk analysis; shipping companies.

1. Introducción

Las Tecnologías de Información y Comunicación (TIC) se han convertido en un factor que impacta en la competitividad de todo tipo de organización, por ello es fundamental que los procesos del negocio estén fusionados de manera integral de lo contrario aspectos como la efectividad del nivel operativo, imagen corporativa o la rentabilidad estarían disminuidas (Gómez, Pérez, Donoso y Herrera, 2010). En este sentido, Areitio (2008) evidencia que al adquirir e implementar nuevas tecnologías se debe ser consciente de la coexistencia de una amplia gama de amenazas, vulnerabilidades y ataques informáticos; y cuyo objetivo principal es acceder a la información privada de las organizaciones. Según ESET (2015) una de cada cinco empresas sufrió ataques de explotación de vulnerabilidades en el año 2014, y por su parte ISACA (2015) manifiesta que los incidentes de seguridad se han incrementado en un 66% desde el año 2009.

En este contexto, Chu, Wei, & Chang (2013) aseveran que las organizaciones están obligadas a establecer protocolos que les permitan identificar las falencias que afectan sus actividades y procesos, evaluar los controles existentes para disminuir la posibilidad de que un riesgo potencial se cristalice en una pérdida cierta, y adoptar medidas para reducir o controlar el riesgo en aquellos sectores donde se observa que se está por encima de los límites permisibles.

Gómez, Pérez, Donoso y Herrera (2010) señalan que ante la necesidad latente de garantizar una seguridad efectiva se crearon 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. Además, según Jugdev & Thomas (2002) también se deben considerar los *Modelos de Madurez* orientados a la seguridad de la información como una alternativa para evaluar en toda su dimensión la situación organizacional en el manejo del riesgo respecto a una situación ideal, y considerando que estos se cimentan en el conocimiento de los procesos la toma de decisiones es más acertada.

Aunado a lo anterior, Becker, Niehaves, Poppelbus, & Simons (2010) establecen que un modelo de madurez en seguridad informática deberá evaluar desde los procesos incongruentes hasta los más óptimos de una empresa, lo cual permitirá identificar rápidamente las áreas donde la entidad debe enfocarse para mejorar y ello conllevará la implementación de buenas prácticas.

Por otra parte, según un estudio realizado por Llop et al. (2013) las empresas de transporte marítimo denominadas *Agencias Navieras* no están exentas de eventos conexos a la seguridad informática, además no cuentan con una herramienta específica para la identificación y categorización del riesgo de su ambiente tecnológico y considerando que sus actividades están relacionadas a la documentación, transporte terrestre de los contenedores, verificación de la carga, seguimiento de la carga desde el puerto origen al puerto destino, y otras operaciones portuarias; es preciso proponer un modelo que satisfaga este requerimiento no atendido.

Por lo antes expuesto el objetivo principal de este trabajo es diseñar un *Modelo para Medir la Madurez del Análisis de Riesgos de los Activos de Información en el contexto de las Empresas Navieras*, de tal manera que permita autoevaluar la realidad de la

organización y establecer una ruta de mejoramiento con estrategias acordes al giro del negocio. Este modelo se cimentará en las mejores prácticas de las metodologías MAGERIT, OCTAVE y MEHARI; debido a que cuentan con una estructura definida, documentada y adaptable a todo tipo de empresa; sus fases de análisis de riesgo son homólogas, permiten distinguir los activos y sus riesgos de forma que sean un punto de referencia para tomar decisiones y hacer mejoras en los procesos internos organizacionales; y admiten después de su implementación la construcción de un plan de actividades que puede ser detallado, monitoreado y examinado de forma periódica.

Para alcanzar el objetivo planteado se construirá un modelo con tres elementos: *Niveles de Madurez, Categorías a Evaluar y Mapa de Control*; los cuales estarán sustentados en la revisión bibliográfica de las metodologías escogidas y de la profundización del modelo de madurez CMMI.

2. Marco Teórico

2.1. Análisis de Riesgo

Según Del Carpio (2006) el análisis de riesgo es un proceso de origen cuantitativo o cualitativo que permite evaluar los riesgos, y que además consiente una estimación de incertidumbre e impacto. Por su parte, Sikdar (2011) afirma que el análisis de riesgo es una etapa que comprende dos aspectos claves: determinar las amenazas a las cuales está expuesta una entidad y valorar su posible materialización. En cambio, 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 este contexto, Curiman y Toth (2004) establecen que el análisis de riesgo no es un proceso aislado respecto a otras iniciativas que conllevan a un nivel óptimo de seguridad, al contrario, es 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 Aguilera (2010) es conveniente conocer la diferencia entre el análisis y la gestión de riesgo; el análisis proporciona un bosquejo del sistema en términos de activos, amenazas y salvaguardas; es decir, que es la base para ejercer un control de todas las actividades; mientras que, la gestión se refiere a la estructuración de las acciones de seguridad para satisfacer las insuficiencias detectadas por el análisis.

Por otra parte, Echenique (2012) considera que dentro del análisis de riesgo es preciso distinguir seis elementos claves:

1. *Probabilidad*: estimación de la posibilidad que un recurso informático quede expuesto a un evento (Canal, 2004).
2. *Amenazas*: cualquier tipo de acción que puede producir un daño material o inmaterial en una empresa, y cuya naturaleza puede ser: física o lógica (Aguilera, 2010).

3. *Vulnerabilidades:* característica o circunstancia de debilidad de un recurso que posibilita la materialización de una amenaza (Canal, 2004).
4. *Activos:* recursos o elementos relacionados a un sistema de información y que tienen valor para la organización (Aguilera, 2010).
5. *Impacto:* es el efecto de una amenaza sobre un activo (Eterovic y Pagliari, 2011).
6. *Riesgo:* estimación del grado de exposición que una amenaza se materialice sobre uno o más activos causando daños a la organización (Gupta, & Xu, 2010).

Areitio (2008) señala que para llevar a cabo un análisis de riesgo robusto es recomendable utilizar los lineamientos establecidos por las metodologías vigentes, las cuales se caracterizan por contemplar entre sus fases aspectos como: realización de un inventario y valoración de los activos, identificación y estimación de las amenazas que puedan afectar a la seguridad de los activos, establecimiento y evaluación de las medidas de seguridad existentes, determinación y ponderación de las vulnerabilidades de los activos, y valoración del impacto que produciría un ataque.

En este ámbito, 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; y aunque tienen características similares 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. Es preciso acotar que este artículo solo abarcará OCTAVE, MAGERIT Y MEHARI debido a que su proceso de análisis de riesgo es análogo, y porque las metodologías excluidas requieren un costo de licencia que las convierte en poco atractivas para su implementación.

2.2. 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 este mismo ámbito Januszkiewicz & Marek (2006) señalan que OCTAVE se diferencia de otras metodologías porque no se limita al análisis del riesgo tecnológico y aspectos tácticos, también abarca el riesgo de la organización y se enfoca en temas estratégicos relacionados con la práctica.

Según Alberts, Dorofee, Stevens & Woody (2003) OCTAVE es autodirigido, lo que significa que el personal de la organización asume el compromiso de establecer la estrategia de seguridad, por ende, es necesario la integración del departamento operativo y de TI así se equilibrarán los aspectos de: riesgos operativos, prácticas de seguridad y tecnología. Además, CERT (2013) indica que para la ejecución de OCTAVE se cuenta con tres fases claramente definidas:

- *Fase 1, Visión Organizativa*: En esta etapa se determinan los activos críticos, requerimientos de seguridad y amenazas sobre los activos críticos, prácticas de seguridad actuales y las vulnerabilidades organizativas (CERT, 2013).
- *Fase 2, Visión Tecnológica:* Se examinan los componentes claves y las vulnerabilidades tecnológicas vigentes (CERT, 2013).

- *Fase 3, Estrategia y Desarrollo del Plan:* Se crean medidas, estrategias y planes de mitigación de riesgo utilizando los resultados obtenidos de las fases anteriores (CERT, 2013).

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 (Alberts, Dorofee, Stevens & Woody, 2003). A continuación, se describen las principales características de cada uno:

- *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, 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).

2.3. 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).

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. MAGERIT propone la realización de cinco pasos para efectuar el análisis de riesgos, los cuales se detallan en la Figura 1.

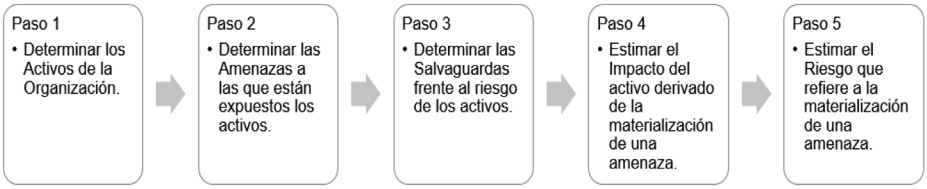

Figura 1 – Pasos para el Análisis de Riesgos de MAGERIT (Ministerio de Haciendas y Administración Pública del Gobierno de España, 2012).

2.4. MEHARI

MEHARI, también conocido como un método de análisis de riesgo armonizado, es una metodología desarrollada en el año 1995 por CLUSIF (**CLU***b de la* **S***écurité de l'***I***nformation* **F***rançais*) 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).

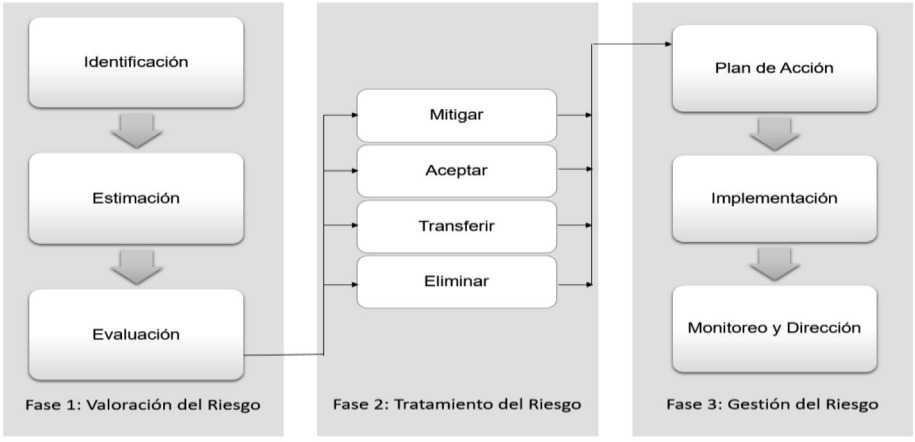

Figura 2 – Proceso de evaluación, tratamiento y gestión del Riesgo de MEHARI (CLUSIF, 2010).

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 2.

2.5. 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. También, Saavedra, Dávila, Melendez & Pessoa (2017) evidencian que un modelo de madurez es un conjunto de elementos organizados en una estructura evolutiva con transiciones medibles entre niveles. Además, Carvalho, Rocha, & Abreu (2017) añaden que un modelo de madurez se sustenta en el principio de que las personas, las organizaciones, los procesos, etc., evolucionan hacia una mayor madurez por consecuencia su desarrollo abarca varias etapas diferentes.

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 Palomino, Dávila, Melendez & Pessoa (2017) el CMMI es un modelo que agrupa las mejores prácticas en actividades de desarrollo y mantenimiento. En este sentido, Crawford (2002) expone que 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 3 se esquematizan estos niveles.

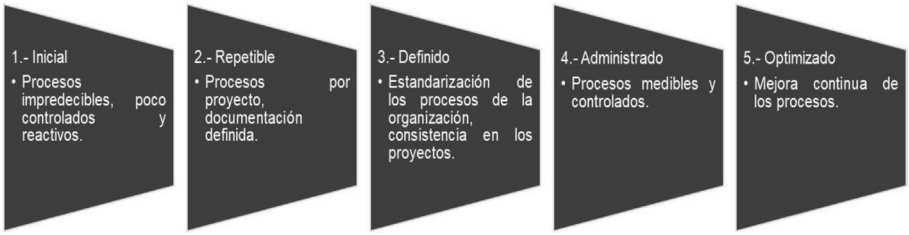

Figura 3 – Niveles de Madurez CMMI (Crawford, 2002).

3. Metodología

El enfoque de la investigación es de origen *Cualitativo* porque se utilizará la teoría como fundamento en la elaboración del Modelo para Medir la Madurez del 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 tres 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 para Medir la Madurez del Análisis de Riesgos de los Activos de Información en el contexto de las Empresas Navieras basado en los resultados obtenidos del paso 1 y 2.

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.

4. Análisis de Resultados

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

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.

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.

4.2. Análisis de las Empresas Navieras en contexto a las Tecnologías de Información

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 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.

4.3. Construcción del Modelo para Medir la Madurez del Análisis de Riesgos de los Activos de Información en el contexto de 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? y ¿El modelo abarca las fases esenciales del análisis de riesgo?

Para definir el modelo se han desarrollado tres elementos: Niveles de Madurez, Categorías a Evaluar y Mejores Prácticas, y Mapa de Control.

4.3.1. 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

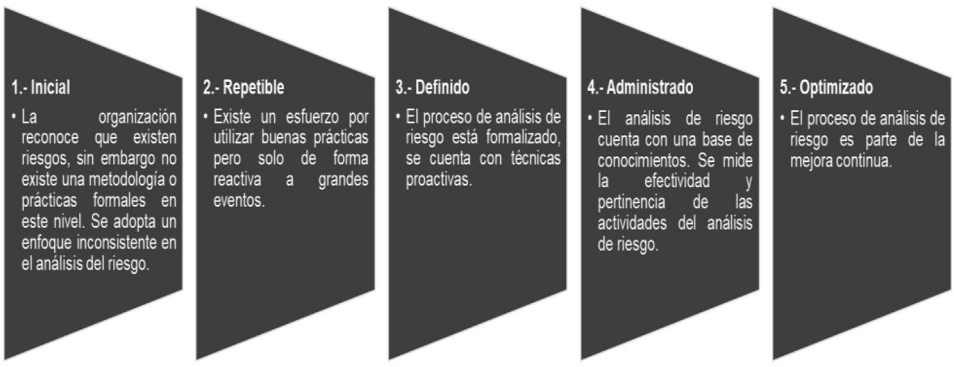

Figura 4 – Niveles de Madurez del Modelo Propuesto con base al CMMI (Elaboración propia, 2017).

conllevan el análisis de riesgos. En la Figura 4 se detallan los niveles de madurez con sus características.

4.3.2. 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, cabe detallar que en la tabla se encuentra marcado a que metodología corresponde la buena práctica.

4.3.3. 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 4 y Tabla 1). En la Tabla 2 se detalla el Mapa de Control.

5. Conclusiones

Un Modelo de Madurez es una medición estructurada del desempeño organizacional que permite identificar vacíos o debilidades para así establecer procesos de mejora continua. Dentro de estos modelos destaca el CMMI cuya principal fortaleza es la priorización de los esfuerzos iniciales como soporte para la transición evolutiva, por tal motivo fue escogido como referencia para delimitar los niveles y especificaciones del modelo propuesto.

Las metodologías MAGERIT, OCTAVE y MEHARI tienen características propias pero complementarias entre sí, lo que permite que al combinarlas se obtenga un análisis de riesgo más robusto; por ello para el modelo diseñado se escogieron las prácticas primordiales asociadas 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 diseñado pretende establecer el grado de madurez en que se encuentra la organización según las prácticas de análisis de riesgo vigentes, lo que permitirá que a partir de ello se enfoquen en las debilidades o falencias que cada categoría evalúa, se tracen estrategias de mejora y se autoevalúe su cumplimiento; todo esto con la finalidad que en el futuro se alcance el nivel de perfección.

Por otra parte, el modelo propuesto tiene como limitante su validez teórica, por ello en una siguiente investigación, a través del método Delphi, se convocará a profesionales del sector para medir la eficiencia de las *Categorías a Evaluar* definidas, así como la pertinencia de las *Mejores Prácticas* según el nivel de madurez; lo cual podrá ser contrastado con los resultados obtenidos en este artículo.

	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.	X	X	
		A.2.- La política ha sido comunicada a toda la entidad.	X	X	
		A.3.- La política de riesgo es revisada y actualizada para incluir los cambios del entorno interno y externo.	X		
		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.	X		
	B.- Responsabilidad	**B.1.-** La entidad posee un departamento de TI con un equipo de análisis de riesgo.	X		
		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.	X		
	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.		X	
		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.		X	
	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.		X	
		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.	X		
		D.3.- Se informa periódicamente y de forma inmediata a la alta dirección la consolidación de un riesgo.	X	X	
Identificar los Activos	**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.	X	X	X
Valorar los Activos Identificados		**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.		X	
		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).	X	X	X

Fases del Análisis de Riesgo					
Determinar las amenazas de 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.	X	X	X
		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.	X	X	X
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.		X	
		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.	X		
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.	X		
		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.	X	X	X
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.	X	X	X
		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.	X	X	X
		I.3.- Se ha definido el riesgo residual que permanecerá cuando una respuesta al riesgo se implemente.	X	X	X
Monitoreo y Dirección	**J.- Actividades de Control**	**J.1.-** Se definen indicadores de desempeño sobre la respuesta a los riesgos para determinar su validez.	X		X
		J.2.- Los efectos de las respuestas a los riesgos se miden frente al apetito de riesgo.		X	
		J.3.- Se evalúa el riesgo residual una vez aplicada la respuesta al riesgo.	X	X	
	K.- Mejora Continua del Análisis de Riesgo	**K.1.-** Exhaustiva recopilación de información para el seguimiento, revisión y aprendizaje del análisis de riesgo.	X		X
		K.2.- La presencia de nuevos riesgos se identifica sistemáticamente de manera oportuna y proactiva.	X	X	X

Tabla 1 – Propuesta de Categorías a Evaluar y Mejores Prácticas con base en las metodologías MAGERIT, OCTAVE y MEHARI (Elaboración propia, 2017).

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

Tabla 2 - Mapa de Control propuesto (Elaboración propia, 2017).

Referencias

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., & 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

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

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

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

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

Carvalho, J., Rocha, Á., & Abreu, A. (2017). HISMM - Hospital Information System Maturity Model: A Synthesis. En: Mejia J., Muñoz M., Rocha Á., San Feliu T., Peña A. (Eds). Trends and Applications in Software Engineering. CIMPS 2016. Advances in Intelligent Systems and Computing, vol 537. Cham: Springer.

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. (2010). *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., & 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

Del Carpio, J. (2006). *Análisis del riesgo en la administración de proyectos de tecnología de información*. Perú: Universidad Nacional Mayor de San Marcos.

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

ESET Security Report. (2015). ESET Security Report, Latinoamérica 2015. Ciudad de México: ESET.

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

Gómez, R., Pérez, D., Donoso, 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

ISACA. (2015). *State of Cybersecurity: Implications for 2015.* USA: Creative Commons

Januszkiewicz, P., & Marek, P. (2006). *The 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.* New York: John Wiley and Sons.

Klimko, G. (2001). *Knowledge management and maturity models: Building common understanding*. In: 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., & Navarro, C. (2013). *Tendencias TIC en puertos*. Valencia, España: Fundación Valenciaport

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., & Lemes, L. (2008). *M*odelo para Avaliar o Nível de Maturidade do Processo de Gestão de Riscos em Segurança da Informação. Paper presented at: *VIII Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. 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

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

Palomino, M., Dávila, A., Melendez, K., & Pessoa, M. (2017). Agile Practices Adoption in CMMI Organizations: A Systematic Literature Review. En: Mejia J., Muñoz M., Rocha Á., San Feliu T., Peña A. (Eds). Trends and Applications in Software Engineering. CIMPS 2016. Advances in Intelligent Systems and Computing, vol 537. Cham: Springer.

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

Saavedra, V., Dávila, A., Melendez, K., & Pessoa, M. (2017). Organizational Maturity Models Architectures: A Systematic Literature Review. En: Mejia J., Muñoz M., Rocha Á., San Feliu T., Peña A. (Eds). Trends and Applications in Software Engineering. CIMPS 2016. Advances in Intelligent Systems and Computing, vol 537. Cham: Springer.

Sikdar, P. (2011). Alternate Approaches to Business Impact Analysis. *Information Security Journal: A Global Perspective*, 20, 128–134.

Sotelo, M., Torres, J., & Rivera, J. (2012). Un proceso práctico de análisis de riesgos de activos de información. Paper presented at: *IV Congreso Internacional de Computación y Telecomunicaciones COMTEL*. 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