UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS

Facultad 5, Laboratorio de Gestión de Proyectos

Centro de Telemática

Guía de gestión del riesgo tecnológico para el tratamiento de la seguridad durante el proceso de desarrollo de software.

Trabajo final presentado en opción al título de Máster en Gestión de Proyectos Informáticos.

Autor: Ing. Lilian Teresa Castro Mecias

Tutor: DrC. Oiner Gómez Baryolo

Co-tutor: MSc. Yenin Calderín Abad

La Habana, Junio 2014

DECLARACIÓN JURADA DE AUTORÍA

Declaro por este medio que yo Lilian Teresa Castro Mecias con carné de identidad 86011424396 soy la autora principal del trabajo final de maestría Guía de gestión del riesgo tecnológico para el tratamiento de la seguridad durante el proceso de desarrollo de software, desarrollada como parte de la Maestría en Gestión de Proyectos Informáticos y que autorizo a la Universidad de las Ciencias Informáticas a hacer uso de la misma en su beneficio, así como los derechos patrimoniales con carácter exclusivo.

Y para que así conste, firmo la presente declaración jurada de autoría en La Habana a los ____ días del mes de _____ del año _____.

_____ _____

Nombre de la Autora Firma

_____ _____

Nombre del Tutor Firma

_____ _____

Nombre del Tutor Firma

RESUMEN

La gestión de proyectos se considera un elemento imprescindible para lograr la finalización exitosa del proyecto y la obtención de un producto con la calidad requerida. La gestión de riesgos se orienta como un proceso que permite aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos adversos para el proyecto. En el software específicamente, el riesgo no se limita al proyecto solamente. Pueden aparecer riesgos después de haber desarrollado con éxito el software y de haberlo entregado al cliente. Estos riesgos están asociados con las consecuencias del fallo del software una vez en el mercado y consecuentemente, en muchas ocasiones, estos fallos han convertido al software en blanco de ataques y vías para los mismos.

La presente investigación se enmarca en la gestión del riesgo tecnológico en proyectos de desarrollo de software. Se propone una guía basada en estándares internacionales y buenas prácticas que permite facilitar la estandarización de la gestión del riesgo tecnológico en los proyectos del Centro de Telemática (TLM). A través de la ejecución de actividades, la aplicación de técnicas de análisis y gestión de riesgos y el desarrollo de artefactos se ofrece una herramienta que permite determinar los requisitos de seguridad que se implementarán en relación a los riesgos identificados.

La guía propuesta favorece el aseguramiento de la calidad y seguridad de los sistemas desarrollados en el Centro de Telemática además de alinearse con la necesidad de incorporar la gestión de la seguridad desde el proceso de desarrollo del software.

Palabras claves: riesgo tecnológico, seguridad, desarrollo de software.

ABSTRACT

Project management is considered an essential element for the successful completion of the project and obtaining a product with the required quality. Risk management is oriented as a process that allows increasing the probability and impact of positive events, and decreasing the probability and impact of adverse events for the project. In the software specifically, the risk is not limited to the project only. Risks may arise after successfully developed the software and I have delivered to the customer. These risks are associated with the consequences of failure of the software once on the market and consequently, in many cases, these failures have made the software and targeted way for them.

This research is part of the management of technological risk in software development projects. Based on international standards and best practices that can facilitate the standardization of the management of technological risk projects TLM Center guide is proposed. Through the implementation of activities, the application of technical analysis and risk management and the development of a tool that allows devices to determine the safety requirements to be implemented in relation to identified risks is provided The proposed guide promotes quality assurance and safety developed at the Center for Telematics well aligned with the need to incorporate safety management from the development process of software systems.

Keywords: technology risk, security, software development

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La tendencia en la adquisición de sistemas de información ha generado mayor crecimiento y competitividad en las organizaciones al apoyar los procesos de negocio, las actividades de procesamiento de la información y las actividades de administración, lo que abre un sinnúmero de posibilidades para ampliar las relaciones entre clientes, proveedores y empleados, y posibilita la rapidez en las respuestas a los cambios en el entorno. (Riascos 2010)

Sin embargo, aparejado a esta situación, se observan informaciones de incidentes que han causado daños a la seguridad de los sistemas y cuyas derivaciones han traído serias consecuencias asociadas a pérdidas de valor económico, perturbación o ruptura de ciclos productivos, incapacidad de cumplir las obligaciones y pérdidas relativas a responsabilidades legales. Resultados de la encuesta realizada por Kaspersky Lab reflejan que las vulnerabilidades en el software son la principal causa de los incidentes de seguridad en las empresas, el reporte refleja que el 85 % de las empresas han informado de incidentes de seguridad y las vulnerabilidades de software son el motivo principal, se estima además que los incidentes significativos pueden causar pérdidas valoradas desde 50,000 hasta 649,000 dólares. (Kaspersky Lab 2013)

Esta situación se agrava de acuerdo con el estudio Risk Index, puesto que la motivación de los ciberataques ha cambiado, desde la delincuencia financiera, los actos de piratería hasta la pérdida de vidas humanas de forma idéntica a un ataque convencional.(Bejarano 2013). Lo cual ha sido analizado por académicos y por la propia industria del desarrollo de software. Las investigaciones realizadas reflejan como recomendaciones realizar análisis detallados y evaluaciones de clasificación del riesgo para identificar las principales vulnerabilidades y las amenazas que puedan explotarlos además definir y adoptar las mejores prácticas para defender las infraestructuras críticas.

Todo esto si bien complementa la defensa de las infraestructuras de Tecnologías de información (TI) no soluciona el verdadero problema, detrás de una violación de seguridad se evidencia la existencia de vulnerabilidades en el software. La incapacidad del software para limitar o contener los ataques de que es objeto se fundamenta en la baja calidad del mismo, que falla y en consecuencia manifiesta un comportamiento distante a lo previsto en sus especificaciones funcionales. Por ello se plantea la necesidad de emplear métodos preventivos que permitan la disminución de las amenazas y favorezcan la confiabilidad y seguridad del software.

En este sentido se destacan propuestas enfocadas a reducir el número de fallos y vulnerabilidades en la tecnología, con una influencia positiva en cómo se desarrolla el software. Los modelos y estándares en esta dirección contemplan la seguridad desde el punto de vista del proceso y la enmarcan como una característica importante para su desarrollo. En (McGraw 2006) se manifiesta que la seguridad del software se basa en tres pilares fundamentales la administración del riesgo, buenas prácticas durante el ciclo de vida del desarrollo y el conocimiento para la seguridad del software. Tomando un papel elemental el análisis y gestión de riesgos pues asegura que los controles de seguridad de un sistema se adopten según la proporción de sus riesgos. Conceptualizando el riesgo como “La posibilidad de que

una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.” (ISO/IEC 27005 2008)

La administración de riesgos se basa en el establecimiento de las necesidades de seguridad del sistema asociada a los activos valiosos gestionados por él, sobre lo cual se identifican las amenazas y se valora el riesgo que representan las amenazas para el cumplimiento de la misión del software. Las ventajas de la administración de riesgos se apreciarán al implementar controles que reduzcan el riesgo a un nivel aceptable y aseguren la capacidad del software de resistir proactivamente los ataques a los que se ve expuesto. Lo cual también favorece el trabajo por obtener la confianza de los usuarios en la calidad del servicio.

En Cuba para la informatización de los servicios, la Universidad de las Ciencias Informáticas (UCI) ejecuta más de 200 proyectos productivos orientados a diversos sectores de la economía dentro y fuera del país. La generalización de los sistemas desarrollados ha logrado alto impacto en la gestión de los procesos realizados por los usuarios en distintos órganos y organismos de la administración central del estado (OACE).

El proceso de producción en la institución considera la realización de pruebas de seguridad y las revisiones del código fuente realizadas en el Laboratorio de Seguridad Informática (LABSI) del Centro TLM. Esta actividad permitió conocer que en la etapa final de pruebas, cuando el software estaba listo para su entrega al cliente, estos sistemas presentaban al menos una vulnerabilidad significativa con impacto alto por ejemplo: inyecciones de Lenguaje de Consulta Estructurada (SQL, por sus siglas en inglés), Secuencias de Comandos en Sitios Cruzados (XSS por sus siglas en inglés), referencia directa insegura a objetos, así como defectuosas configuraciones de seguridad. Estas vulnerabilidades constituyen un serio riesgo para la información si la aplicación llega a ser comprometida, provocando una seria degradación en la calidad del servicio. (LABSI 2012)

En relación con lo cual se desarrolló y aplicó una encuesta a Jefes de proyectos, arquitectos, asesores de planificación y administradores de la calidad de 10 de los Centros de Desarrollo de la Red, con un promedio de 3 años de experiencia en el desempeño del rol. La observación participativa y la encuesta realizada arrojaron las siguientes dificultades:

- Los procesos que institucionalizan las políticas del Modelo Integrado de Madurez y Capacidad - CMMI para la gestión de riesgos en los proyectos de desarrollo de la institución permiten identificar, documentar, analizar y monitorear el estado de los riesgos del proyecto pero carece de las técnicas y métodos necesarios para cubrir la gestión del riesgo tecnológico.
- Las técnicas de gestión de riesgos utilizadas no se adecuan al tratamiento necesario para el riesgo tecnológico, de forma que se identifiquen las amenazas a los activos del sistema, se determinen las medidas necesarias para su protección y se valore el daño potencial asociado a las amenazas identificadas.

Todo lo cual trae como consecuencia la entrega de un producto sensible a eventos que amenacen el cumplimiento de su misión y la exposición del sistema con el consiguiente riesgo, excesos de gastos en la entidad cliente por concepto de soluciones de infraestructura para la protección del sistema, en caso

contrario excesos de tiempo y recursos del equipo de desarrollo en la solución de los problemas detectados en el software.

De la problemática anteriormente planteada se deriva el **problema científico** de la investigación:

Las limitaciones para la gestión del riesgo tecnológico en las actividades de gestión de riesgos de los proyectos, afecta la seguridad del software desarrollado en la Universidad de las Ciencias Informáticas.

Se enmarca como **objeto de estudio** la gestión de riesgos, a partir de lo cual se define como **objetivo general** de la investigación: elaborar una guía para la gestión del riesgo tecnológico que permita asegurar el cumplimiento de los objetivos de seguridad del software en los proyectos de desarrollo de la Universidad de las Ciencias Informáticas.

Como **objetivos específicos** se determinan:

1. Fundamentar la investigación a partir del análisis de los referentes teóricos relacionados con la gestión de riesgos en el contexto de la seguridad del software y la gestión de proyectos.
2. Definir una guía para la gestión del riesgo tecnológico en proyectos de desarrollo de software a través de la adopción de buenas prácticas que permita asegurar el cumplimiento de los objetivos de seguridad del software.
3. Validar la guía diseñada mediante su aplicación práctica en la población definida.

El **campo de acción** se ubica en la gestión del riesgo tecnológico.

Para el cumplimiento de los objetivos se identificaron las siguientes tareas de investigación:

1. Análisis bibliográfico en torno al objeto de estudio y campo de acción delimitado, que permitan definir el marco teórico de la investigación.
2. Diagnóstico de la situación actual en los proyectos productivos en cuanto al proceso de gestión de riesgos que permita identificar las prácticas utilizadas y las deficiencias en relación al proceso que apoye la seguridad.
3. Selección de las mejores prácticas utilizadas en la gestión del riesgo tecnológico para minimizar los problemas de seguridad en el software durante el desarrollo.
4. Definición de la estructura de la guía a través de la ejecución de actividades, roles, entradas y salidas que permita la gestión del riesgo tecnológico durante el ciclo de vida de desarrollo del software.
5. Definición de las técnicas de validación interna y externa a utilizar para evaluar la guía diseñada.
6. Validación de la propuesta mediante su implementación en la población definida.

Se determina realizar una investigación transaccional correlacional que permita el análisis entre los conceptos y variables asociado a la gestión del riesgo tecnológico con el impacto en el desarrollo de software seguro. La investigación se enmarca en las tendencias del empleo de buenas prácticas en el campo de la seguridad y el desarrollo de software; como vías para asegurar el cumplimiento de los objetivos de seguridad del software.

Para el desarrollo de la investigación se propone la siguiente hipótesis:

La guía para la gestión del riesgo tecnológico en los proyectos de desarrollo de la institución favorecerá el cumplimiento de los objetivos de seguridad del software.

Definición y operacionalización de las variables

Variable independiente: Guía de gestión del riesgo tecnológico en los proyectos de desarrollo de la institución.

Variable dependiente: Cumplimiento de los objetivos de seguridad del software.

Tabla 1: Operacionalización de las variables. Fuente Elaboración propia

Variable Independiente	**Dimensión**	**Subdimensión**	**Unidad de Medida / Escala de valoración**
Guía de gestión del riesgo tecnológico en los proyectos de desarrollo de la institución	Calidad de la guía	Integración al proceso de desarrollo de software.	Alto (Se definen actividades para las 3 fases) Medio (Se definen actividades en al menos dos fases) Bajo (Se definen actividades para una sola fase) Nulo (No existe definición de actividades)
			Alto (Se identifican roles en más del 80% de las actividades) Medio (Se identifican roles entre el 50 y 79% de las actividades) Bajo (Se identifican roles en menos del 50% de las actividades)
			Alto (Más del 80% de las responsabilidades definidas para los roles se relacionan con las actividades de la guía) Medio (entre el 50 y el 79% de las responsabilidades definidas para los roles se relacionan con las actividades de la guía) Bajo (Menos del 50% de las responsabilidades definidas para los roles se relacionan con las actividades de la guía)
			Si (Cuenta con recursos de soporte suficientes para comprender la guía propuesta) No (No cuenta con recursos de soporte)

		Comprensión de la guía	Bastante adecuado (Más del 85% de la descripción de la guía está adecuadamente orientada para dotar al usuario de la metodología necesaria para la gestión del riesgo tecnológico y aprender del proceso) Adecuado (Entre el 60% y el 84% de la descripción de la guía se encuentra adecuadamente orientada para dotar al usuario de la metodología necesaria para la gestión del riesgo tecnológico y aprender del proceso) Poco Adecuado (Menos del 59 % de la descripción de la guía orienta adecuadamente al usuario sobre el enfoque necesario para la gestión del riesgo tecnológico)
			Bastante adecuado (Más del 85% de la descripción de la guía está adecuadamente orientada para dotar al usuario de la metodología necesaria para la gestión del riesgo tecnológico y aprender del proceso) Adecuado (Entre el 60% y el 84% de la descripción de la guía se encuentra adecuadamente orientada para dotar al usuario de la metodología necesaria para la gestión del riesgo tecnológico y aprender del proceso) Poco Adecuado (Menos del 59 de la descripción de la guía orienta adecuadamente al usuario sobre el enfoque necesario para la gestión del riesgo tecnológico)
			Alto (Se indican los referentes teóricos sobre los que se fundamentan más del 85% de las actividades de la guía) Medio (Se indican los referentes teóricos sobre los que se fundamentan entre el 60 y el 84% de las actividades de la guía) Bajo (Se indican los referentes teóricos sobre los que se fundamentan menos del 59% de las actividades de la guía) Nulo (No se indican los referentes teóricos sobre los que se fundamentan las actividades de la guía)

		Aplicabilidad de la guía	Alto (En más del 80% de las actividades se definen técnicas y herramientas para su ejecución) Medio (Entre el 50 y 79% de las actividades se definen técnicas y herramientas para su ejecución) Bajo (Se definen técnicas y herramientas en menos del 50% de las actividades)
			Alto (Permite determinar la vulnerabilidad del sistema ante amenazas, gestionar controles para asegurar sus activos y valorar la eficacia de los controles definidos) Medio (Utiliza elementos para la gestión del riesgo tecnológico que permitan asegurar el software ante amenazas) Baja (Ninguna relación con las vulnerabilidades del sistema y la gestión del riesgo tecnológico.)
			Bastante adecuado (La guía propuesta tiene influencias en la seguridad del software y se encuentra alineada con la necesidad de la gestión de la seguridad desde su desarrollo) Adecuado (La guía propuesta a través de la gestión del riesgo tecnológico minimiza los problemas de seguridad y favorece el cumplimiento de los objetivos de seguridad del software) Poco Adecuado (Ninguna influencia en la seguridad del software)
Variable Dependiente	**Dimensión**	**Subdimensión**	**Unidad de medida**
Cumplimiento de los objetivos de seguridad del software	Correspondencia	Rastreabilidad desde la Fase de Inicio hacia	Adecuado (Se establecen los Objetivos de seguridad del software y se mapean a Requisitos de seguridad.) Poco Adecuado (Se establecen los Objetivos de seguridad del software sin relación con los Requisitos de seguridad) Nulo (No se establecen los objetivos de seguridad del software)

	en las Especificaciones funcionales del software.	las fases de Elaboración y Construcción.	Bastante Adecuado (Se representan los Casos de uso (CU) seguros en el Diagrama de CUS y se describen los elementos asociados a él) Adecuado(Se representan los CU seguros en el Diagrama de CUS) Poco Adecuado (No se representan los CU seguros en el Diagrama de CUS)
			Bastante Adecuado (Se desarrolla el diseño del sistema en relación con los Requisitos de seguridad determinados y se incluyen en el Expediente de Arquitectura del proyecto.) Adecuado (Se desarrolla el diseño del sistema en relación con los Requisitos de seguridad determinados) Poco Adecuado (No existe relación entre los Requisitos de seguridad determinados y la arquitectura del sistema)
			Alto (Se implementan todos los CU seguros y se hace referencia en los paquetes y/o clases del código fuente a los CU que implementan, según corresponda) Medio (Se implementa una parte de los CU seguros) Bajo (No se implementan los CU seguros que se determinaron en la ejecución de la guía)
			Alto (Por cada Amenaza potencial se diseña un Caso de prueba y ejecuta el escenario de prueba asociado) Medio (Se diseñan solamente Casos de prueba para una representación de las amenazas identificadas) Bajo (No se determinan escenarios y casos de prueba)
	Evaluación de Seguridad	Vulnerabilidades de seguridad	Alto (Más del 80% de los riesgos identificados son valorados de alto) Medio (Más del 80% de los riesgos identificados son valorados de medio y no hay ninguno valorado de alto) Bajo: (Más del 80% de los riesgos identificados son valorados de bajo y no hay ninguno valorado de alto)

Durante el desarrollo de la investigación se utilizaron diferentes métodos científicos. Dentro de los métodos teóricos:

El histórico lógico posibilitó el análisis del comportamiento del objeto de estudio en los últimos años, permitiendo determinar las principales causas del desenlace del problema, así como las posibles soluciones a desarrollar, a partir del análisis de estudios anteriormente realizados.

El análisis y la síntesis permitieron desarrollar un estudio de la gestión de riegos, enfatizando en las buenas prácticas asociadas a esta actividad. Posibilitaron la determinación de los principales elementos a tener en cuenta y las relaciones entre ellos, así como sus implicaciones en el desarrollo del software.

El método hipotético-deductivo permite llegar a soluciones anticipadas para el problema definido, de ahí que al analizar las principales tendencias en cuanto a la gestión del riesgo tecnológico, sus implicaciones, los principales estándares a seguir, así como las propuestas de solución a problemas de este tipo, se pudiera establecer una respuesta anticipada en función de uno de los recursos más afectados: la seguridad del software.

Entre los métodos empíricos:

La observación facilitó la determinación de la problemática analizada mediante su percepción directa, fue la primera fuente de intercambio para determinar las contradicciones o deficiencias existentes, de ahí que se determinaran las formas o mecanismos utilizados en la muestra analizada para gestionar el riesgo tecnológico.

La encuesta permitió precisar los elementos significativos de la guía propuesta, facilitando una caracterización más acertada del objeto de estudio. Se identificaron y cuantificaron los mecanismos utilizados para la gestión de riesgos, el nivel de conocimiento de estándares y procesos asociados con esta actividad así como su implementación en los proyectos de desarrollo de la Institución. Posteriormente se desarrolló un cuestionario que se aplicó en la muestra seleccionada con la intención de encontrar potencialidades y limitaciones de la guía. A partir del análisis de los resultados obtenidos se realizan los ajustes en el diseño de los componentes de la propuesta.

La población de estudio está constituida por los proyectos de desarrollo del Centro TLM que se encuentren en las Fases de Inicio registrados al cierre de la investigación. En este caso la muestra seleccionada es el proyecto GRHS, lo que representa el 100% de la población.

Se utilizó un diseño experimental del tipo Cuasiexperimento partiendo de la aplicación de la guía para la gestión del riesgo tecnológico en la muestra seleccionada además se utiliza un grupo de control para la comparación postprueba que permita el análisis de los resultados.
Se realizará de acuerdo al esquema siguiente:

G1	X	O1
G2	--	O2

Donde:
G1: corresponde al grupo experimental constituido por el proyecto del Centro TLM seleccionado.
X: corresponde a la aplicación de la propuesta como tratamiento o estímulo del grupo experimental.
G2: corresponde al grupo de control constituido por un proyecto que no recibe el estímulo.
O1: corresponde a la observación sobre el grupo experimental luego de aplicada la propuesta.
O2: corresponde a la observación sobre el grupo de control sin la aplicación de la propuesta.

Para medir las variables operacionales se utilizó el Paquete Estadístico para las Ciencias Sociales - por sus siglas en inglés – SPSS v13.0: Se emplea en la realización de pruebas estadísticas que permitan validar los instrumentos aplicados y el procesamiento de los resultados.

Como aportes prácticos de la investigación se consideran:
Una guía para la gestión del riesgo tecnológico en proyectos de desarrollo de software que posibilita:

- Determinar los requisitos de seguridad del software en función de la proporción de sus riesgos.
- Contribuir al desarrollo de software seguro a través del empleo de herramientas y técnicas para la identificación de amenazas y asegurar los activos del sistema que es objeto de análisis.

Proveer un enfoque cuyos resultados constituyen la entrada a las actividades de evaluación de la seguridad tales como el análisis estático del código y las pruebas de seguridad.

Novedad Científica

1. La elaboración de una guía para la gestión del riesgo tecnológico desde el propio desarrollo del software y la incorporación de los conceptos básicos de seguridad informática al desarrollo de software con visibilidad en las fases de inicio, desarrollo y cierre del proyecto.

Listado de publicaciones, eventos y avales de investigación.

1. Castro Mecias, Lilian Teresa. *Seguridad en el Proceso de desarrollo de software. Evento Nacional de Segurmática 2010.*

2. Castro Mecias, Lilian Teresa; Martínez Thompson, Rogfel; García Pérez, Félix Maikel. (2011)*Incorporando la seguridad al proceso de desarrollo de software.* Taller Innovación en el sector de las TIC. 10ma Semana tecnológica.

3. Castro Mecias, Lilian Teresa; García Pérez, Félix Maikel. (2011). *Modelo para mitigar riesgos de seguridad desde fases tempranas del proceso de desarrollo de software.* Evento base de COMPUMAT 2011.

4. Castro Mecias, Lilian Teresa. *Ciclo de Desarrollo Seguro en aplicaciones web*. (2011). XVI Fórum de Ciencias y Técnica 2011 Facultad 2.

5. Castro Mecias, Lilian Teresa. (2011) *Competencias del rol de probador de seguridad para el proceso de certificación de roles en estudiantes de 4to año*. Evento Base Universidad 2012. Universidad de Ciencias Informáticas.

6. Oria Pardo, Leibys; Noa Cobas, José Miguel; Castro Mecias, Lilian Teresa;(2012) *Herramienta para el análisis y modelado de amenazas en sistemas* informáticos. UCIENCIA. VI Taller de Telemática y Seguridad en Redes y Sistemas.

7. Castro Mecias, Lilian Teresa; (2012). *Prácticas de Seguridad en el proceso de desarrollo de software*. UCIENCIA. VI Taller de Telemática y Seguridad en Redes y Sistemas.

8. Castro Mecias, Lilian Teresa; (2012). Gestión de la seguridad en aplicaciones durante el proceso de desarrollo. *3er Congreso Iberoamericano de Ingeniería de proyectos*.

9. Castro Mecias, Lilian Teresa. (2012). *Gestión de riesgos de seguridad en el desarrollo de aplicaciones web. Evento Nacional de Segurmática 2012.*

10. Castro Mecias, Lilian Teresa; Oria Pardo, Leibys; García Pérez, Félix Maikel;(2013) *Gestión de riesgos de seguridad en el desarrollo de aplicaciones web.* XI Seminario Iberoamericano de Seguridad en las Tecnologías de la Información. Informática 2013.

11. Castro Mecias, Lilian Teresa; Calderín Abad, Yenin; (2014) *Gestión de riesgos tecnológicos en proyectos de desarrollo de software*. Conferencia Científica de la Universidad de Ciencias Informáticas.

La investigación se encuentra estructurada en tres capítulos.

En el Capítulo 1 se establece el marco conceptual de la investigación, se analizan los principales referentes teóricos relacionados con la gestión de riesgos en el contexto de la seguridad del software y la gestión de proyectos para fundamentar la investigación así como la utilidad de estas prácticas en el proceso de desarrollo de software.

En el Capítulo 2 se define la Guía para la gestión del riesgo tecnológico en los proyectos de desarrollo de software de la institución a través del establecimiento de un conjunto de actividades, técnicas y desarrollo de artefactos que aseguren el cumplimiento de los objetivos de seguridad del software.

En el Capítulo 3 se refleja el diseño realizado para validar la guía propuesta, así como el análisis de los resultados obtenidos de su aplicación en el Centro TLM. Se evalúa e interpreta la información resultante.

CAPITULO 1 FUNDAMENTO TEÓRICO DE LA INVESTIGACIÓN

1.1 Introducción

La gestión de riesgos se considera un proceso necesario para el trabajo del equipo de proyecto. Este proceso permite valorar la probabilidad y el impacto de los eventos adversos de forma que se logren acciones que minimicen dichos efectos. Desde la perspectiva de seguridad en proyectos de Tecnologías de la información (TI), la gestión de riesgos implica entender y responder a los factores que pueden conducir a algún fallo en la confidencialidad, integridad o disponibilidad de un sistema de información. En el presente capítulo se conceptualizan los elementos que permiten establecer las bases teóricas de la investigación relacionadas con la gestión de riesgos, además se analizan algunos métodos que proponen establecer controles a las amenazas identificadas a través de requisitos de seguridad del software.

1.2 Análisis bibliométrico

La siguiente tabla muestra el comportamiento de la bibliografía consultada para la investigación teniendo en cuenta, los años de consulta y las categorías de las fuentes bibliográficas.

Tabla 2: Análisis bibliométrico. Fuente Elaboración propia

	Últimos 3 años	**Años anteriores**	**% de categorías**
Libros y monografías	5	7	13,3
Tesis de doctorado	2	3	5,5
Tesis de Maestrías	4	5	10
Artículos en revistas referenciadas	14	8	24,5
Memorias de eventos	9	5	15,6
Artículos publicados en la web	8	7	16,7
Reportes técnicos	7	6	14,4
Total	49	41	
% de actualidad	54,5 %	45,5%	

La búsqueda de información relacionada con el objeto de estudio de la presente investigación estuvo relacionada con los modelos, estándares y buenas prácticas en el marco de la gestión de proyectos y la gestión del riesgo tecnológico así como los elementos relacionados con la determinación de controles para minimizar el impacto de los riesgos de este tipo. Se utilizó fundamentalmente el Google Académico

así como la base de datos bibliográfica SCIELO, para un 56,3 % de actualidad. También se utilizaron como material de consulta tesis de Maestrías, doctorados y publicaciones en revistas referenciadas.

1.3 Asegurar el software

Hace algunos años asegurar el software se refería a una forma abreviada de garantizar la calidad del mismo, tratando dos propiedades puntuales: calidad y confiabilidad. Actualmente, la frase “asegurar el software” se adopta para expresar la idea de garantizar la seguridad y fiabilidad del software.

El Instituto Nacional de Estándares y Tecnologías, por sus siglas en inglés (NIST) Software Assurance Metrics and Tools Evaluation (SAMATE) y Department of Homeland Security (DHS) exponen que el objetivo de las actividades de asegurar el software es lograr un software que exhiba:

a) confiabilidad, por lo cual no hay vulnerabilidades o debilidades explotables, ya sea de origen malicioso o no intencionados.
b) ejecución predecible, por lo que hay confianza justificada de que las funciones del software son ejecutadas en la forma prevista.
c) conformidad, conjunto de actividades multidisciplinarias planificadas de forma sistemática que aseguran que los productos y procesos del software cumplen con los requerimientos, estándares y procedimientos.

El Object Management Group (OMG) proporciona la definición de asegurar el software como: Demostrar “confiabilidad justificada de que el software puede cumplir con sus objetivos de negocio y de seguridad".(DHS 2006)

Luego de analizar las definiciones anteriores teniendo en cuenta la existencia de patrones de ataques conocidos, se toma como definición que el aseguramiento del software significa que el mismo:

a) no puede ser forzado intencionalmente a fracasar en el cumplimiento de sus requerimientos funcionales y, continuará siendo fiable para la tarea que se construyó.
b) debe ser diseñado, implementado y configurado para seguir funcionando correctamente ante la presencia de la mayoría de los ataques, fallas o debilidades, tolerando los errores y fracasos que resulten de tales ataques.
c) debe ser diseñado, implementado y configurado para aislar, contener y limitar los daños ocasionados por los ataques que el software fue incapaz de resistir.

En base a lo cual se sustenta que el trabajo debe partir de un análisis de riesgos que considere las amenazas que pueden afectar los componentes del sistema y en consecuencia determinar las acciones para minimizar el efecto de estas amenazas. (McGraw 2006)

1.4 Marco Conceptual asociado a la gestión de riesgos

Riesgo

El Instituto de Ingeniería de software en (SEI 2012) define el riesgo como la posibilidad de sufrir daño o pérdida.

El Project Management Institute en (PMI 2013) define el riesgo de un proyecto como un evento o condición inciertos que, si ocurre, tiene un efecto positivo o negativo al menos en uno de los objetivos de dicho proyecto.

Considerando el riesgo en el contexto de la seguridad se conceptualiza del modo siguiente:

En la Guía de gestión de riesgos para sistemas de tecnologías de información - NIST SP 800-30, el riesgo se define como una función de la probabilidad que una fuente de amenaza está ejerciendo sobre una vulnerabilidad potencial en particular, y el impacto resultante de ese evento adverso sobre la organización. (Stoneburner 2002)

Una medida de la exposición a la que está sujeta un sistema o sistema potencial. (Yazar 2002)

La organización internacional para la estandarización – ISO define el riesgo como la "La posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias." (ISO/IEC 27005 2008)

En la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información – Magerit conceptualiza el riesgo como la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema. (MAP 2012)

La presente investigación se centra en la gestión del riesgo tecnológico, para la cual la autora tomará como referente la definición de riesgo dada por la ISO, en lo adelante se conceptualizan los términos amenaza, activo, vulnerabilidad y salvaguarda con el fin de la comprensión del concepto anterior.

Amenaza

El Instituto Nacional de Estándares y Tecnología define el término Amenaza como cualquier circunstancia o evento con el potencial de afectar adversamente las operaciones de la organización (incluyendo la misión, funciones, imagen o reputación), activos de la organización, los individuos, otras organizaciones, o de la nación a través de un sistema de información a través de acceso no autorizado, destrucción, divulgación, modificación de información y/o denegación de servicio. (Stoneburner 2002)

Activo

El activo esencial gestionado por los sistemas se conoce como la información o dato. Magerit define los Activos como recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objetivos propuestos por su dirección. (MAP 2012)

Vulnerabilidad

Se define en la guía para la Gestión de riesgos en Sistemas de Tecnologías de información como una falla o debilidad en los procedimientos de seguridad del sistema, el diseño, la implementación o los

controles internos que podrían ser ejercidas (provocado accidentalmente o explotado intencionalmente) y dar lugar a un fallo de seguridad o una violación de la política de seguridad del sistema. (Stoneburner 2002)

Salvaguarda

Procedimiento o mecanismo tecnológico que reduce el riesgo. (MAP 2012)

En (ISO/IEC 27005 2008) se trabaja como Control y se define como las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Gestión de Riesgos

El término gestión de riesgos se define según varias posiciones, muchas de las cuales separan el análisis de la gestión de los riesgos. Según la Guía de los Fundamentos de Dirección de proyectos PMBOK la gestión de riesgos del Proyecto incluye los procesos relacionados con la planificación de la gestión de riesgos, la identificación y el análisis de riesgos, las respuestas a los riesgos, y el seguimiento y control de riesgos de un proyecto; la mayoría de estos procesos se actualizan durante el proyecto.

Los objetivos de la Gestión de los Riesgos del Proyecto son aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos adversos para el proyecto. (PMI 2013)

La Agencia Europea de Seguridad de la Información y Redes (ENISA, por sus siglas en inglés), conformada por expertos de ocho estados miembros. El grupo de trabajo tiene entre sus objetivos producir y revisar metodologías existentes de análisis y gestión de riesgos, acciones fundamentales en esta área y la comparación de diferentes metodologías.

Para ENISA el proceso de Evaluación de riesgos es un proceso científico y tecnológico que comprende cuatro etapas: la identificación de las amenazas, caracterización de las amenazas, la evaluación de la exposición y caracterización del riesgo.

La gestión de riesgos es el proceso, que consiste en ponderar políticas alternativas, en consulta con las partes interesadas, analizar la evaluación de riesgos y otros factores legítimos y, si es necesario, seleccionar las opciones apropiadas de prevención y control.(ENISA 2006)

Magerit ofrece los conceptos de análisis y gestión de riesgos de la siguiente manera:

Análisis de riesgos: Identificación de las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como activos); para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización, obteniendo cierto conocimiento del riesgo que se corre.

Gestión de riesgos: Selección e implantación de las medidas o salvaguardas de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios. La gestión de riesgos se basa en los resultados obtenidos en el análisis de los riesgos.

Es posible concluir como (Ochoa 2010) que el análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis. En la siguiente figura se muestra la relación entre los conceptos que engloban la gestión de riesgos asociado a las tecnologías de la información. Figura 1

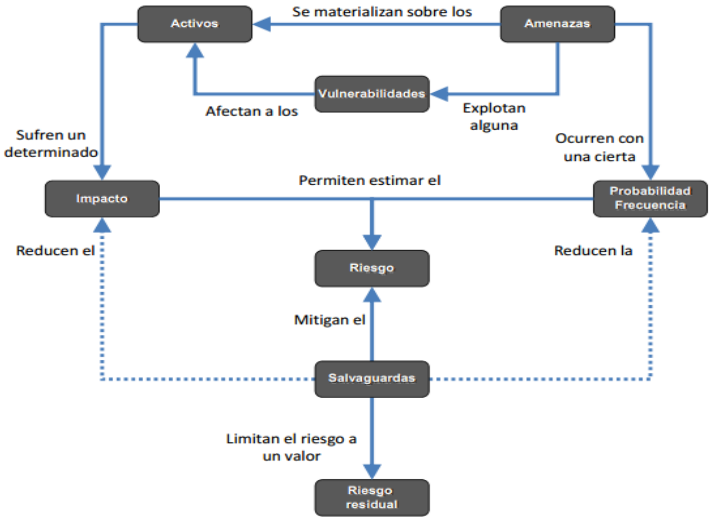


Figura 1: Mapa conceptual asociado a la gestión del riesgo. Fuente (MAP 2012)

1.5 Metodologías de Gestión del riesgo tecnológico

Existen numerosas metodologías de análisis y gestión de riesgos, la elección de una u otra depende de factores específicos de la organización. Al finalizar el epígrafe se realiza un análisis crítico basado en los objetivos de la investigación.

1.5.1 MAGERIT – Metodología de análisis y gestión de riesgos de los Sistemas de información

El Consejo Superior de Administración electrónica ha elaborado y promueve Magerit como respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos. El uso de las TIC supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios.

Filosofía

Magerit persigue los siguientes objetivos concienciar a los responsables de las organizaciones de la existencia de riesgos y de la necesidad de gestionarlos, ofrecer un método sistemático para analizar los riesgos derivados del uso de las TIC, ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control. Además de buscar la uniformidad de los informes que recogen los hallazgos y las conclusiones de las actividades de análisis y gestión de riesgos.(MAP 2012)

Principios Básicos

- Magerit considera la gestión de los riesgos como una piedra angular en las guías de buen gobierno público o privado, donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos que implican.
- El conocimiento de los riesgos permite calibrar la confianza en que los sistemas desempeñarán su función como la Dirección espera.

Estructura o Fases

El análisis de riesgos propuesto por Magerit permite determinar qué es lo que tiene la organización y qué es lo que podría pasar. Siendo una aproximación metódica de pasos pautados:

Tabla 3. Proceso de la Metodología de Análisis y gestión de riesgos de los Sistemas de información Magerit. Fuente Elaboración propia

Proceso de Magerit v3	
MAR.1 – Caracterización de los activos	MAR.11 – Identificación de los activos MAR.12 – Dependencias entre activos MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas	MAR.21 – Identificación de las amenazas MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas	MAR.31 – Identificación de las salvaguardas pertinentes MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo	MAR.41 – Estimación del impacto MAR.42 – Estimación del riesgo

Magerit ofrece una guía para el análisis y gestión de riesgos que permite la realización de las actividades de forma sistemática pero no se corresponde de forma total con los objetivos de la investigación pues el análisis no se enfoca al desarrollo de software, los roles definidos están enfocados a la dirección, gestión y mantenimiento de una infraestructura de TI. Las técnicas para la gestión de los riesgos carecen del enfoque necesario para la determinación de los controles de seguridad del software

desde las fases iniciales del desarrollo. El desarrollo de la investigación tendrá en cuenta las buenas prácticas utilizadas para la identificación y caracterización de amenazas.

1.5.2 ISO/IEC 27005:2008

Esta norma ISO/IEC 27005:2008 proporciona directrices para la gestión de riesgos de seguridad de la información. Esto apoya los conceptos generales especificados en ISO/IEC 27001 y ha sido diseñada para ayudar a la puesta en práctica satisfactoria del análisis y la gestión del riesgo, fase principal del diseño de todo sistema de gestión de la seguridad de la información (SGSI). En 2011 fue revisada y actualizada para reflejar el contenido de los documentos de gestión de riesgos ISO 31000:2009, Gestión de riesgos - Principios y directrices, ISO/IEC 31010:2009, Gestión de riesgos - las técnicas de evaluación de riesgos y la ISO Guía 73: 2009, La gestión del riesgo – Vocabulario. (ISO/IEC 2008)

Filosofía

Es aplicable a todos los tipos de organizaciones (sociedades mercantiles, administraciones públicas, organizaciones no lucrativas) que tengan la intención de manejar los riesgos que podrían comprometer la seguridad de la información de la organización. Sus disposiciones hacen énfasis en el concepto de SGSI de ISO/IEC 27001:2005.

No proporciona ninguna metodología específica para la gestión de riesgos, pero aporta un enfoque genérico. Dependiendo, cada organización redefinirá el enfoque de gestión de riesgos, en función, por ejemplo, del alcance del sistema de gestión de seguridad, con base en el contexto de la gestión del riesgo, o en el sector de la industria. (Bahtit 2013)

Principios Básicos

- Sirve de apoyo a la ISO 27001 y a la implantación de un SGSI.
- Ayuda a las organizaciones con consejos sobre el por qué, qué y cómo de la gestión de los riesgos de seguridad de la información en apoyo a los objetivos de su gobierno.
- La norma tiene el propósito de alinearse con ISO 31000:2009 con el fin de ayudar a las organizaciones que deseen gestionar sus riesgos de seguridad de la información de una manera similar a la forma de gestionar otros riesgos.

Estructura o Fases

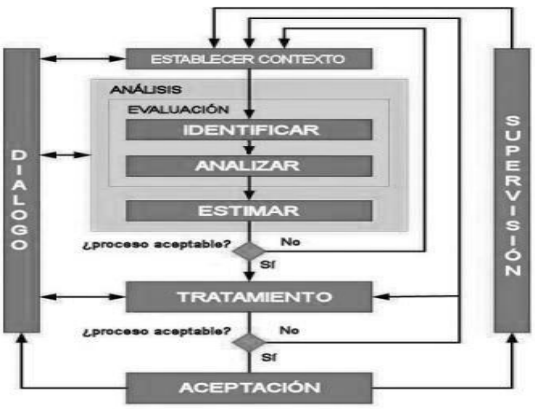


Figura 2. Proceso de ISO/IEC 2005:2008. Fuente (ISO/IEC 2008)

El estándar ISO/IEC 27005 ofrece un marco declarativo asociado al análisis y gestión de riesgos de seguridad. La investigación tendrá en cuenta las buenas prácticas del estándar en relación con el enfoque PDCA (Planificar. Hacer, Controlar y Actualizar). A diferencia de otros estándares enfoca su análisis de forma que sea adaptada según las características de la organización pero las técnicas sugeridas no se enfocan a la gestión del riesgo tecnológico desde el desarrollo del producto de software de forma que apoye la definición de requerimientos de seguridad y el control de este atributo en fases posteriores. El estándar se subordina completamente al establecimiento de un SGSI

1.5.3 SP 800 30 - Risk Management Guide for Information Technology systems

Desarrollado por el Instituto Nacional de Estándares y Tecnología - por sus siglas en inglés- NIST en el 2002. La SP800-30 se encuentra alineada con el resto de las publicaciones del NIST sobre normalización y estandarización de las tecnologías. Forma parte de los informes de publicaciones especiales de seguridad de la serie 800. Contiene las definiciones y una guía práctica necesaria para evaluar y mitigar los riesgos identificados desde el interior del sistema de TI.

Filosofía

- El objetivo de realizar la gestión de riesgos es permitir a la organización cumplir con su misión.
- Afianzar la seguridad de sistemas de TI que guarden, procesen y transmitan información organizacional.
- Ayudar a la dirección a autorizar los sistemas de TI en base a la documentación de apoyo que es el resultado del desempeño de la gestión de riesgos.

Principios Básicos

Los informes de la series 800 forman el conjunto de directrices del NIST relacionadas con la seguridad de los sistema de información. Es una guía detallada de las consideraciones que deben hacerse para llevar a cabo una evaluación y una gestión de riesgos orientada a la seguridad de los sistemas de información.

Estructura o Fases

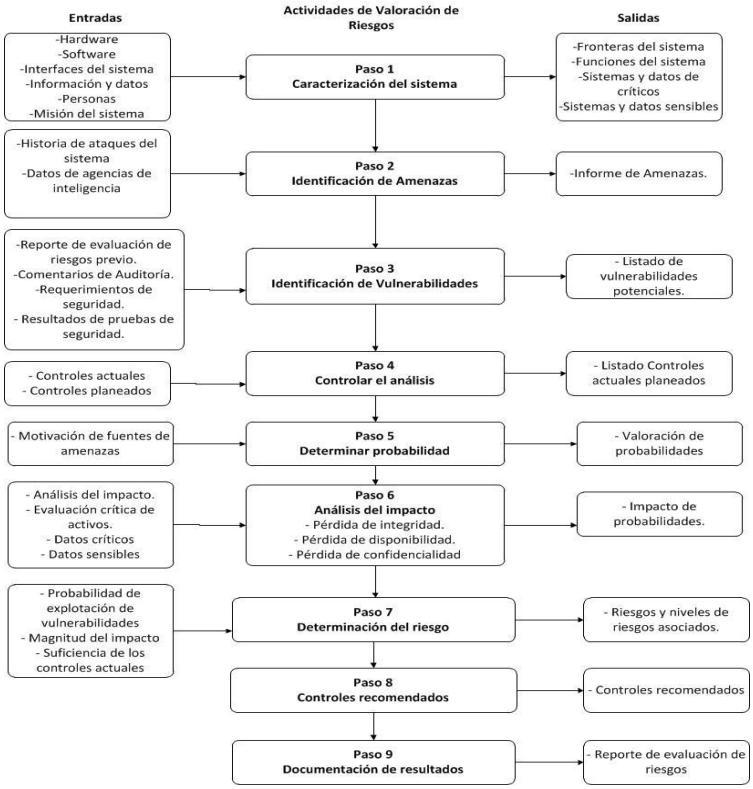


Figura 3. Diagrama de flujo de trabajo SP 800-30. Fuente Traducida a partir de (Stoneburner 2002)

La Guía para gestión de riesgos en sistemas de tecnologías de información forma parte de la serie 800 relacionada con la seguridad. La SP 800-30 describe un proceso a partir de entradas, actividades y salidas en cada paso de la guía que sirve de referencia para el trabajo de análisis y gestión de los riesgos. Sin embargo es insuficiente en el cómo realizar muchas actividades, es decir adolece de técnicas que permitan identificar las amenazas y determinación de los controles asociado a la realización de esta tarea durante las fases iniciales del desarrollo del sistema.

Resumen metodologías y estándares de gestión del riesgo tecnológico

Sobre la base de algunos atributos definidos por (ENISA 2006) se muestran los métodos analizados anteriormente para el análisis y gestión del riesgo tecnológico, se incluye la norma ISO/IEC 27005:2008 y Magerit. El número de asteriscos (*) puede variar de ninguno a tres, representa el grado de cumplimiento de la fase.

Tabla 4. Resumen atributos presentes en los modelos de gestión del riesgo tecnológico. Fuente elaborado a partir de (ENISA, 2006).

	Identificación de amenazas	Caracterización de amenazas	Evaluación de riesgos	Tratamiento de riesgos	Comunicación de riesgos	Tipo de organización
MAGERIT	***	***	***	***		Todas

ISO/IEC 27005	**	**	**	***	***	Todas
SP 800-30	***	***	***	***		Todas

1.6 Metodologías de gestión de riesgos en el contexto de la gestión de proyectos

La gestión y el tratamiento de los riesgos, a lo largo del desarrollo de un proyecto de software, permite evitar o reducir notablemente los problemas que se presentan y que hacen que los proyectos fracasen (Boehm 1991). Se realiza un análisis del tratamiento dado a los riesgos en algunas metodologías en el contexto de la gestión de proyectos. Al finalizar el epígrafe se realiza un análisis crítico basado en los objetivos de la investigación.

1.6.1 PMBOK

El estándar PMBOK es conocido como la guía de cuerpo de conocimiento para la gestión de proyectos. Es un estándar para la gestión de proyectos propuesto por el Instituto de Gestión de Proyectos (PMI). Esta guía es reconocida como estándar internacional IEE Std 1490-2003. Su propuesta está basada en proporcionar fundamentos de gestión de proyectos aplicables en diferentes áreas.

Filosofía

El principal propósito del documento que comprende la guía PMBOK, es identificar y definir el conocimiento y las prácticas de gestión de proyectos que generalmente son aplicables a la mayoría de los proyectos, la mayor parte del tiempo. Lo cual no quiere decir que los conocimientos descritos deban aplicarse siempre de forma uniforme en todos los proyectos; el equipo de dirección del proyecto es responsable de determinar lo que es apropiado para cada proyecto determinado. Con la identificación y definición de dichas prácticas, esta guía pretende además de identificar y definir el conocimiento y las prácticas del área de gestión de proyectos, establecer un léxico común para esta área.

Principios básicos

La estructura de la guía PMBOK está compuesta por nueve áreas de conocimiento con sus respectivas prácticas. Descritas, a su vez en términos, de componentes de proceso. Estos últimos están internamente clasificados en entradas necesarias para el proceso, herramientas, técnicas y salidas correspondientes para cada práctica. Dedica un área de conocimiento a la gestión de riesgos y establece las actividades a realizar con sus correspondientes indicaciones respecto a técnicas y entradas requeridas para la ejecución de la actividad.

Estructura o Fases

En relación a la gestión de riesgos, concibe las fases de planificar la gestión de riesgos, identificar los riesgos, realizar el análisis cualitativo y cuantitativo de los riesgos, planificar la respuesta a los riesgos y controlar los riesgos. A continuación se presenta el objetivo de cada fase.

La planificación de la gestión de riesgos es el proceso de definir cómo realizar las actividades de gestión de riesgos de un proyecto.

La identificación de los riesgos es el proceso de determinar los riesgos que pueden afectar al proyecto y documentar sus características.

La realización del análisis cualitativo de los riesgos es el proceso de priorizar riesgos para análisis o acción posterior, evaluando y combinando la probabilidad de ocurrencia e impacto de dichos riesgos.

La realización del análisis cuantitativo de los riesgos es el proceso de analizar numéricamente el efecto de los riesgos identificados sobre los objetivos generales del proyecto.

La planificación de la respuesta a los riesgos es el proceso de desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.

El proceso de controlar los riesgos consiste en implementar los planes de respuesta a los riesgos, monitorear los riesgos identificados, monitorear los riesgos residuales, identificar nuevos riesgos y evaluar la efectividad del proceso de gestión de los riesgos a través del proyecto. (PMI 2013)

La disciplina de gestión de riesgos del PMBOK a través de la definición de sus actividades, herramientas, técnicas y las salidas en cada caso ofrece un marco de trabajo aceptado en la institución para la gestión de riesgos. Las actividades de identificación de riesgos, análisis cualitativo, planificación de la respuesta y el control de los riesgos servirán de base para la definición de la propuesta, debido a que no cuentan con las herramientas y técnicas que permiten la gestión del riesgo tecnológico.

1.6.2 Modelo Integrado de Madurez y Capacidad - CMMI

El Modelo Integrado de Madurez y Capacidad (CMMI) fue desarrollado inicialmente por el Gobierno de Estados Unidos y el Instituto de Ingeniería de software (SEI) para aplicarlos a la mejora de procesos de desarrollo y servicios en todo el ciclo de vida. CMMI utiliza en su modelo la premisa de la gestión de procesos “la calidad de un sistema o producto está muy influenciado por la calidad del proceso utilizado para desarrollarlo y mantenerlo”. (SEI 2010)

Filosofía

Los componentes del modelo se estructuran en áreas de proceso, prácticas específicas y prácticas genéricas. Una práctica específica (SG) describe las únicas características que deben estar presentes para satisfacer el área del proceso. Se llaman prácticas genéricas (SP) porque la misma declaración de la práctica aplica a múltiples áreas del proceso. Una meta genérica describe las características que deben estar presentes para institucionalizar los procesos que lleve a cabo un área del proceso.

Principios básicos

CMMI contempla 5 niveles para evaluar la madurez de los procesos en las organizaciones. El nivel II de CMMI establece las Áreas de proceso (AP) de Gestión de requerimientos, Planificación de proyecto,

Monitorización y control de proyecto, Gestión de acuerdos con proveedores, Medición y análisis, Aseguramiento de la calidad de proceso y de producto y Gestión de la configuración.

En cuanto a la gestión de riesgos el AP de Planificación de proyecto y Monitoreo y control del proyecto a través de sus políticas establecen la indicación de identificar, documentar y analizar los riesgos del proyecto así como monitorear el estado de estos riesgos. A su vez estas AP en sus prácticas y subprácticas convienen lo siguiente:

AP Planificación de proyecto, indica desarrollar un plan de proyecto e incluye la práctica identificar los riesgos del proyecto. Las subprácticas asociadas refieren identificar los riesgos, documentarlos, revisarlos y obtener un acuerdo con los involucrados sobre la completitud y la corrección de los riesgos documentados.

AP Monitoreo y control del proyecto indica que se debe monitorizar el proyecto frente al plan, que incluye la práctica monitorizar los riesgos del proyecto. Las subprácticas en este caso son: revisar periódicamente la documentación de los riesgos en el contexto del estado y de las circunstancias actuales del proyecto, corregir la documentación de los riesgos para incorporar los cambios y comunicar el estado de los riesgos a las partes interesadas relevantes. Pero la gestión de riesgos como área de procesos es contemplada en el nivel 3 de madurez y en la categoría Gestión de Proyecto.

Estructura o Fases

Tabla 5. Prácticas genéricas y específicas del área de procesos de gestión de riesgos de CMMI nivel 3. Fuente Elaboración propia

Área de procesos de gestión de riesgos. CMMI nivel 3.	
SG 1 Preparar la gestión de riesgos.	SP 1.1 Determinar las fuentes y las categorías de los riesgos. SP 1.2 Definir los parámetros de los riesgos. SP 1.3 Establecer una estrategia de gestión de riesgos.
SG 2 Identificar y analizar los riesgos.	SP 2.1 Identificar riesgos. SP 2.2 Evaluar, categorizar y priorizar los riesgos.
SG 3 Mitigar los riesgos.	SP 3.1 Desarrollar los planes de mitigación de riesgo. SP 3.2 Implementar los planes de mitigación de riesgo.

CMMI declara las prácticas genéricas y especificas que deben ser satisfechas por las organizaciones para satisfacer la implementación del modelo. El cómo se define en la institución a través de libros de procesos que ofrece a los equipos de trabajo indicaciones de cómo desarrollar las actividades relacionadas con el proceso de desarrollo del software. En relación a la gestión de riesgos los procesos

definidos no cuentan con actividades, herramientas y/o técnicas que permitan la gestión del riesgo tecnológico y que favorezca el tratamiento de la seguridad durante el ciclo de vida del desarrollo del software.

1.7 Investigaciones relacionadas con la Gestión de riesgos en la Universidad

En (Zulueta 2007) se presenta un “Modelo de Gestión de Riesgos en Proyectos de Desarrollo de Software (MoGeRi)” como resultado de una investigación para obtener el título de Máster en Ciencias. Está basado en el análisis de los puntos en común de varias metodologías. MoGeRi se desarrolló adaptada a las características de la Universidad de las Ciencias Informáticas (UCI) en ese momento. El modelo se ha aplicado satisfactoriamente en varios proyectos de desarrollo de la UCI como en (González 2008)(Gutiérrez 2008)(Palarea 2008)(Escobar 2009)(Reyes 2009)(Alvarez 2011). Las actividades de MoGeRi se organizan en seis procesos que permiten la planificación, identificación de los riesgos, los procesos de análisis y la planificación de respuestas a los mismos, así como su seguimiento y control.

Definido en 2010 en la tesis para optar por el título de Máster en Ciencias (Arenas 2010) expone un “Proceso de Gestión de riesgos para proyectos de desarrollo de software de Softel”, el mismo se encuentra contextualizado en el marco de desarrollo de software en esa entidad a partir del estudio de sus características. El proceso definido fue evaluado por método de expertos luego de ser aplicado en Softel, demostrando su utilidad práctica para continuar su implantación y ser generalizado a otros proyectos con el consiguiente beneficio a la mejora de la gestión de los proyectos de la organización siempre que cumplan las características de este tipo de organización.

En (Rivera 2010) se presenta un “Modelo de un sistema de razonamiento basado en casos para el análisis en la gestión de riesgos” para la Unidad de Compatibilización, Integración y Desarrollo de Productos Informáticos para la Defensa (UCID) como tesis de maestría. En la investigación el autor define un modelo de razonamiento basado en casos para asistir a la búsqueda y reutilización de riesgos con características similares, definiendo un conjunto de principios y premisas para aplicarlo en entornos de desarrollo de software. Propone el empleo de una base de conocimiento de riesgos y a partir de esta se describen los procesos de inferencia y aprendizaje, que garantizan la recuperación y empleo de riesgos similares en el proceso de análisis.

En (Lujan 2012) se detalla un Proceso de gestión de riesgos, con productos de trabajo, técnicas e indicadores. Además propone el uso de una herramienta inteligente que utilice las experiencias en función de identificar riesgos y estrategias de mitigación a partir de la experiencia de la organización en la gestión de riesgos. El proceso propuesto consta de seis actividades entre las que se encuentran determinación del alcance, planificación, identificación, análisis, planificación de la estrategia y seguimiento y control. La aplicación del Proceso de gestión de riesgos para el Desarrollo de Aplicaciones Informáticas definido en la investigación apoya a la organización con resultados que permiten tomar decisiones relacionadas con la gestión de riesgos.

En (Moya 2013) se define un proceso para gestionar riesgos en los proyectos de desarrollo de software del Centro de Informatización Universitaria (CENIA), como elemento que contribuye con la formación de los jefes de proyectos en la implementación de respuestas anticipadas. Incluye la descripción de los subprocesos que conforman la propuesta: planificación de la gestión de riesgos, identificación y análisis de los riesgos, definición y aplicación de acciones para la resolución de eventualidades, comunicación y control de los riesgos y evaluación del proceso de gestión de riesgos. El aporte de la investigación radica en la definición de un proceso para gestionar riesgos en los proyectos de desarrollo de software del CENIA y en la aplicación del modelo lingüístico virtual para analizarlos.

Las investigaciones analizadas se basan en el análisis de los modelos y buenas prácticas relacionadas con la gestión de riesgos asociadas a proyectos de software. En cada caso su definición se contextualiza en las condiciones de la infraestructura productiva y el ajuste de los procesos relacionados con la producción de software en la institución. No se ajustan a las necesidades de la presente investigación pues las técnicas que se emplean no se ajustan a la gestión del riesgo tecnológico de forma que se estructuren las necesidades de seguridad mediante la determinación de los requisitos de seguridad del software.

1.8 Técnicas de identificación de riesgos

La identificación de riesgos es considerada como la fase principal de un proceso continuo de gestión de riesgos. De una buena identificación de riesgos depende la efectividad de las demás fases. Es preciso facilitar los métodos y técnicas de identificación de riesgos que permiten establecer una base de riesgos sólida. Sin embargo los enfoques existentes tienden a orientarse en la experiencia y carecen de técnicas y métodos que apoyen la fase de identificación. (Hurtado 2010)

1.8.1 Tormenta de Ideas (Brainstorming)

Es usada extendidamente en la planificación de proyectos con el objetivo de advertir e identificar posibles escenarios de riesgos, en un proyecto particular. Es un simple y efectivo intento para ayudar a las personas, pensar creativamente en grupo, sin inhibir sentimientos o ser criticados por otros.(Vargas 2008). Este método si bien es creativo y sinérgico, si no se ejecuta de forma adecuada y bien coordinada puede generar caos. A continuación se muestra el proceso para la ejecución de esta técnica:

Figura 4. Proceso para desarrollar el método de tormenta de ideas. Elaborado a partir de (Hurtado 2010)

1.8.2 Método basado en analogías

Este método se basa en la comparación de dos escenarios idénticos. Es necesario tener como base algún tipo de antecedentes. Deben existir referencias para poder generar un listado de riesgos. Sin embargo, la información previa, los antecedentes y experiencia deben estar ajustados a las condiciones o el escenario actual, de lo contrario este método no puede ajustarse a las condiciones reales actuales. Es indispensable la experiencia previa en situaciones similares a las que se desea aplicar el método.

Figura 5. Proceso para desarrollar el método basado en analogías. Elaborado a partir de (Hurtado 2010)

1.8.3 Listas de Chequeos, formatos o plantillas

La recopilación de información a partir de la experiencia previa de otros proyectos permite la utilización de plantillas, formatos o listas de chequeo. Estas tres opciones se pueden utilizar cuando existe en la organización los datos históricos de proyectos anteriores. Estas opciones de identificación de riesgos están generadas bajo la premisa de que los nuevos proyectos nunca tienen un conjunto de riesgos del todo nuevo, sino que los nuevos proyectos deben refinar un listado de riesgos preestablecidos. Estas opciones para identificar riesgos, generalmente son utilizadas a partir de una estructura de desglose de riesgos (WBS de riesgos).

1.9 Métodos para abordar la gestión de riesgos

Las actividades propias de la gestión de riesgos tienen su fundamento en el resultado del trabajo realizado a partir del análisis de riesgos, de forma que se estructuren las acciones de seguridad para satisfacer las necesidades detectadas por el análisis de riesgos. El proceso de gestión de riesgos descrito por las metodologías analizadas, indican la necesidad de determinar salvaguardas o controles para mitigar el efecto de los eventos negativos, como una fase importante en el proceso.(Yazar 2002)(MAP 2012)(Stoneburner 2002)(Alberts 2003) (ENISA 2006) Las actividades de gestión de riesgos permiten responder a los factores que pueden conducir a algún fallo en la confidencialidad, integridad o disponibilidad de un sistema de información.

Determinar las respuestas más acertadas en etapas tempranas del proceso de desarrollo, facilitará al equipo de desarrollo la implementación de los controles de seguridad requeridos. Para abordar estar tarea asociado al proceso de desarrollo de software se considera el análisis de los métodos propuestos por la Ingeniería de requisitos de seguridad (IRS) que permitan la elección de requisitos funcionales y no funcionales de seguridad, en correspondencia con el valor de los activos del sistema y la proporción del riesgo.

Ingeniería de Requisitos de Seguridad

La Ingeniería de Requisitos de Seguridad (IRS) es el proceso de elicitar, especificar y analizar los requisitos de seguridad para las ideas fundamentales del sistema en cuanto a cuáles son las necesidades de seguridad, es decir se refiere a considerar la prevención de los daños en el mundo real y considerarlos como restricciones sobre requisitos funcionales. (Salini 2011)

La IRS reconoce a los requisitos de seguridad como:

Requisitos funcionales de seguridad: Una condición o capacidad necesaria en el sistema para controlar o limitar el cumplimiento de los requisitos.

Requisitos no funcionales de seguridad: Una propiedad del sistema necesaria para asegurar el cumplimiento de los requisitos frente al abuso o mal uso.

Requisitos de seguridad derivados: A partir de los requisitos funcionales y de otros requisitos de seguridad.

1.9.1 Security Requirements Engineering Process (SREP)

SREP propone un total de 9 pasos para la realización del proceso de obtención de los requisitos de seguridad, está basado parcialmente en la metodología SQUARE pero incorpora consideraciones de los Criterios Comunes (ISO/IEC 15408) integrados en el Ciclo de Vida de desarrollo del software junto con la reutilización de requisitos de seguridad. (Mellado 2007). El proceso se muestra en la figura 8.

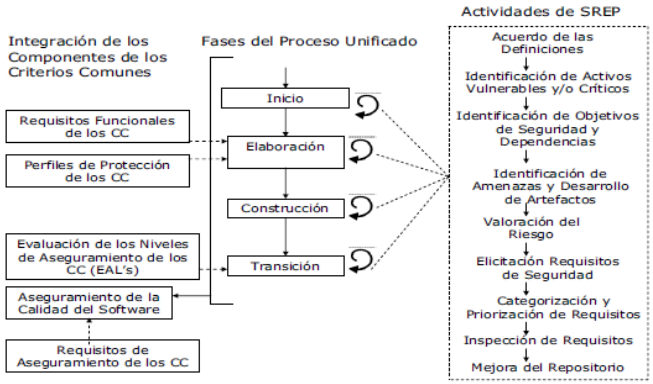


Figura 6. Visión general de SREP. Fuente (Mellado 2007)

1.9.2 Modelo de procesos para identificación de requisitos de seguridad

El proceso establece requisitos de seguridad a partir de identificar riesgos para alcanzar la seguridad del software, visto como un atributo de calidad. Todo el proceso se inicia a través de una completa gestión de riesgos basados en activos durante la fase de ingeniería de requisitos del desarrollo de software. Todos los posibles riesgos relacionados con el proyecto se especifican, en primer lugar se identifican y analizan por cuantificación de sus impactos y asignada a un atributo de calidad. Estos riesgos identificados deben ser controlados a un nivel aceptable mediante la integración de las estrategias de gestión de riesgo basado en los requisitos de seguridad resultantes. Finalmente se deben

obtener las tecnologías de seguridad, protocolos y mecanismos para alcanzar la calidad y seguridad del software. (Islam 2010) El proceso se muestra en la Figura 9.

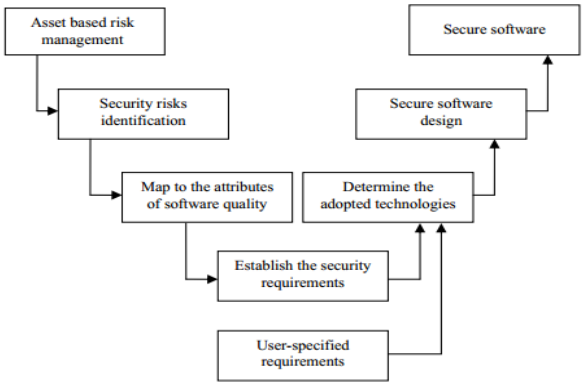


Figura 7. Modelo de procesos para identificación de requisitos de seguridad. Fuente (Islam 2010)

1.9.3 Método de Ingeniería de seguridad y requisitos relacionados con la seguridad

Según (Firesmith 2011) el Método de Ingeniería de seguridad y requisitos relacionados con la seguridad, por sus siglas en inglés- ESSR consiste en un análisis basado en tareas, que incluye un análisis de los siguientes aspectos: análisis de involucrados, análisis de activos, análisis de abusos, análisis de vulnerabilidades, análisis de peligro, análisis de riesgo, alcance del análisis de seguridad y determinación de las defensas.

Análisis de activos: determina los activos que deben ser protegidos de cualquier daño no autorizado. Modelan cada activo defendido, determinan su valor e identifican los tipos y la gravedad de los daños que pueda sufrir.

Análisis de abusos: examina las formas en que el sistema y los activos de los que el sistema es el responsable puede ser abusado. Se deben modelar estos abusos, utilizando técnicas apropiadas (por ejemplo, modelado de casos de abuso, árboles de ataque).

Análisis de intrusos: determina las personas externas al sistema que pueden abusar de forma accidental o malintencionada del sistema y de los activos que tiene que defender de cualquier daño no autorizado.

Resumen de los métodos para la IRS

Los métodos analizados para la IRS concuerdan en la adopción de un enfoque distinto para asegurar el software. Este enfoque se determina por la realización de un análisis de riesgos que identifique las necesidades de seguridad y se cubran a partir de la implementación de los controles o salvaguardas establecido por el equipo de desarrollo.

La identificación de los requisitos de seguridad es el momento para analizar los ataques que el sistema debe evitar, los tipos de vulnerabilidades que no debe incorporar, las amenazas de las que deberá protegerse así como la máxima seguridad aceptable. De manera que permita defenderse él mismo y

proteger los activos, bienes, servicios y personas asociados en correspondencia con la valoración del riesgo realizada.

1.10 Técnicas para la elicitación de requisitos de seguridad

La elicitación de requisitos es un área de investigación activa sin embargo en la actualidad hay pocos estudios que comparan la eficacia de los diferentes métodos para la obtención de requisitos de seguridad. A continuación se analizan una serie de métodos.

1.10.1 Issue-Based Information Systems - IBIS

Desarrollado por Horst Rittel, él método IBIS en la década de 1970 para mejorar la definición, la discusión y resolución de problemas denominados como malignos, es un intercambio entre los involucrados que aportan su experiencia personal y la perspectiva a la solución de problemas.

En IBIS, todos los problemas se descomponen en forma de preguntas abiertas para los grupos de interés. Una pregunta podría ser, por ejemplo, ¿Cómo se protege el sistema de las amenazas internas? Cada problema se resuelve después por posiciones propuestas, que son soluciones a la cuestión planteada por las partes interesadas. Cada posición tiene argumentos correspondientes que, o bien apoyan o se oponen a la posición. El ingeniero de requisitos se encarga de registrar la articulación de las cuestiones, posiciones y argumentos. Los resultados se presentan en la forma de un mapa IBIS (IM).

Los mapas IBIS son analizados por el equipo de ingeniería de requisitos y el cliente para obtener los requisitos de seguridad actuales. La eficacia de IBIS en la obtención de los requisitos de seguridad depende de la calidad de las preguntas de la entrevista. En la medida de lo posible, el alcance de las preguntas debe cubrir todo el rango de los requisitos de seguridad que podría implicar el sistema. Lo más importante, es que el entrevistador debe ser persistente para alentar a las partes interesadas para explicar su fundamento cuando se propone una solución a un problema. (SEI 2006)

1.10.2 Casos de mal uso, casos de abuso

La adaptación de los casos de uso es un conjunto de aproximaciones para el desarrollo de requerimientos que enfocan la seguridad del software. Se han nombrado como casos de abuso, casos de mal uso y casos de uso hostiles para distinguirlos del caso de uso estándar. Lo que tienen en común todos ellos es que ven el software desde el punto de vista de un adversario. Del mismo modo que los casos de uso se utilizan exitosamente para elicitar requisitos, los casos de mal uso son utilizados para identificar potenciales amenazas, a partir de las cuales es posible elicitar requisitos de seguridad o casos de uso de seguridad. (Alexander 2002)
La interacción del usuario autorizado con el sistema es diagramada simultáneamente con las interacciones del usuario hostil. Y así como en los casos de uso las conexiones entre actor y acción se etiquetan con términos como extiende e incluye, las conexiones en un caso de mal uso son etiquetadas con amenaza y mitiga. Los casos de mal uso forman los cimientos para construir un conjunto de casos de uso seguros para contrarrestar cada una de las amenazas. Como su caso de uso, cada caso de mal uso conduce a un requerimiento y el correspondiente escenario de prueba para el software. De este

modo, gran parte del trabajo invertido en la construcción de los casos de mal uso resulta en el desarrollo de requisitos funcionales de seguridad.
El objetivo es identificar amenazas a la seguridad en cada una de las funciones, áreas, procesos, datos y transacciones involucradas en el caso de uso a partir de potenciales riesgos, como pueden ser los accesos no autorizados desde adentro y desde afuera, ataques de Denegación de servicios (DoS), violaciones a la privacidad, confidencialidad e integridad y ataques malintencionados por parte de hackers. Además de estudiar los modos de ataque, el proceso podría también intentar descubrir posibles errores de los usuarios y la correspondiente respuesta de la aplicación. (Damodaran 2006)

1.11 Conclusiones del capítulo

La revisión bibliográfica muestra la tendencia a encontrar consensos en el uso de prácticas que garanticen la seguridad del software y la necesidad de integrarla desde fases tempranas del Ciclo de Vida de Desarrollo del software, recomendando con gran énfasis para ello el análisis y gestión de riesgos.

Los métodos para la gestión de la seguridad a través de la gestión del riesgo tecnológico no enfocan la realización de estas actividades al proceso de desarrollo del software sino a su aplicación en una infraestructura dependiente de sistemas de información y el análisis de las amenazas y valoración de los riesgos en dicho entorno.

Las metodologías y modelos analizados asociadas a la gestión de proyectos carecen de técnicas y herramientas con el enfoque adecuado para la gestión del riesgo tecnológico, es decir no poseen indicaciones en relación a la identificación de amenazas a los activos del software, valoración del riesgo que representan esas amenazas así como para el control y seguimiento del riesgo.

En la institución no se encontraron evidencias del empleo de técnicas, métodos, modelos o procedimientos de gestión de riesgos que incluyan el análisis y obtención de requisitos de seguridad como vía para asegurar los activos de los sistemas de información y minimizar los eventos adversos que puedan afectarlo.

La propuesta se ajusta a partir del proceso de gestión de riesgos del PMBOK en base a lo cual se diseña una guía que contenga las actividades, herramientas y técnicas requeridas para la gestión del riesgo tecnológico.

La propuesta tendrá en cuenta las buenas prácticas de los métodos de gestión del riesgo tecnológico Magerit, la publicación especial SP 800-30 y la norma ISO/IEC 27005:2008. Para la determinación de requisitos de seguridad el método propuesto por Mellado y la técnica de los casos de abuso para elicitar requisitos a partir de un análisis de riesgos.

CAPÍTULO 2 GUÍA DE GESTIÓN DEL RIESGO TECNOLÓGICO PARA EL TRATAMIENTO DE LA SEGURIDAD DURANTE EL DESARROLLO DE SOFTWARE.

2.1 Introducción

En este capítulo se describe una guía que, basada en el análisis y gestión del riesgo tecnológico, permite obtener los requisitos de seguridad del software. Además se definen las entradas, actividades, involucrados y salidas necesarias de cada una de las actividades componentes de la propuesta. Se muestra una descripción gráfica con el objetivo de facilitar la comprensión de todos sus elementos.

2.2 Guía de gestión del riesgo tecnológico

La guía fue diseñada a partir de las mejores prácticas contenidas en los modelos estudiados (MAP 2012)(Mellado 2007)(Stoneburner 2002) (ISO/IEC 27005 2008) y ajustado a las fases del proceso de gestión de riesgos en (PMI 2013). Además determina las técnicas y herramientas para la gestión del riesgo tecnológico desde el proceso de desarrollo de software. Se definen las responsabilidades de los roles involucrados en la ejecución de las actividades, las cuales se enmarcan en las fases del ciclo de vida de desarrollo del software establecido en la Universidad.

La guía propuesta tiene los siguientes objetivos:

- Mitigar, reducir o eliminar el riesgo a partir de que se determinen los requisitos de seguridad del software adecuados, considerando la probabilidad de ocurrencia y el impacto potencial de las amenazas identificadas.
- Proveer al especialista de una entrada en la Fase de pruebas que permita evaluar la eficacia de los requisitos de seguridad implementados y el comportamiento del sistema en el desempeño de su misión.
- Proporcionar un conjunto de técnicas y herramientas para abordar las actividades para el análisis y gestión del riesgo tecnológico.

A partir de lo cual se consideran los siguientes beneficios:

- Determinar los requisitos de seguridad del sistema teniendo en cuenta la proporción de sus riesgos y la naturaleza de los controles necesarios para la protección de los activos del software.
- Facilitar la rastreabilidad de la seguridad en las Fases de implementación y pruebas a través de los requisitos de seguridad.
- Integrar buenas prácticas para la gestión de la seguridad desde fases tempranas del Ciclo de Vida de desarrollo del software, concretamente con el análisis y gestión de riesgos.
- Utilizar la documentación del análisis y gestión del riesgo tecnológico en proyectos similares de la organización que provean a los equipos de proyecto una aproximación inicial en relación a amenazas potenciales y requisitos de seguridad.

En la Figura 10 se muestran las actividades que componen la guía, en lo adelante se realiza una descripción de cada una de ellas.

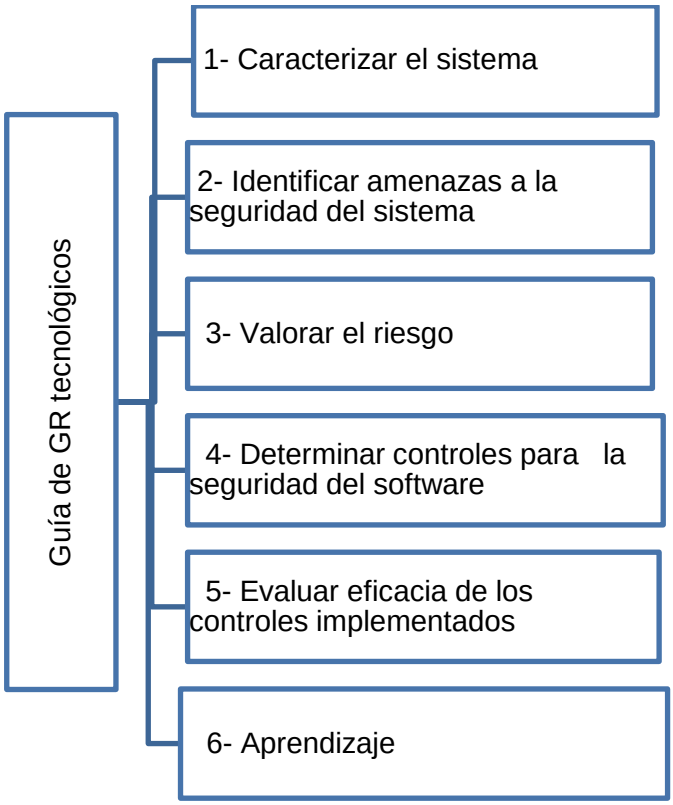


Figura 8. Guía para la gestión del riesgo tecnológico. Fuente Elaboración propia

Ajustándose al área de conocimiento de gestión de riesgos en (PMI 2013) y basado en las deficiencias detectadas en la investigación la guía para la gestión del riesgo tecnológico define actividades en los procesos identificación de los riesgos, análisis cualitativo de los riesgos, planificación de la respuesta a los riesgos y control de los riesgos. Incorpora una actividad de Aprendizaje (Microsoft 2002) debido a la poca madurez en relación a la gestión de este tipo de riesgos y el uso de herramientas y técnicas para este fin. El aprendizaje permitirá favorecer la mejora continua y la documentación de las lecciones aprendidas en los proyectos de la organización.

Tabla 6. Integración de la propuesta a los procesos del PMBOK. Fuente elaboración propia

Procesos del PMBOK	**Guía para la gestión del riesgo tecnológico**
Planificar la Gestión de Riesgos	
Identificar los Riesgos	A-1 Caracterizar el sistema A-2 Identificar amenazas a la seguridad del sistema de TI.

Realizar el Análisis Cualitativo de los Riesgos.	A-3 Valorar el riesgo.
Realizar el Cuantitativo de los Riesgos.	
Planificar la Respuesta a los Riesgos	A-4 Determinar controles de seguridad.
Controlar los Riesgos	A-5 Evaluar eficacia de los controles implementados.
	A-6 Aprendizaje

2.2.1 Descripción de las actividades

A-1 Caracterizar el sistema

La ejecución de la actividad tiene como objetivo determinar las fronteras del proceso de gestión del riesgo tecnológico en el proyecto qué es objeto de análisis. Se parte de determinar los objetivos de seguridad para el software de acuerdo con las reglas del negocio y postura de la organización que permita garantizar que las funciones para las que el software se ha concebido se ejecutan de acuerdo a sus especificaciones. Por tanto es necesario:

A-1.1 Determinar las regulaciones, estándares y políticas de seguridad de la organización con influencia en el sistema.

A-1.2 Definir postura de los interesados en la entidad cliente respecto a la seguridad del producto.

A-1.3 Determinar los activos que son valiosos y críticos para el sistema y que son necesarios asegurar.

A-1.4 Determinar los objetivos de seguridad para los activos valiosos gestionados por el sistema.

A-1.5 Comunicación a los involucrados sobre el estado del proceso.

Esta actividad proporciona información del sistema y su entorno operativo así como el dominio de interés y la definición de dependencias con otros sistemas de TI. Se requiere un profundo conocimiento del ambiente de procesamiento del sistema. El equipo debe recoger la información del sistema asociada fundamentalmente a: hardware, software, interfaces del sistema para la conectividad, misión del sistema, datos sensibles, requerimientos funcionales del sistema de TI, etc.

Salidas: Objetivos de Seguridad del Software

A-2 Identificar amenazas a la seguridad del sistema

El objetivo es determinar y documentar las amenazas que pueden causar daños al sistema, partiendo del conocimiento de los objetivos de seguridad definidos. Se deben determinar las amenazas relevantes sobre cada activo, identificando las principales fuentes de amenazas potenciales aplicables al sistema

evaluado. Para ello se pueden realizar las siguientes actividades:

A-2.1 Análisis del histórico de riesgos de la organización. Esta información es útil en la medida en que se identifiquen elementos que puedan ser usados de forma análoga para el sistema que es objeto de análisis (ataques candidatos). El histórico de los riesgos de la organización provee a los involucrados en este proceso una aproximación del impacto y probabilidad de ocurrencia de las amenazas.

A-2.2 Determinar casos de uso que gestionan activos críticos del sistema. Se debe determinar los casos de uso, que colaboran en el cumplimiento de los objetivos del sistema, que utilizan, procesan y transmiten información relativa a los activos valiosos o críticos del sistema. (Mellado 2007)

A-2.3 Determinar cómo puede ser amenazado el Caso de uso. Determinar las amenazas que pueden ocasionar fallos en el sistema de forma que se puedan afectar los principios de la Confidencialidad, Disponibilidad e Integridad de la información.

A-2.4 Clasificar amenazas. Las amenazas que enfrenta la aplicación se pueden categorizar sobre la base de los objetivos y propósitos de los ataques. Método STRIDE, acrónimo de Suplantación de identidad, Manipulación de datos, Repudio, Revelación de información, Denegación de servicio y Elevación de privilegios. (Meier 2010)

A-2.5 Desarrollar y especificar Casos de Abuso y/o Mal uso. (Alexander 2002)

A-2.6 Confeccionar Modelos de Amenazas: Tienen como objetivo representar gráficamente las amenazas que pueden conducir a un ataque a través de arboles de ataque y casos de mal uso.

A-2.7 Determinar las vulnerabilidades del sistema para las amenazas a los activos del sistema que se identificaron. (MAP 2012)

Los artefactos de salida en su conjunto forman el Modelo de amenazas que fundamenta las formas que un posible atacante puede lograr acciones mal intencionadas.

Salidas:

Listado de Amenazas categorizadas.

Modelos de Amenazas.

A-3 Valorar el riesgo

Tiene como objetivo establecer el riesgo aproximado a partir de realizar la estimación de la probabilidad de ocurrencia y el impacto potencial al que está sometido el sistema. La ejecución de la actividad ofrece una consideración sistemática del daño probable que puede causar un fallo en la seguridad, con las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

La valoración del riesgo también facilita la priorización de las amenazas de acuerdo al daño causado y la probabilidad de ocurrencia. La técnica que se empleará con este propósito es DREAD, acrónimo de los términos Daño potencial, Reproducibilidad, Explotabilidad, Usuarios afectados y Descubrimiento. Cada elemento recibirá una puntuación, tomando como referencia que Alto sería 3, Medio 2 y Bajo 1. La

estimación del riesgo aproximado se obtiene a partir de la sumatoria de las categorías divididas entre 5. (Meier 2010)

El análisis asociado a cada categoría puede estar enfocado de la siguiente forma:

¿Cuál es el daño que puede originar la vulnerabilidad si llega a ser explotada?

¿Es fácil reproducir las condiciones que propicien el ataque?

¿Es sencillo llevar a cabo el ataque?

¿Cuántos usuarios se verían afectados?

¿Es fácil encontrar la vulnerabilidad?

La respuesta a las amenazas se puede dar basándose principalmente en el riesgo asociado a cada una. Una amenaza puede ser eliminada (implica eliminar la funcionalidad del sistema donde se presenta la misma) cuando la funcionalidad es opcional o cuando el riesgo asociado es tan alto que no se puede asumir. Frente a una amenaza puede decidirse no hacer nada y aceptar el riesgo, cuando el impacto es bajo o si la mitigación fuese demasiado costosa comparada con el riesgo asociado. Por último, puede transferir el riesgo a una tercera parte, por ejemplo al usuario u otra aplicación que interactúe con la nuestra.

Salidas:

Reporte de Valoración del riesgo asociado a cada amenaza.

A-4 Determinar controles de seguridad del software

El equipo de desarrollo debe decidir que respuesta tendrá cada amenaza, qué defensas serán implementadas en el código fuente de la aplicación y cómo la arquitectura garantizará la protección de los activos gestionados por el sistema, quiénes son los responsables de mitigar cada una de ellas.

La ejecución de la actividad incluye identificar las técnicas y tecnologías necesarias para mitigar los riesgos identificados. Las técnicas y tecnologías deben adecuarse a la manera en que se decidirá responder a cada una de las amenazas, teniendo en cuenta los objetivos de seguridad y el cumplimiento de las especificaciones funcionales y no funcionales del software.
Estos elementos deben traducirse a requisitos de seguridad de modo que se complete la Especificación de los requisitos del software y el diseño, la implementación y las pruebas sustenten las decisiones tomadas en este proceso.

A-4.1 Especificar requisitos

Tiene como objetivo derivar los requisitos funcionales y no funcionales de seguridad a partir de los objetivos de seguridad y los controles de seguridad o salvaguardas acordadas, para mitigar o minimizar el impacto de las amenazas hacia los activos críticos o valiosos del sistema (Mellado 2007). Para ello se deben realizar las siguientes actividades:

A-4.1.2 Análisis de los Casos de mal uso, arboles de ataque y lo que suponen estas amenazas.

A-4.1.3 Mapear objetivos de seguridad a requisitos funcionales de seguridad.

A-4.1.4 Transformar objetivos de seguridad en restricciones de los requisitos funcionales (requisitos no funcionales de seguridad).

A-4.1.5 Especificar requisitos funcionales de seguridad.

A-4.1.6 Actualizar el documento de especificación de requisitos del software, en este caso los requisitos funcionales que tengan influencia en la seguridad del software.

A-4.1.7 Descripción de los Casos de Uso de seguridad.

En organizaciones con cierta experiencia en la gestión del riesgo tecnológico se consideran buenas prácticas apoyar esta actividad con un repositorio de amenazas de seguridad reutilizables asociado a requisitos de seguridad representados, con casos de uso indebido y casos de uso de seguridad así como definir los requisitos de seguridad para las amenazas preferiblemente con la ayuda de una taxonomía de requisitos de seguridad.

Salidas:

Especificación de requisitos (actualizado)

Descripción de Casos de Uso seguros.

A- 5 Evaluar eficacia de los controles implementados

La actividad tiene como objetivo la realización de una Auditoría de seguridad que permita evaluar la eficacia de los controles implementados. La técnica de análisis estático del código y la realización de pruebas de seguridad orientadas al riesgo deben ser utilizadas para este propósito.

Esta actividad requiere:

A-5.1 Planificar si son necesarias las actividades de capacitación del equipo relacionadas con programación segura.

A-5.2 Análisis estático del código teniendo en cuenta las amenazas consideradas en el Modelado de Amenazas.

A-5.3 Evaluación de la eficacia de los controles implementados a través de la realización de pruebas de seguridad orientadas al riesgo.

A-5.4 Análisis de resultados así como determinación de controles en función del riesgo.

A-5.5 Actualizar el Plan de riesgos con la información asociada a la gestión del riesgo tecnológico e incluir puntos de monitoreo de estos riesgos. (Planes y registro de Monitoreo)

Salidas:

Plan de desarrollo de software (actualizado).

Planes y registro de Monitoreo (actualizado).

Informes Auditoría de seguridad

A-6 Aprendizaje

La actividad tiene como objetivo formalizar las lecciones aprendidas, los artefactos relevantes del

proyecto y las herramientas de forma que permita detectar deficiencias. (Microsoft, 2012). Se proponen las siguientes actividades:

A-6.1 Revisión de informes para formalizar lecciones aprendidas.

A-6.2 Realizar talleres de análisis de experiencias.

A-6.3 Evaluar la realización de las actividades con el objetivo de determinar errores.

A-6.4 Analizar tendencias en proyectos de la organización relacionadas con la gestión del riesgo tecnológico.

A-6.5 Mejorar la gestión del riesgo tecnológico a partir del análisis de resultados.

A-6.6 Documentar lecciones aprendidas.

Salidas:

Relatoría del taller de análisis de experiencias.

Listado de insuficiencias, buenas prácticas y oportunidades de mejora.

2.2.2 Herramientas y técnicas aplicables en la guía propuesta

Reuniones de planificación y análisis: Se realiza con el objetivo de determinar el alcance que tendrá la gestión del riesgo tecnológico para el proyecto. Estableciendo las regulaciones, políticas y/o normas con significación en la seguridad del software. Además el histórico de riesgos de la organización a los efectos de ser utilizados en los análisis requeridos en las actividades de identificación de amenazas y valoración del riesgo. (PMI 2013)

Tormenta de Ideas (Brainstorming): La tormenta de ideas facilita identificar posibles escenarios de riesgos, en un proyecto particular con la participación de los roles involucrados y expertos en el dominio del desarrollo del sistema. Puede realizarse partiendo del análisis del histórico de riesgos de la organización y la experiencia de proyectos anteriores. (Hurtado 2010)

Método basado en analogías: Se emplea en el proceso de identificar las amenazas a la seguridad del sistema teniendo como base referencias para poder generar un listado de amenazas. Prestando atención a que los antecedentes y experiencia deben estar ajustados a las condiciones o el escenario actual del sistema que se analiza. (Hurtado 2010)

Revisiones de documentación: Se realiza las revisiones de la especificación de requisitos del software, descripciones de casos de uso o historias de usuario, diagramas de actividades, diagrama de procesos de la organización, políticas de seguridad y cualquier documentación que permita conocer la misión del software, el ambiente de procesamiento del sistema, dependencias, componentes, etc. (PMI 2013)

Diagramas de flujo de datos: Se emplean para la representación gráfica con el objetivo de descomponer el sistema en partes y demostrar que cada una de las partes no sea susceptible a amenazas pertinentes. Los diagramas de flujo de datos usan un conjunto estándar de símbolos que consta de cuatro elementos: flujos de datos, almacenes de datos, procesos e interactivos y, para el modelado de amenazas, se incluyen los límites de seguridad. (Microsoft 2006)

Casos de Mal uso/uso indebido: los casos de mal uso son utilizados para identificar potenciales amenazas, a partir de las cuales es posible elicitar requisitos de seguridad o casos de uso de seguridad. La interacción del usuario autorizado con el sistema es diagramada simultáneamente con las interacciones del usuario hostil. (Alexander 2002) Figura 11

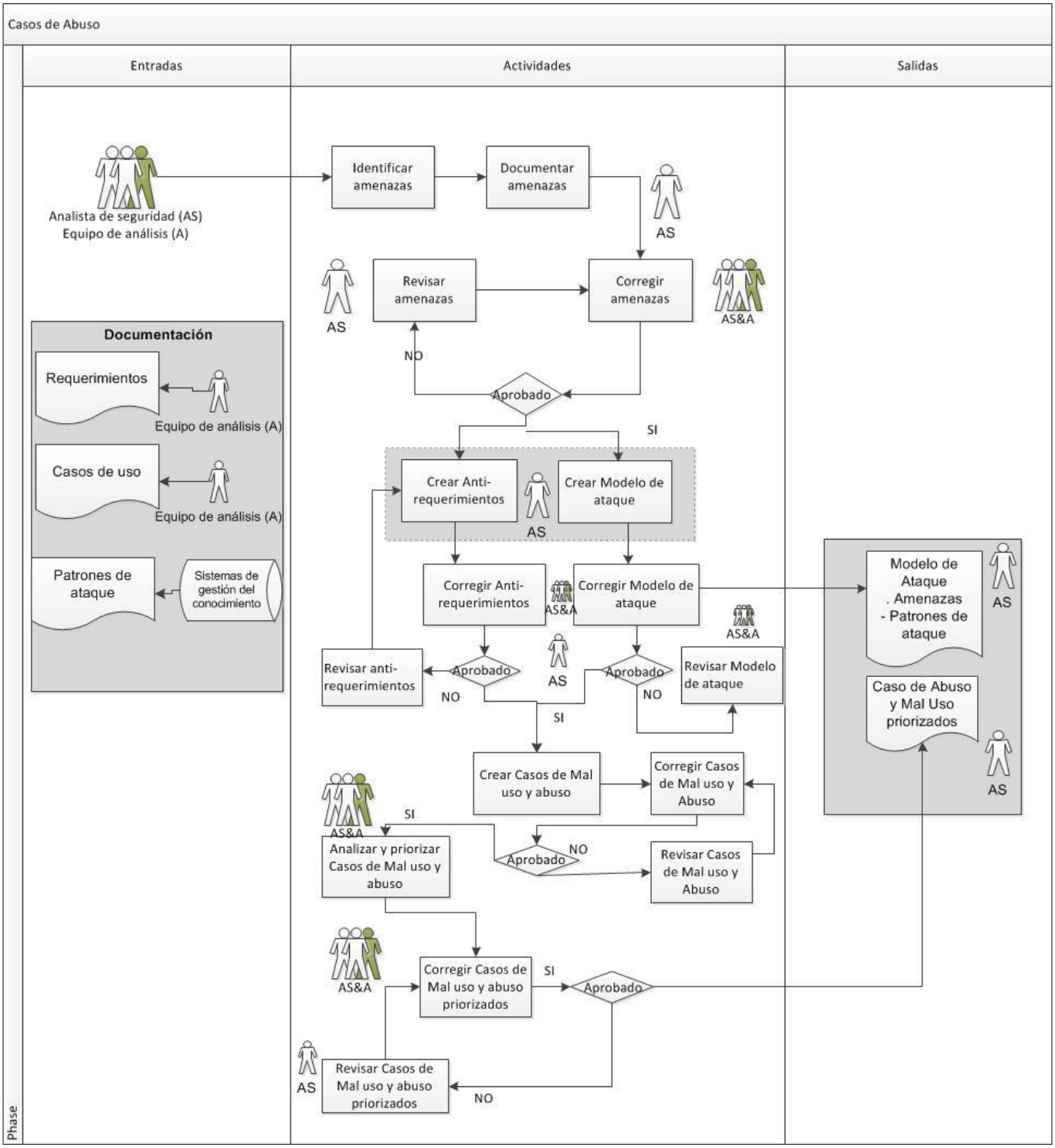


Figura 9. Diagrama de procesos para construir Casos de Abuso. Elaborado a partir de (McGraw 2006)

Patrones de ataque: Los patrones de ataques son la manifestación de una amenaza o varias en el contexto de una tecnología concreta. Son los elementos concretos que permiten al atacante hacer realidad una amenaza. En este sentido se proponen familiarizarse con los ataques que afectan a la tecnología con que se desarrolla el software y construir las defensas apropiadas. (Microsoft 2006)

Método STRIDE: Se propone su uso para categorizar las amenazas que enfrenta la aplicación sobre la base de los objetivos y propósitos de los ataques. STRIDE es el acrónimo de Suplantación de identidad, Manipulación de datos, Repudio, Revelación de información, Denegación de servicio y Elevación de privilegios. (Meier 2010)

Método DREAD: Tiene como objetivo establecer el riesgo aproximado a partir de realizar la estimación de la probabilidad de ocurrencia y el impacto potencial al que está sometido el sistema. Intenta conseguir el consenso en esta tarea a través de la definición de 5 categorías Daño potencial, Reproducibilidad, Explotabilidad, Usuarios afectados y Descubrimiento. La estimación del riesgo aproximado se obtiene a partir de la sumatoria de las categorías divididas entre 5. (Meier 2010)

Segursoft: es una herramienta utilizada para soportar el volumen de información y generación de artefactos producidos de la aplicación de la guía para la gestión del riesgo tecnológico. Soporta la ejecución de las actividades definidas y la elaboración de reportes con información asociada a los proyectos analizados.

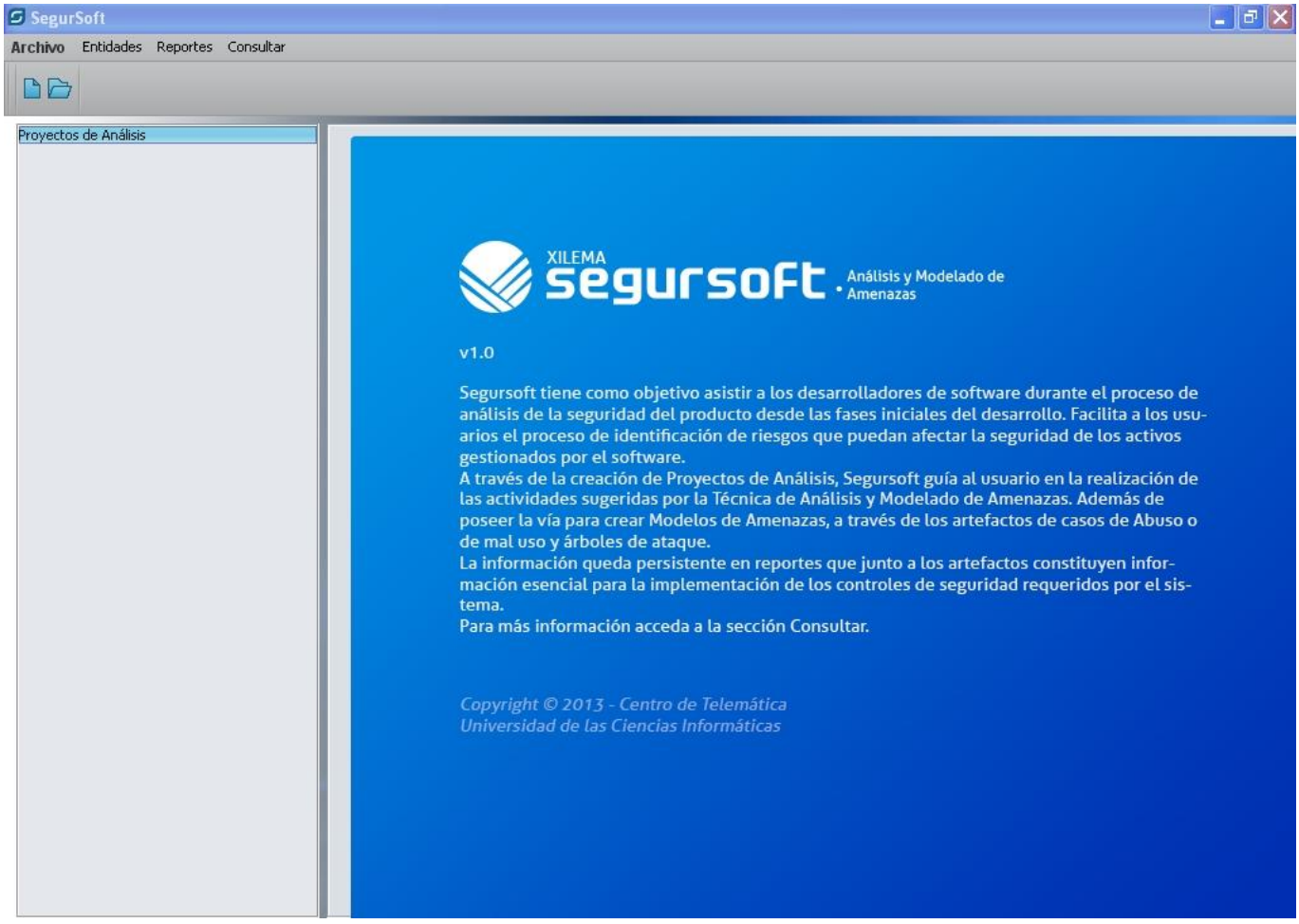


Figura 10. Segursoft

Lista de chequeo: El uso de listas de chequeo es útil para abordar la inspección de requisitos de forma que satisfacen los objetivos de seguridad planteados para el software y son verificables por pruebas, demostración, revisión o análisis. Además se propone emplear para la evaluación de seguridad a fin de comprobar el cumplimiento de los objetivos de seguridad y obtener una medida del riesgo probable. (PMI 2013)

Plantillas: Se incluyen plantillas para la documentación del análisis realizado durante la gestión del riesgo tecnológico así como la estandarización de los artefactos con extensiones para la seguridad (plantillas de descripción de casos de uso seguros, de requisitos de seguridad y de casos de mal uso).(PMI 2013)

Auditorías del riesgo: Se realizan con el objetivo de evaluar la eficacia de los requisitos que se determinaron para hacer frente al riesgo tecnológico. Se desarrolla a través de análisis estático del código y pruebas de seguridad. (PMI 2013)

Plan de gestión del proyecto: Dado que tiene como objetivo proporcionar una orientación sobre el desarrollo y la planificación de las actividades del cronograma a través de los planes suplementarios a él. Se debe actualizar a fin de incluir los requisitos en las iteraciones del desarrollo y las actividades de verificación de la seguridad. (PMI 2013)

2.2.3 Descripción gráfica de la guía para la gestión del riesgo tecnológico

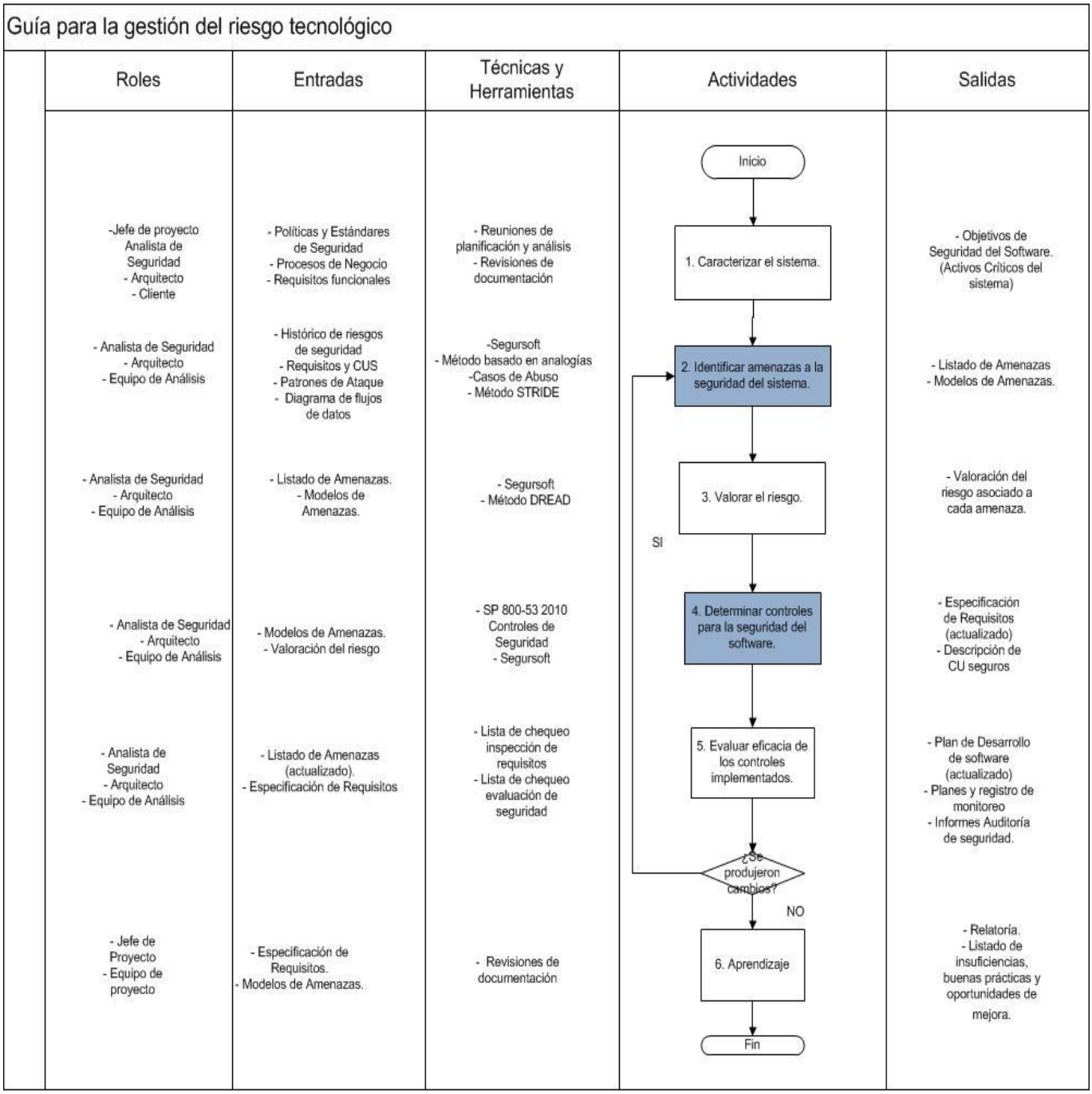


Figura 11. Actividades de la Guía para la gestión del riesgo tecnológico. Fuente Elaboración propia

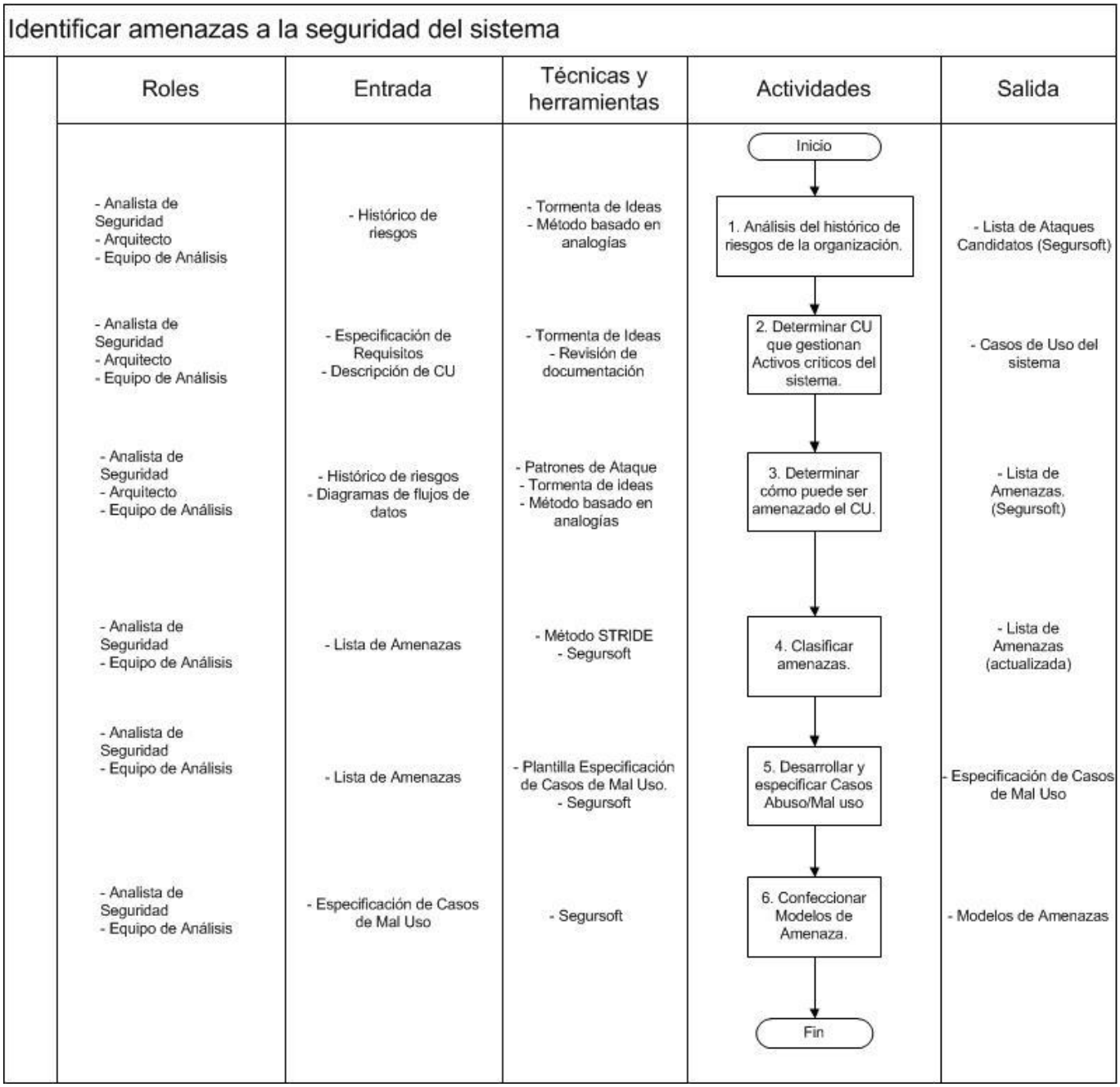


Figura 12. Actividades necesarias para identificar y documentar amenazas. Fuente Elaboración propia

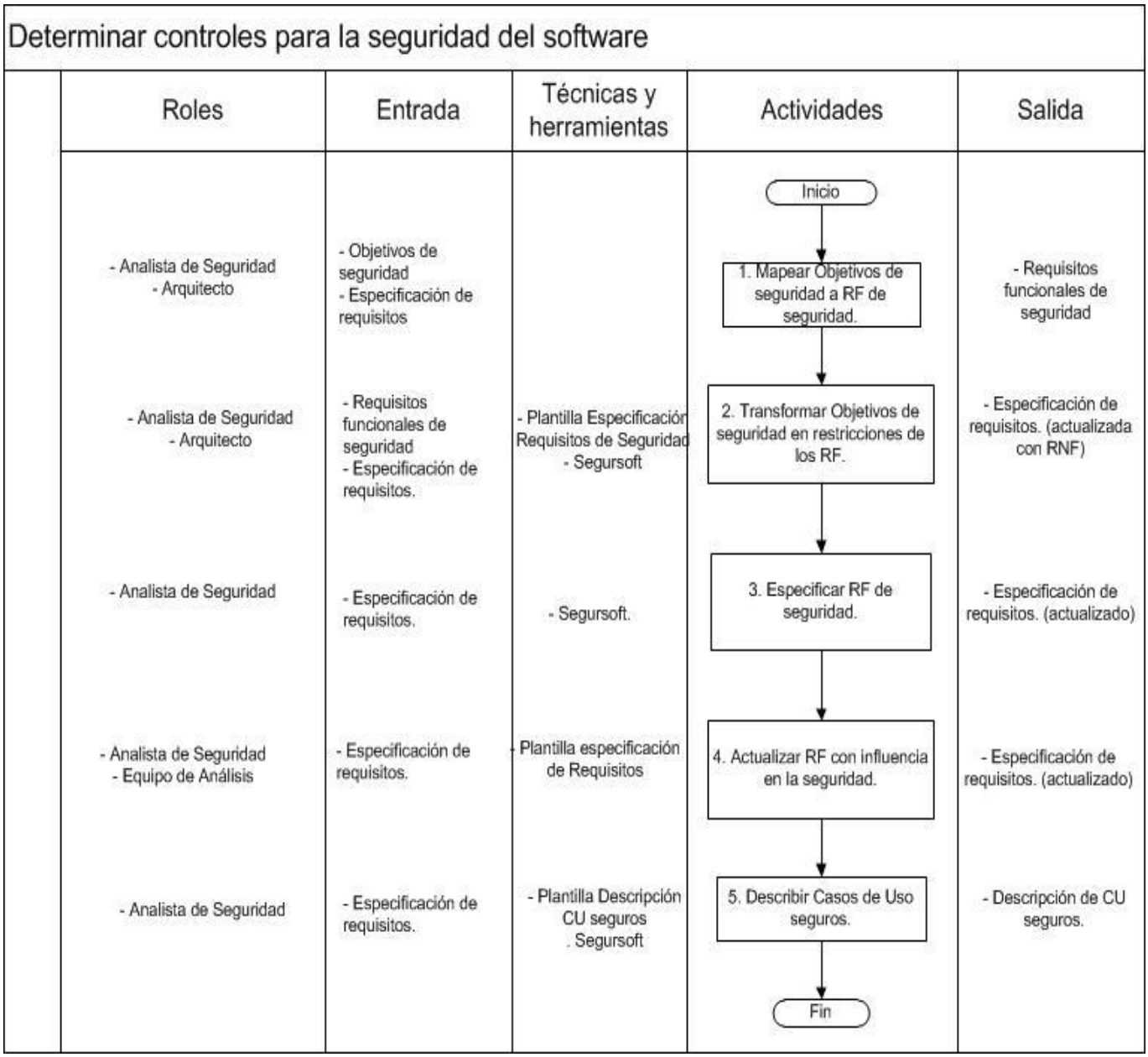


Figura 13. Actividades necesarias para determinar controles para la seguridad del software. Fuente Elaboración propia

2.2.4 Roles

Se muestran las responsabilidades definidas para cada rol con incidencia en las actividades propuestas en la guía.

Tabla 7. Roles y responsabilidades. Fuente Elaboración propia

Roles	Responsabilidades

Analista de Seguridad	- Identifica objetivos y visión de la seguridad. - Identifica amenazas a la seguridad del producto. - Establece Lista de patrones de ataques. - Desarrolla Modelos de amenazas. - Describe Casos de abuso y/o Mal uso. - Conduce las actividades de valoración del riesgo. - Desarrolla los artefactos resultantes de la aplicación de la guía. - Actualiza los modelos y artefactos producto de los cambios.
Equipo de análisis	- Realiza el diagnóstico de la organización o área del proyecto. - Realiza el levantamiento de los procesos y reglas del negocio con énfasis en la seguridad. - Realiza actividades de análisis, elicitación y especificación de requisitos. - Participa en las actividades de identificación de amenazas, desarrollo de casos de abuso y valoración del riesgo. - Mantiene la rastreabilidad de los requisitos con el resto de los productos de trabajo. - Informa de los cambios en los requisitos.
Arquitecto	- Identifica Objetivos de seguridad - Establece Lista de patrones de ataques. - Identifica amenazas a la seguridad del producto. - Determina controles de seguridad para mitigar las amenazas. - Conduce la implementación de los controles de seguridad en el diseño y arquitectura del software. - Analiza los cambios que afecten o introduzcan amenazas a la seguridad del software.
Cliente	- Establece la política de seguridad para el sistema.

	- Informa sobre estándares, normas y procedimientos de seguridad aplicables al sistema. - Define activos valiosos y críticos gestionados por el sistema. - Participa en las actividades de valoración del riesgo. - Acepta los requisitos de seguridad.
Jefe de Proyecto	- Define la organización del proyecto. - Administra, desarrolla y coordina los recursos para abordar las actividades de gestión del riesgo tecnológico. - Participa en las actividades de valoración del riesgo. - Mantiene el histórico de riesgos de seguridad. - Aprueba los requisitos de seguridad del software. - Actualiza los planes del proyecto. - Dirige, coordina y aprueba las actividades de gestión de cambios del proyecto. - Gestiona las entrevistas entre clientes y equipo de desarrollo. - Coordina la capacitación de los involucrados en cuanto a la seguridad del software.
Administrador de la Calidad	- Realiza inspección de requisitos. - Identifica oportunidades de mejora. - Realiza el diseño de escenario de pruebas para ayudar a la inspección de los requisitos. - Verifica y valida las propiedades de seguridad del software.

2.2.5 Integración al Proceso de desarrollo del software

Se articulan las actividades de la propuesta en las fases que componen el modelo de ciclo de vida de los proyectos de desarrollo de software definido en la Universidad de Ciencias Informáticas. (UCI 2012) Se relacionan a continuación las actividades involucradas en cada caso.

Tabla 8. Integración de las actividades de la Guía en las fases del proceso de desarrollo de software. Fuente elaboración propia

Fase	Actividades	Hito
Inicio	A-1 Caracterizar el sistema A-2 Identificar amenazas a la seguridad del sistema de TI. A-3 Valorar el riesgo.	Establecimiento de los objetivos de seguridad y valoración del riesgo por cada amenaza asociada a los activos críticos del sistema.
Desarrollo	A-4 Determinar controles de seguridad. A-5 Evaluar eficacia de los controles implementados.	Refinar la valoración de riesgos y la definición de los objetivos de seguridad. Diseñar la arquitectura en la que se insertan los requisitos de seguridad en relación al riesgo. Implementación del sistema contra sus requisitos y objetivos de seguridad determinados. Evaluación de la eficacia de los controles implementados a través de la realización de pruebas de seguridad orientadas al riesgo.
Cierre	A-6 Aprendizaje	Formalizar lecciones aprendidas que permita detectar deficiencias y mejorar el proceso.

2.3 Conclusiones del capítulo

En el presente capítulo se presentó el diseño de un guía que tiene en cuenta la concepción y desarrollo de la seguridad desde las fases iniciales del desarrollo del producto, concretamente siguiendo un enfoque de gestión de riesgos. El mismo ofrece un conjunto de actividades para el análisis, valoración y gestión del riesgo tecnológico que puede afectar la seguridad del software.

La guía propuesta sienta las bases para la implementación de buenas prácticas de seguridad en la institución, de forma que en lo adelante se puedan alcanzar metas superiores relacionadas con garantías de la seguridad del producto y la gestión de los riesgos técnicos que pueden afectar la calidad del software.

El principal aporte de la investigación es la definición de una guía para la gestión del riesgo tecnológico

que ofrece herramientas y técnicas para determinar los requisitos de seguridad del software a partir de un proceso de análisis de riesgos.

Los límites de la propuesta están determinados por la capacidad de la misma para gestionar el riesgo tecnológico mediante la implementación y validación de los requisitos de seguridad del software, de forma que le permitan cumplir con sus objetivos de seguridad.

A partir de su aplicación y conforme ocurre el aprendizaje la guía debe fortalecerse a través de la definición de elementos que permitan:

- Valorar económicamente los activos del software y en correspondencia los mecanismos que se determinen para su protección.
- Definir una taxonomía y repositorio para los requisitos de seguridad que faciliten a los involucrados hacer uso de requisitos de seguridad adaptables a realidades particulares de dominios de aplicación.

CAPÍTULO 3 APLICACIÓN DE LA GUÍA Y ANÁLISIS DE RESULTADOS

3.1 Introducción

En el presente capitulo se hace un análisis de la aplicación de la guía para la gestión del riesgo tecnológico en el Centro de Telemática. Se comienza por la aplicación del criterio de expertos como vía para valorar la guía propuesta así como un análisis de los resultados obtenidos. Se exponen los resultados de su aplicación en un proyecto del Centro TLM y se muestra el comportamiento de los indicadores definidos para la evaluación de las variables operacionales. Además se analiza la valoración económica y social de la propuesta.

3.2 Valoración de la guía para la gestión del riesgo tecnológico a través del criterio de expertos

La aplicación del método de criterio de expertos se llevó a cabo a través del cumplimiento de los pasos siguientes: a) identificación de los posibles expertos, b) selección de los expertos, c) realización de la consulta a los expertos y d) procesamiento y valoración de la información obtenida. Para identificar los posibles expertos se tuvieron en cuenta, la experiencia profesional en relación con el objeto de investigación, la participación en investigaciones relacionadas con esta temática, el dominio teórico de la temática, la preparación académica y científica, y la experiencia, de modo que estuvieran en capacidad de ofrecer valoraciones y hacer recomendaciones pertinentes, en relación con los aspectos que le serían consultados. Se identificaron 17 posibles expertos.

Selección de expertos

La selección de los expertos, se inició con la aplicación de una encuesta a los posibles expertos para determinar su coeficiente de competencia (K), el cual se obtiene de la expresión:

$$\boldsymbol{K = (kc + ka) \,/\, 2} \qquad \textbf{(1)}$$

Donde *kc* es el coeficiente de conocimiento o información y *ka* es el coeficiente de argumentación.

Esta tarea se ejecuta mediante la autovaloración de los especialistas seleccionados sobre los niveles de información y argumentación que tienen sobre el tema planteado. De los 17 especialistas valorados se seleccionaron 9 expertos cuyo coeficiente de competencia (K) resultó Alto y Medio. Los 9 expertos son graduados universitarios y una gran parte de ellos ha obtenido títulos de formación académica: 4 especialistas y 5 másteres.

Tabla 9. Expertos utilizados en la validación de la investigación. Fuente elaboración propia

	Expertos	**Entidad**
1	MSc. Rogfel Thompson Martinez	ICIMAF
2	MSc. Yadira Ruiz Constanten	Facultad 2. UCI
3	Ing. Aymara Marin Díaz	Calidad UCI

4	Ing. Lilian Sauco Altuna	Centro de Telemática. UCI
5	Ing. Pablo Yunier Medina Martínez	Dirección de Seguridad Informática. UCI
6	MSc. Alina Surós Vicente	Centro de Identificación y Seguridad Digital. UCI
7	Ing. Yoannis Costilla Camejo	Calisoft
8	MSc. Dariena Ramirez Luján	Centro de Informatización de la Gestión Documental. UCI
9	MSc. Fidel Enrique Castro Dieguez	Centro de Desarrollo. Universidad de Granma

Realización de la consulta a expertos

Después de contar con los 9 expertos seleccionados se sometió a su consideración un instrumento para la validación de la Guía para la gestión del riesgo tecnológico. El instrumento se compone de 22 sentencias así como 5 categorías evaluativas que permitan conocer la opinión de los expertos. Las categorías evaluativas empleadas fueron muy adecuado (MA), bastante adecuado (BA), adecuado (A), poco adecuado (PA) e inadecuado (I). Anexo 1.

Análisis de la concordancia de las valoraciones de los expertos

En un segundo momento se calcula el coeficiente de Kendall que permite analizar la concordancia en las valoraciones realizadas por los expertos (coeficiente de Kendall).

En este caso el coeficiente concordancia (W) será un índice de la divergencia del acuerdo efectivo entre los expertos. El coeficiente de concordancia de Kendall se obtiene de la expresión

$$\boldsymbol{W = 12S/K^2(N^3 - N)} \qquad \textbf{(2)}$$

Donde S representa el cuadrado de las desviaciones medias, K el número de expertos y N el número total de aspectos a evaluar.

El valor de W oscila entre 0 y 1. El valor de 1 significa una concordancia de acuerdos total y el valor de 0 un desacuerdo total.

Se aplica además la Prueba de Significación de Hipótesis para comprobar el grado de significación de Kendall, planteándose la hipótesis nula y la alternativa de la siguiente forma: donde H0: no existe concordancia entre los expertos y H1: existe concordancia entre los expertos.

El cálculo del Chi cuadrado real: $\boldsymbol{x^2 = \mathrm{K(N-1)W}}$ **(3)**

$\boldsymbol{x^2} = 0{,}518$

El Chi cuadrado calculado se compara con el tabulado en la tabla del percentil de la distribución Chi cuadrado. Para tener un 95% de confianza se utilizará $\boldsymbol{\alpha = 0{,}05}$.

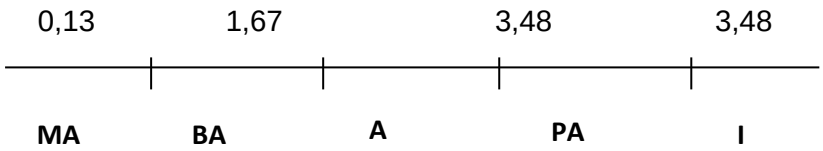
Si se cumple que $x^2real < x^2(\propto, \mathbf{N}-\mathbf{1})$, entonces se infiere que existe concordancia de criterios entre los expertos al considerar válida la hipótesis alternativa H1. Como 0,518 < 33,924 existe concordancia entre los expertos.

Procesamiento estadístico

Los criterios vertidos por los expertos se someten a una prueba estadística no paramétrica que permite concluir qué valoración final tiene cada uno de los aspectos a evaluar.

Para los datos anteriores se debe confeccionar una distribución de frecuencia a partir de los datos primarios para cada uno de los aspectos sometidos a consulta.

Se determina sobre la base de la tabla anterior, la distribución de frecuencia acumulativa de cada fila. Y por último los puntos de corte para conocer la categoría de cada criterio según los expertos consultados. Los intervalos obtenidos para cada categoría de evaluación a partir de los puntos de corte son.



Luego se realiza la comparación con los puntos de corte y se concluye cuál fue la valoración que obtuvo cada aspecto según criterio de los expertos. De acuerdo con esto el 95% de los aspectos analizados fueron valorados de Muy Adecuado (MA), lo que demuestra la pertinencia que los expertos aprecian en la propuesta realizada permitiendo aseverar que su aplicación contribuirá a la gestión del riesgo tecnológico con el propósito de garantizar el cumplimiento de los objetivos de seguridad del software.

Los resultados obtenidos de la validación pueden observarse en la figura 14, que se muestra a continuación.

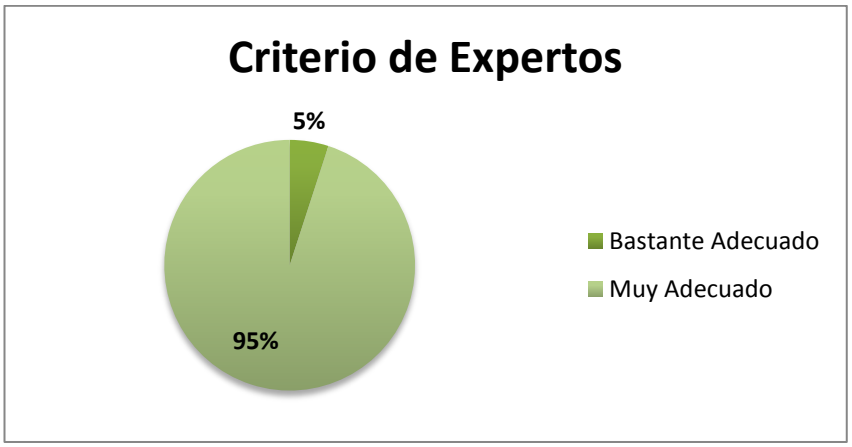


Figura 14. Comportamiento de la valoración de los expertos según las categorías evaluativas. Fuente Elaboración propia

3.2.1 Valoración de los expertos de acuerdo a los indicadores definidos en la investigación.

La Calidad de la guía para la gestión del riesgo tecnológico en los proyectos de desarrollo de la institución (Variable Independiente) se evalúo a través de los siguientes indicadores, a continuación se muestran su comportamiento en cada caso.

Tabla 10. Sub-dimensiones e indicadores para evaluar la Calidad de la guía propuesta. Fuente Elaboración propia.

Integración al proceso de desarrollo de software

- Indicador 1.1: nivel de definición de actividades para la gestión del riego tecnológico en las Fases de Inicio, Desarrollo, Cierre.
- Indicador 1.2: nivel de participación de los roles en la guía de gestión del riesgo tecnológico.
- Indicador 1.3: nivel de coherencia de las responsabilidades definidas para los roles con las actividades de la guía de gestión del riesgo tecnológico.

Comprensión de la guía

- Indicador 2.1: recursos de soporte para comprender las actividades.
- Indicador 2.2: capacidad de la descripción textual y gráfica de la guía para su comprensión.
- Indicador 2.3: nivel de indicación a los referentes teóricos relacionados por cada actividad.

Aplicabilidad de la guía

- Indicador 3.1: nivel de utilización de técnicas para la ejecución de las actividades.
- Indicador 3.2: nivel de influencia de la guía en la seguridad del software.
- Indicador 3.3: pertinencia de la guía para la gestión del riesgo tecnológico.

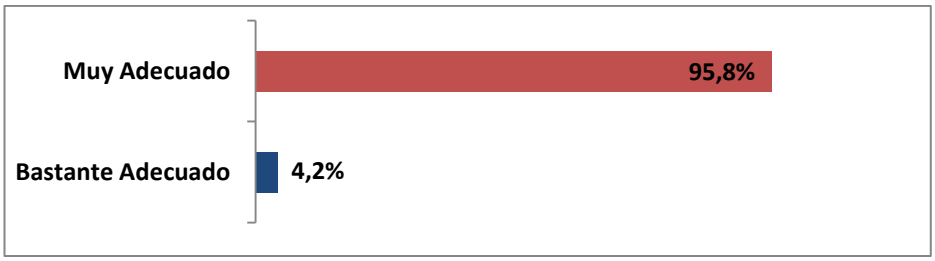


Figura 15. Comportamiento de la valoración de los expertos Sub-dimensión Integración al proceso de desarrollo de software. Fuente Elaboración propia

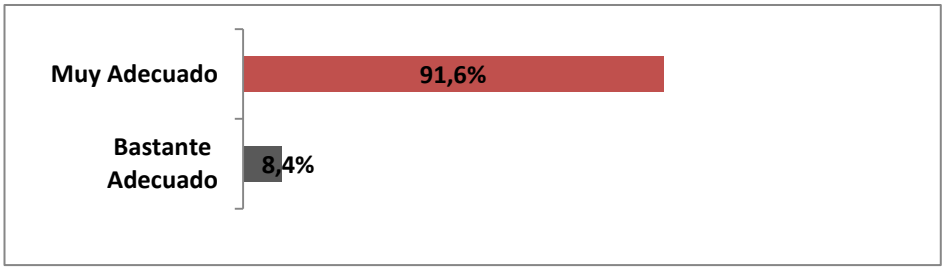


Figura 16. Comportamiento de la valoración de los expertos Sub-dimensión Comprensión de la guía. Fuente Elaboración propia

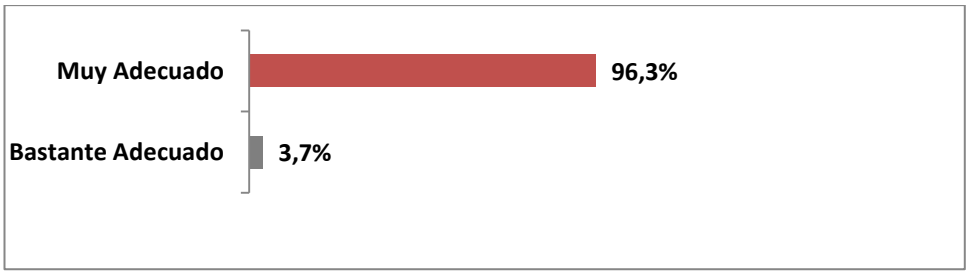


Figura 17. Comportamiento de la valoración de los expertos Sub-dimensión Aplicabilidad de la guía. Fuente Elaboración propia

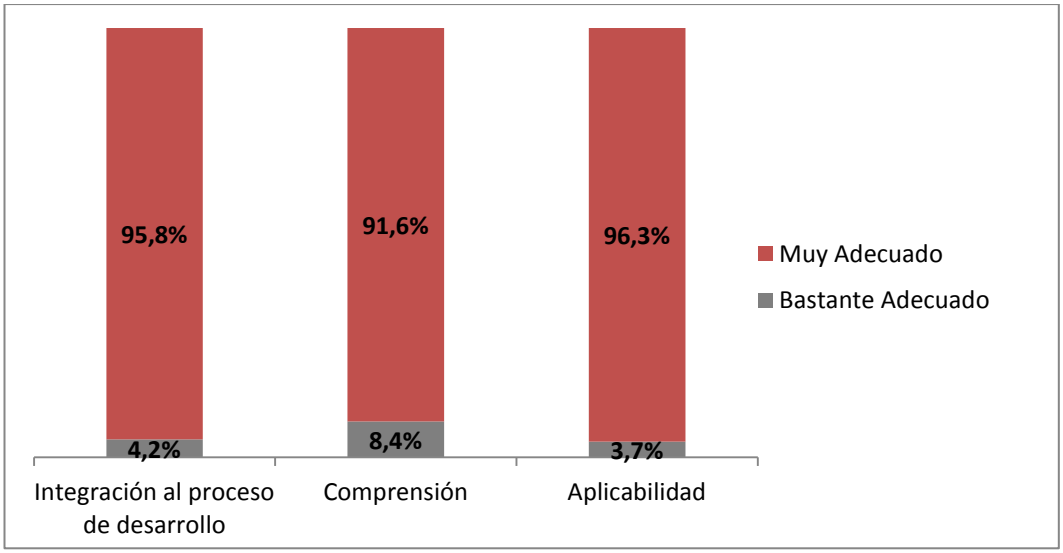


Figura 18. Resumen del comportamiento de los indicadores para evaluar la Calidad de la guía de gestión del riesgo tecnológico. Fuente Elaboración propia

Valoración de los indicadores que permiten evaluar la variable dependiente

Para la evaluación de la variable dependiente que está determinada por la influencia de la guía en el cumplimiento de los objetivos de seguridad del software se analizaron en las dos dimensiones.

Dimensión Correspondencia en las especificaciones funcionales del software, la cual se evaluará a través de los indicadores establecimiento de los objetivos de seguridad, desarrollo de casos de uso seguros, evidencias de los requisitos de seguridad en la arquitectura del software, implementación de los CU seguros y escenarios de pruebas orientados al riesgo. Utilizando en cada caso la unidad de medida definida en la tabla 1 Operacionalización de las variables.

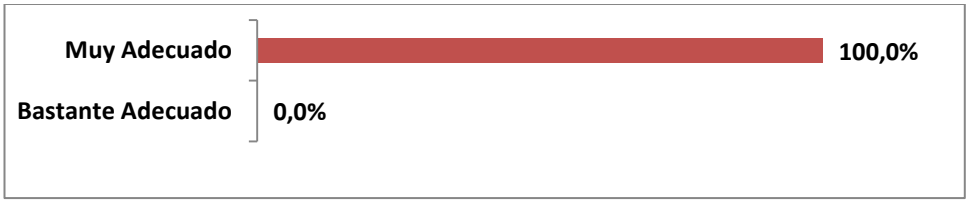


Figura 19. Comportamiento de la valoración de los expertos Dimensión Correspondencia en las especificaciones funcionales del software. Fuente Elaboración propia

Para la dimensión Evaluación de seguridad se definen los indicadores cantidad de vulnerabilidades con afectaciones en la confidencialidad, cantidad de vulnerabilidades con afectaciones en la de integridad y cantidad de vulnerabilidad con afectaciones en la disponibilidad.

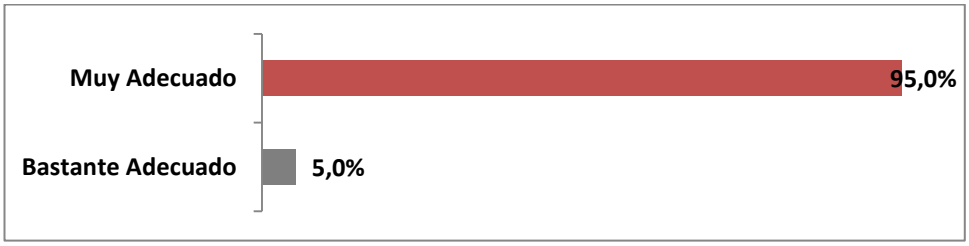


Figura 20. Comportamiento de la valoración de los expertos Dimensión Evaluación de seguridad. Fuente Elaboración propia

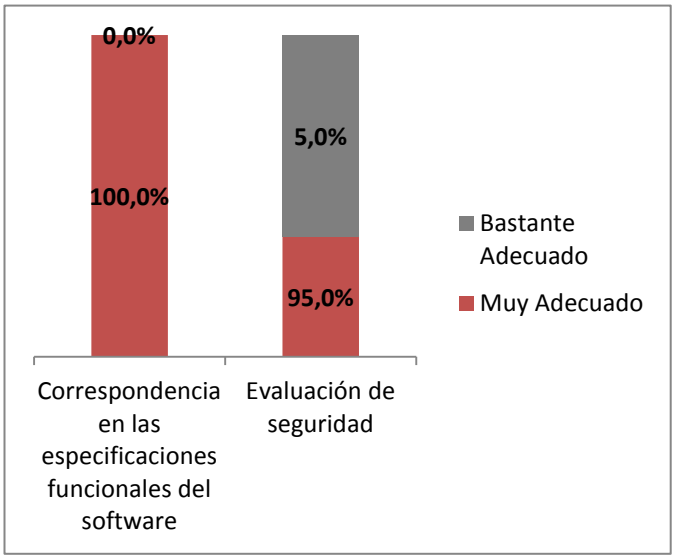


Figura 21. Resumen del comportamiento de los indicadores para evaluar la Variable dependiente. Fuente Elaboración propia

3.3 Síntesis de la aplicación de la guía para la gestión del riesgo tecnológico

La guía diseñada para la gestión del riesgo tecnológico, se aplicó en el Centro de Telemática de la Facultad 2. Para la selección de la muestra se tuvieron en cuenta los proyectos del Centro en la Fase de Inicio del desarrollo puesto que tenía las condiciones ideales para la aplicación de la investigación y consecuentemente obtener los resultados de la aplicación en fases posteriores. De acuerdo a lo cual se aplicó la propuesta en el proyecto Gestión de recursos hardware y software (GRHS).

El equipo del proyecto tiene como objetivo desarrollar una aplicación de software (agente) que se encargue de obtener información de las estaciones de trabajo en términos del hardware y el software instalado, y que sea capaz de detectar cualquier cambio en la configuración de los equipos, así como de ejecutar acciones ante estos cambios. Además de desarrollar una aplicación web para gestionar la información guardada en la base de datos por la aplicación servidor, la generación de reportes y la configuración de políticas en el sistema, alarmas, entre otras.

Antes de la aplicación de la guía se realizó de forma previa la capacitación de los Especialistas funcionales de los proyectos GRHS, puesto que fue una de las recomendaciones realizadas por los expertos.

Artefactos de la aplicación de la guía

Figura 22. Activos del sistema GRHS. Fuente Segursoft

Para los objetivos de seguridad siguientes:

- OS1: Prevenir la revelación no autorizada de información (Confidencialidad).
- OS2: Prevenir la alteración no autorizada de información (Integridad).
- OS3: Asegurar la disponibilidad de la información a los usuarios autorizados. (Disponibilidad)
- OS4: Asegurar la autenticidad de los usuarios. (Autenticidad)
- OS5: Asegurar la trazabilidad. (No Repudio)

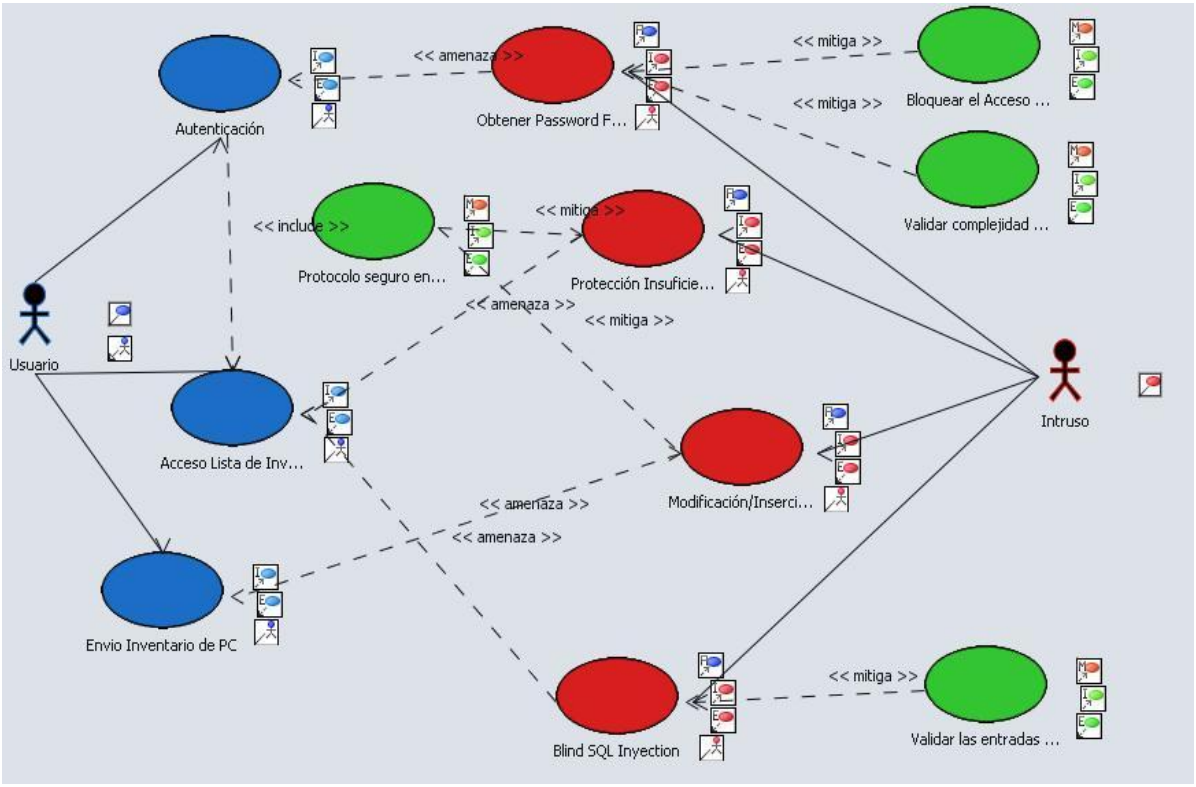


Figura 23. Modelos de Amenaza empleando Casos de Abuso. Fuente Segursoft.

3.3.1 Análisis de resultados

La aplicación práctica de la guía evidenció la necesidad refinar algunos elementos asociados a la especificación de Casos de abuso y/o Mal Uso así como incluir plantillas genéricas que faciliten el completamiento de la información asociada a los artefactos que se generan como la Descripción de Casos de uso seguros. Los especialistas también refieren la importancia de un conocimiento avanzado en relación a la temática de la presente investigación.

Para contribuir al análisis de los resultados de la aplicación de la propuesta se aplicó un instrumento a los especialistas de los proyectos GRHS que permitiera conocer la Calidad de la propuesta de la investigación y la valoración de las variables operacionales a través de cada uno de los indicadores que se definieron. Tabla 1. Se solicitó la valoración en la escala de Alto, Medio, Bajo y Nulo, los cuales se asignarían a partir de la unidad de medida establecida en la operacionalización de las variables.

La fiabilidad del cuestionario aplicado se determinó a través del Método Alfa de Cronbach, obteniéndose resultados satisfactorios que garantizan la fiabilidad de la escala.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,714	,714	24

La calidad de la propuesta fue evaluada a través de los indicadores definidos para cada dimensión, los especialistas que participaron en la validación se muestran en el Anexo 2.

Tabla 11. Resultados de la aplicación del instrumento. Fuente Elaboración Propia

Dimensión	Sub-dimensión	Indicadores	Puntuación Indicador	% con respecto al total
Calidad de la guía	Integración al proceso de desarrollo	Indicador 1.1	120	88,89
		Indicador 1.2	122	90,37
		Indicador 1.3	129	95,56
	Comprensión de la guía	Indicador 2.1	126	93,33
		Indicador 2.2	120	88,89
		Indicador 2.3	117	86,67
	Aplicabilidad de la guía	Indicador 3.1	126	93,33
		Indicador 3.2	129	95,56
		Indicador 3.3	121	89,63

A continuación se muestra el resultado de los indicadores tomados en cuenta para evaluar la calidad de la propuesta. El valor más bajo que se obtuvo en el indicador de comprensión, debido al plazo relativamente corto para la asimilación de las técnicas y herramientas que se proponen y las necesidades de especialización asociadas con amenazas, ataques y riesgos con afectaciones en la seguridad del software. La Figura 24 muestra los valores obtenidos por los atributos que evalúan la calidad de la guía para la gestión del riesgo tecnológico y el total que podían alcanzar los indicadores por cada dimensión.

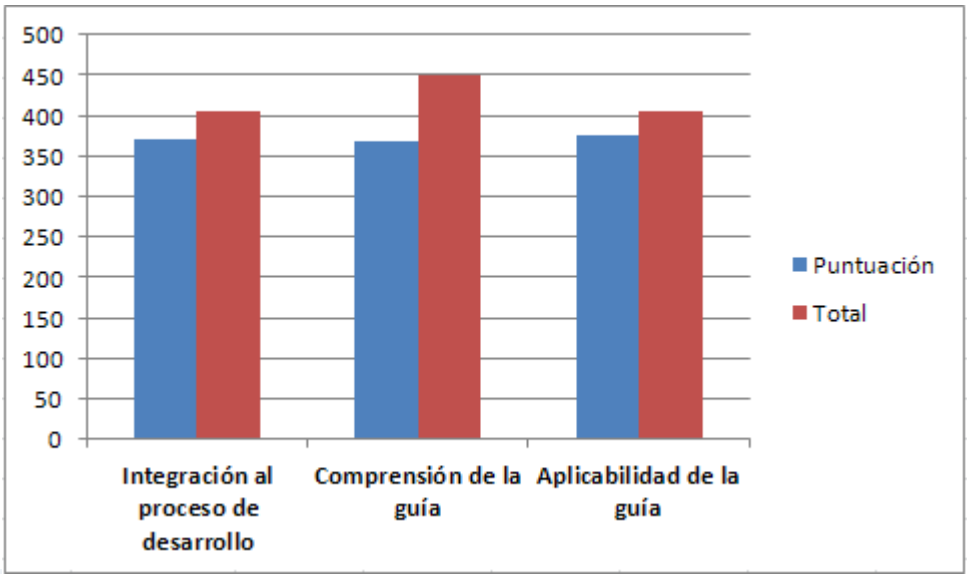


Figura 24. Comportamiento de los indicadores de calidad con respecto al total. Fuente Elaboración propia

Un análisis descriptivo de los atributos mostrados en la Tabla 12 permite conocer la desviación estándar según las dimensiones anteriores, lo cual puede traducirse en que los valores obtenidos demuestran un bajo índice de dispersión en la opinión de los encuestados.

Tabla 12. Desviación estándar de acuerdo a las dimensiones definidas. SPSS

	Minimum	Maximum	Variance	Std Deviation
Integración al proceso de desarrollo	13	14	0	1
Comprensión de la guía	12	14	1	1
Aplicabilidad de la guía	9	10	0	1

En general los resultados fueron buenos, en las tres dimensiones se obtuvieron puntuaciones altas con respecto a su total. Los niveles de consenso fueron altos en casi todos los casos.

Cumplimiento de los objetivos de seguridad del software

Para el análisis de la variable dependiente se determinaron las dimensiones correspondencia en la especificación de requisitos del software y evaluación de seguridad.

La primera dimensión se evalúo a partir de los indicadores establecimiento de los objetivos de seguridad, desarrollo de casos de uso seguros, evidencias de los requisitos de seguridad en la arquitectura del software, implementación de los CU seguros, escenarios y casos de prueba orientados al riesgo.

La dimensión evaluación de seguridad se analizó a partir de los indicadores cantidad de vulnerabilidades con afectaciones en la Confidencialidad, cantidad de vulnerabilidades con afectaciones en la Integridad, cantidad de vulnerabilidades con afectaciones en la Disponibilidad.

Antes de realizar la observación que permita evaluar la variable dependiente se realiza un análisis en cuanto a equivalencia de los grupos conformados para el Cuasiexperimento, de forma que los resultados obtenidos arrojen elementos significativos sobre el efecto del tratamiento experimental en la

variable dependiente. Tabla 13.

Tabla 13. Equivalencia entre el grupo Experimental y de Control. Fuente Elaboración propia

Indicadores	Experimental	Control
Proceso de desarrollo	Administrado, según institucionalización de las AP de CMMI nivel 2.	Administrado, según institucionalización de las AP de CMMI nivel 2.
Tipo de arquitectura.	Cliente-Servidor	Cliente-Servidor
Necesidades de seguridad	Información de activos de software y hardware de una red, la alteración de la información o no disponibilidad del sistema para su control puede dar margen a actos de robo y/o incumplimientos de políticas de seguridad.	Información limitada, relacionada con evaluaciones de software y servidores en cuanto a amenazas de seguridad.
Conocimientos avanzados del equipo de proyecto que permita adoptar un enfoque proactivo de seguridad en cuanto a (amenazas, vulnerabilidades, patrones de ataques)	No, los conocimientos del equipo se enfocan a las tecnologías empleadas en el desarrollo y las capacidades con las que cuentan las mismas para la seguridad del producto.	No, los conocimientos del equipo se enfocan a las tecnologías empleadas en el desarrollo y las capacidades con las que cuentan las mismas para la seguridad del producto.

El comportamiento de los grupos según las variables que se determinaron para el análisis de equivalencia, permitió determinar la correspondencia entre el grupo experimental y de control para la postprueba.

La observación para evaluar la variable dependiente se condujo a través de la realización de una Auditoría de seguridad en ambos grupos experimental y de control. La revisión de los artefactos y la evaluación de seguridad fueron realizadas por especialistas de seguridad del Centro de Telemática con el objetivo de verificar el cumplimiento de los objetivos de seguridad del sistema. Esta tarea incluyó la revisión del código fuente mediante la técnica de análisis estático y un análisis dinámico mediante la realización de pruebas de seguridad. El análisis dinámico realizado tuvo lugar tomando como aproximación la Lista de Chequeo propuesta por el proyecto de seguridad, por sus siglas en inglés, OWASP-Open Web Application Security Project. Figura 25.

Test Name	Ref. Number	Status	Risk
Spiders, Robots and Crawlers	*IG-001*	Not Done	
Search Engine Discovery/Reconnaissance	*IG-002*	Done	L
Identify application entry points	*IG-003*	Done	H
Testing for Web Application Fingerprint	*IG-004*	Done	M
Application Discovery	*IG-005*	Done	H
Analysis of Error Codes	*IG-006*	Not Done	
SSL/TLS Testing (SSL Version, Algorithms, Key length, Digital Cert. Validity) - SSL Weakness	*CM-001*	Done	H
DB Listener Testing - DB Listener weak	*CM-002*	Not Done	
Infrastructure Configuration Management Testing - Infrastructure Configuration management weakness	*CM-003*	Done	H
Application Configuration Management Testing - Application Configuration management weakness	*CM-004*	Not Done	
Testing for File Extensions Handling - File extensions handling	*CM-005*	Not Done	
Old, backup and unreferenced files - Old, backup and unreferenced files	*CM-006*	Done	M
Infrastructure and Application Admin Interfaces - Access to Admin interfaces	*CM-007*	Not Done	
Testing for HTTP Methods and XST - HTTP Methods enabled, XST permitted, HTTP Verb	*CM-008*	Done	
Credentials transport over an encrypted channel - Credentials transport over an encrypted	*AT-001*	Not Done	
Testing for user enumeration - User enumeration	*AT-002*	Not Done	
Testing for Guessable (Dictionary) User Account - Guessable user account	*AT-003*	Done	
Brute Force Testing - Credentials Brute forcing	*AT-004*	Not Done	

Figura 25. Lista de Chequeo para pruebas de seguridad de OWASP.

Resultados evaluación de seguridad

Para un conjunto de 60 test realizados en ambos grupos (Control y Experimental) los resultados mostrados en la siguiente figura reflejan la disminución de las vulnerabilidades de seguridad con impacto Alto, Medio y Bajo atendiendo a las dimensiones de Confidencialidad, Integridad y Disponibilidad. Figura 26

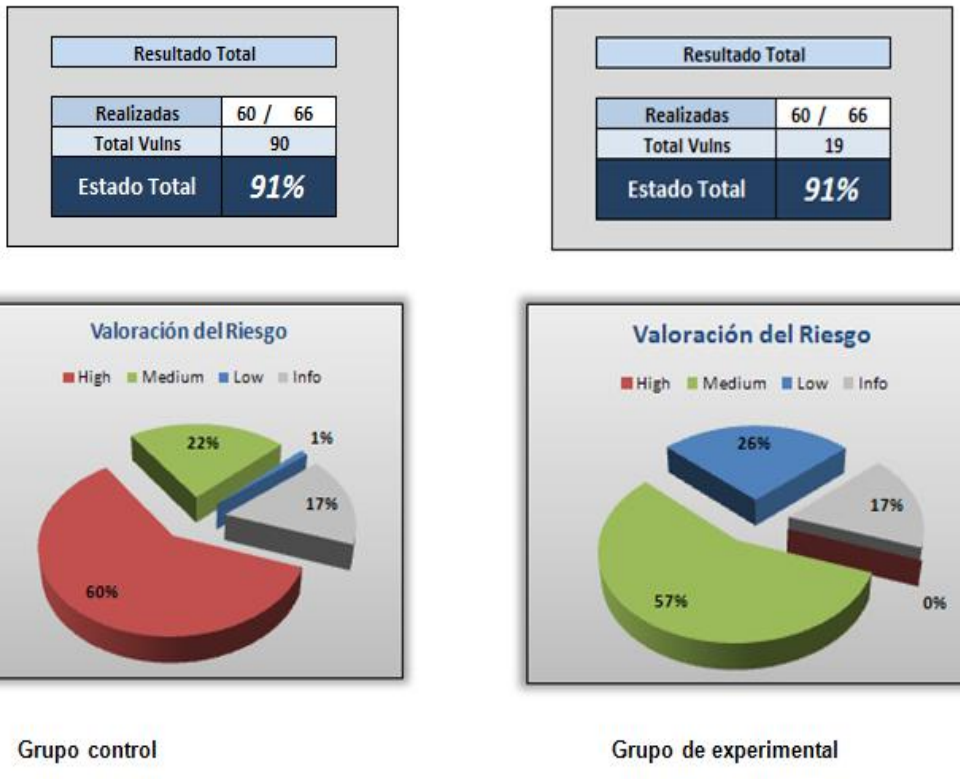


Figura 26. Resultados de la evaluación de seguridad con respecto a los indicadores de Confidencialidad, Integridad y Disponibilidad. Fuente Elaboración propia

A partir de los resultados que se presentan es posible concluir que en el proyecto en el cual se aplicó la guía propuesta en la investigación se disminuyó el riesgo tecnológico en las dimensiones de Confidencialidad, Integridad y Disponibilidad, especialmente en aquellos con impacto Alto cuyas derivaciones pueden causar mayores afectaciones en el sistema de información y sus usuarios.

3.4 Análisis económico de la propuesta

El análisis económico de la propuesta se realizó teniendo en cuenta el costo de implantación, el ahorro percibido a partir de sus efectos en el grupo experimental y de control y los beneficios en el ámbito político, económico y social.

3.4.1 Costo de implantación

Costo Total = Total de horas del tiempo dedicado del trabajador * tarifa horaria

Empleando la jornada laboral de 8h y una tarifa horaria de $15. 00 MN, se obtuvieron los siguientes resultados.

Tabla 14. Costo de implantación. Fuente Elaboración propia.

Actividades	**Cantidad de personas**	**Duración (días)**	**Tarifa horaria**	**Costo total**
A-1 Caracterizar el sistema	3	5	15	$ 225
A-2 Identificar amenazas a la seguridad del sistema de TI.	3	12	15	$ 540
A-3 Valorar el riesgo.	2	10	15	$ 300
A-4 Determinar controles de seguridad.	4	15	15	$ 900
A-5 Evaluar eficacia de los controles implementados.	2	5	15	$ 150
A-6 Aprendizaje	2	7	15	$ 210
Total				**$ 2325.00**

3.4.2 Valoración del Esfuerzo y Costos de producción

Realizando una valoración en términos de la disminución del esfuerzo y costos de producción para la solución de las vulnerabilidades que se encontraron en la Fase de pruebas. En el sistema GRHS y en el sistema seleccionado anteriormente, se estiman lo siguiente:

Esfuerzo de producción= Tiempo de desarrollo *Cantidad de personas

Costo de producción= Tiempo de desarrollo * Tarifa horaria*Cantidad de personas

Tabla 15. Costo y esfuerzo de producción Grupo Experimental. Fuente Elaboración propia.

Tiempo de desarrollo (días)	**Cantidad de personas**	**Tarifa Horaria**	**Esfuerzo de producción**	**Costo de producción**
15	3	15	120 horas	$ 5400.00

Tabla 16. Costo y esfuerzo de producción Grupo de Control. Fuente Elaboración propia.

Tiempo de desarrollo (días)	Cantidad de personas	Tarifa Horaria	Esfuerzo de producción	Costo de producción
48	3	15	384	$ 17 280.00

La aplicación de la guía propuesta concibe un ahorro de $ 11 880.00 y 264 horas/hombres solamente por concepto de disminución de esfuerzo y costos de producción asociado a la tarea de solucionar las vulnerabilidades encontradas.

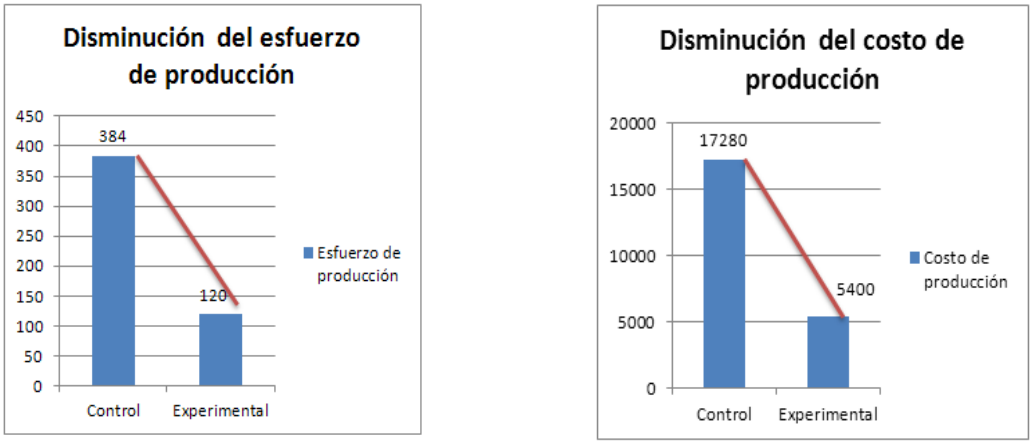


Figura 27. Comparación del esfuerzo y costos de producción en los grupos experimental y de control. Fuente Elaboración propia

3.4.3 Análisis económico y social de la propuesta

El riesgo tecnológico puede ser causa y consecuencia de otro tipo de riesgos, una falla en el sistema de información puede implicar riesgos en otros ámbitos, como pérdidas financieras, multas, acciones legales, afectación sobre la imagen de la organización, causar problemas operativos o afectar las estrategias de la organización.

Estudios realizados en (Telang 2004) demuestran que la divulgación de vulnerabilidades conduce a una pérdida significativa del valor de mercado para los proveedores de software. Esto indica que el mercado reacciona negativamente a la noticia de una divulgación de vulnerabilidades, ya que el descubrimiento de una vulnerabilidad podría sugerir una pérdida en el flujo de caja de los proveedores de software. Se demuestra que, en promedio, un proveedor de software pierde alrededor de 0,63% del valor de mercado en el día del anuncio de la vulnerabilidad. (Cavusoglu 2004) muestran que los valores de capitalización de mercado de las empresas disminuyen, en promedio, en $ 2.1 mil millones en los dos primeros días en que ocurre un fallo de seguridad. En función de las características de la falla de seguridad se relacionan costos asociados a interrupción de negocios, pérdida de ingresos, productividad del usuario final, recuperación y terceras partes vinculadas a los procesos de negocio.

Las vulnerabilidades de software afectan a los flujos de efectivo de un proveedor, debido a dos razones: una, el vendedor tiene que gastar tiempo y esfuerzo en la prestación de un parche para la vulnerabilidad y dos, la insatisfacción de los clientes, debido a que los defectos en los productos podría dar lugar a

pérdida de ventas en el futuro.

Se ha planteado que el Costo asociado a la revelación de una vulnerabilidad para los proveedores de software se puede obtener mediante la siguiente expresión:

Costo de revelación de la vulnerabilidad del proveedor de software = costo de parchear la vulnerabilidad+ λ*(Costo de explotar el software por los usuarios y/o costo de parchear el sistema)

λ: es el factor de internalización, traducido en la pérdida de usuarios que se internaliza por el vendedor debido a una venta perdida o pérdida de la reputación.

Este mismo estudio plantea que $ 1 necesario para resolver un problema durante la fase de diseño crece de $ 60 a $ 100 para resolver el mismo problema después que la aplicación ha sido entregada.

Beneficios

Los resultados indican que el ahorro de costes y otras ventajas se consiguen cuando el análisis de la seguridad y las prácticas de ingeniería seguras se introducen temprano en el ciclo de desarrollo. Dado que casi las tres cuartas partes de los defectos relacionados con la seguridad son cuestiones de diseño que podrían resolverse económicamente durante las primeras etapas, existe una gran oportunidad para el ahorro de costes cuando se aplican los principios de ingeniería de software seguro durante el diseño. (Hoo 2005)

En relación a la propuesta que se presenta se plantean beneficios en cuanto a incidir en una valoración adecuada del esfuerzo y costos asociadas al proyecto puesto que se parte de un análisis de riesgos para determinar la seguridad necesaria que evite incidir en la corrupción del alcance o la obtención un producto bañado en oro.

Además se alinea con la estrategia formulada en el país por el Ministerio de Informática y Comunicaciones. Con el objetivo de detectar y neutralizar las posibles acciones del enemigo en la esfera de las TIC implementa en la Resolución 127/2007 un basamento legal que establece los requerimientos de seguridad en el empleo de las tecnologías de la información que propendan a la disminución de los riesgos en la seguridad informática. (MIC, 2007)

En el orden político responde al llamado realizado por el Comandante de la Revolución Ramiro Valdés en el Panel de Alto Nivel “Políticas Nacionales TICs por el desarrollo y la soberanía” enfocado en la necesidad de determinar políticas en relación con la soberanía tecnológica encaminadas al trabajo por la seguridad e invulnerabilidad de las redes de telecomunicaciones. (Menéndez 2009)

La propuesta apoya la política expresada en los Lineamientos del Partido y la Revolución en relación con la vinculación de las investigaciones al proceso de producción, el aumento de la credibilidad en las relaciones internacionales para el cumplimiento de los compromisos contraídos y la indicación de sostener y desarrollar los resultados en el campo de la industria del software y el proceso de informatización de la sociedad, además contribuye a elevar la soberanía tecnológica en el desarrollo de la infraestructura de telecomunicaciones al trabajar la seguridad y la respuesta a los riesgos que puedan afectar los sistemas e infraestructuras críticas. Lineamiento 24, 73, 130, 135 y 223. (PCC 2011)

3.5 Conclusiones del capítulo

En el capítulo se realizó la validación de la guía propuesta para la gestión del riesgo tecnológico a través de la consulta a expertos y la aplicación práctica en un proyecto del Centro TLM, en base a lo cual se determinó que:

La calidad de la guía propuesta evaluada por los expertos a través de los indicadores definidos se considera Muy Adecuada en un 95% así como resultados por encima del 86% en el instrumento aplicado a los Especialistas del Centro TLM, lo cual es aceptado por la autora.

El indicador de comprensión obtuvo la más baja puntuación lo cual refleja las necesidades de especialización respecto a la seguridad en el desarrollo de software y la pertinencia de la guía propuesta para abordar la gestión del riesgo tecnológico.

Los resultados obtenidos producto de la aplicación práctica reflejaron la finalización de un producto de software capaz de cumplir de forma efectiva con sus objetivos de seguridad.

La propuesta apoya la política económica y social del país expresado en los Lineamientos del Partido y la Revolución, además contribuye a la disminución del esfuerzo y costos de producción así como a la entrega de productos de software con la calidad y seguridad requerida, lo cual favorece la satisfacción del cliente y la posibilidad para el surgimiento de nuevas oportunidades de negocio.

CONCLUSIONES

La gestión de riesgos se enmarca como un proceso crítico para la gestión de la seguridad durante el proceso de desarrollo de software, la indefinición de actividades con este objetivo afecta el cumplimiento de los objetivos de seguridad planteados para el software.

La guía propuesta ofrece un marco de trabajo que asegura que los requisitos de seguridad de un sistema se adapten según la proporción de sus riesgos y puede apoyar la estandarización de este trabajo en los proyectos de desarrollo de la institución.

La propuesta se encuentra alineada con los estándares y buenas prácticas de seguridad en el desarrollo de software así como con las políticas de la Dirección de Seguridad de la institución enmarcadas en asegurar los activos del proceso de producción que se lleva en los Centros de Desarrollo.

La validación teórica realizada a través de la consulta a expertos así como la aplicación práctica de la guía arrojaron una evaluación favorable en relación con las mediciones obtenidas de la Calidad y el cumplimiento de los objetivos de seguridad del software.

La aplicación de la guía apoya la política económica y social del país expresado en los Lineamientos del Partido y la Revolución además disminuye significativamente el esfuerzo y costos de producción asociados a la solución de vulnerabilidades de seguridad, en aproximadamente 264 horas/hombres y un ahorro de $11 880.00 por concepto de costos de producción.

RECOMENDACIONES

1. Incluir en la guía elementos relacionados con la gestión del riesgo tecnológico para tener en cuenta en la puesta en producción del sistema.
2. Definir un repositorio reutilizable de amenazas asociado a requisitos de seguridad representados.

REFERENCIAS BIBLIOGRÁFICAS

ALBERTS, Christopher and STEVENS, James, 2003, *Introduction to the OCTAVE Approach* [online]. Pittsburgh. [Cited: 6 de febrero de 2013] Available from: http://resources.sei.cmu.edu/asset_files/UsersGuide/2003_012_001_51556.pdf

ALEXANDER, Ian, 2002, Modelling the Interplay of Conflicting Goals with Use and Misuse Cases Direct Conflict of SubGoals. *Proceedings of 8th International Workshop on Requirements Engineering Foundation for Software Quality* [online]. 2002. Vol. Germany, p. 1–7. [Cited: 10 de abril de 2013] Available from: http://ceur-ws.org/Vol-109/paper1.pdf

ALVAREZ, Eylena, 2011, *Procedimiento para la Gestión de Riesgos en el Proyecto Minería.* [online]. Universidad de Ciencias Informáticas. [Cited: 6 de enero de 2013] Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TD_04556_11/1/TD_04556_11.pdf

ARENAS, Ana Silvia Valladares, 2010, *Proceso de Gestión de riesgos para proyectos de desarrollo de software de Softel* [online]. *Maestría*. Universidad de Ciencias Informáticas. [Cited: 13 de enero de 2013] Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TD_03909_10/1/TD_03909_10.pdf

BAHTIT, 2013, Risk Management for ISO 27005 Decision support. *International Journal of Innovative Research in Science, Engineering and Technology*. 2013. Vol. 2, no. 3, p. 530–538. [Cited: 23 de abril de 2013] Available http://www.ijirset.com/upload/march/1_Risk%20Management%20for%20ISO%2027005.pdf

BEJARANO, Instituto Español de Estudios Estrategicos, 2013, *Más sobre la amenaza cibernética* [online]. [Cited: 12 de enero de 2013] Available from: http://www.ieee.es/Galerias/fichero/docs_analisis/2013/DIEEEA452013_MasAmenazaCibernetica_MJCB.pdf

BOEHM, 1991, Software risk management: principles and practices. *IEEE Software*. 1991. Vol. 8, no. 1.

CAVUSOGLU, MISHRA, Raghunathan, 2004, The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce*. 2004.

DAMODARAN, Meledath, 2006, SECURE SOFTWARE DEVELOPMENT. *Issues in Information Systems* [online]. 2006. Vol. VII, no. 1, p. 150–154. [Cited: 4 de mayo de 2013] Available from: http://iacis.org/iis/2006/Damodaran.pdf

DHS, 2006, SECURITY IN THE SOFTWARE LIFECYCLE. [online]. 2006. No. August, p. 18–23. [Cited: 8 de mayo de 2013] Available from: http://home.himolde.no/~molka/lo205/booknotes-06/Security-Software-Lifecycle2006.pdf

ENISA, 2006, *Risk Management : Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools* [online]. Europa. [Cited: 15 de mayo de 2013] Available from: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory

ESCOBAR, Mercedes, 2009, *Aplicación y Mejora del Modelo de Gestión de Riesgos MoGeRi en el proyecto productivo Sistema de Facturación y Cobro para la Empresa de Gas Manufacturado.* [online].

Universidad de Ciencias Informáticas. [Cited: 23 de enero de 2013] Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TD_2762_09/1/TD_2762_09.pdf

FIRESMITH, Donald, 2011, a-collaborative-method-for-engineering-safety-and-security-related-requirements. *Software Engineering Institute* [online]. 2011. [Cited: 17 de mayo de 2013] Available from: http://blog.sei.cmu.edu/post.cfm/a-collaborative-method-for-engineering-safety-and-security-related-requirements

GONZÁLEZ, Yusleimi, 2008, *Gestión de Riesgos del Proyecto Sistema de Gestión Penitenciaria (SIGEP).* [online]. Universidad de Ciencias Informáticas. [Cited: 17 de enero de 2013] Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TD_1490_08/1/TD_1490_08.pdf

GUTIÉRREZ, Carlos and RAIDEL CANO PÉREZ, 2008, *Gestión de los Riesgos en el Proyecto "A Jugar"* [online]. Universidad de Ciencias Informáticas. [Cited: 17 de mayo de 2013] Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TD_1231_08/1/TD_1231_08.pdf

HOO, Kevin Soo, 2005, Tangible ROI through Secure Software Engineering. *Secure Business Quarterly*. 2005. Vol. 1, no. 2, p. 1–3. Cambridge: Secure Business Quarterly.

HURTADO, Gloria Piedad Gasca, 2010, *Metodología de Gestión de Riesgos para la Adquicisión de Software en Pequeños Entornos-MEGRIAD*. Tesis doctoral. Universidad Politécnica de Madrid.

ISLAM, Shareeful and DONG, Wei, 2010, Security Requirements Addressing Security Risks for improving Software Quality. *Programa de Investigación y Desarrollo China*. 2010. No. 60673118.

ISO/IEC 27005, 2008, *ISO/IEC 27000 Vocabulario y definiciones* [online]. [Citado: 17 de enero de 2013] Available from: http://www.iso27000.es/glosario.html

ISO/IEC, 2008, *Gestión de riesgos de seguridad de la información. Tecnologías de la información-Técnicas de seguridad- ISO 27005:2008*. Zúrich, Suiza: Organización Internacional para la Estandarización.

KASPERSKY LAB, 2013, *Global Corporate IT Security Risks : 2013* [online]. [Cited: 4 de enero de 2013] Available from: http://media.kaspersky.com/en/business-security/Kaspersky_Global_IT_Security_Risks_Survey_report_Eng_final.pdf

LABSI, 2012, *Informe técnico. Problemas de seguridad en el software.* Centro TLM. UNiversidad de Ciencias Informáticas. [Cited: 02 de diciembre de 2012]. La Habana.

LAMSWEERDE, Axel Van, 2003, From System Goals to Intruder Anti-Goals : Attack Generation and Resolution for Security Requirements Engineering. *In Proceedings of the Requirements for High Assurance Workshop*. 2003. Vol. 6, no. 2, p. 3–7.

LUJAN, Darena Ramirez, 2012, *Proceso de Gestión de Riesgos para el Desarrollo de Aplicaciones Informáticas en la UCI.* [online]. Universidad de Ciencias Informáticas. [Cited: 24 de enero de 2013] Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/7966/1/TM_06223_12.pdf

MAP, 2012, MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. *Ministerio de Hacienda y Administraciones Públicas*. Madrid, 2012. [Cited: 7 de mayo de 2013]. Avaivable from:

http://www.seap.minhap.gob.es/dms/es/publicaciones/centro_de_publicaciones_de_la_sgt/Monografias0/parrafo/Magerit_2012/Magerit_v3_libro1_metodo.pdf

MCGRAW, Gary, 2006, *Software Security Building Security In*. United States : Addison Wesley Professional. ISBN 9780321356703.

MEIER, 2010, Improving Web Application Security: Threats and Countermeasures. *Microsoft* [online]. 2010. [Cited: 10 de junio de 2013] Available from: http://msdn.microsoft.com/en-us/library/ff649874.aspx

MELLADO, Daniel, 2007, Un Proceso de Ingeniería de requisitos de seguridad en la práctica. *IEEE Latin American Transactions*. 2007. Vol. 5, no. 4, p. 211–217.

MENÉNDEZ, Ramiro Valdés, 2009, Políticas Nacionales TICs por el desarrollo y la soberanía . *Informática 2009* [online]. [Cited: 10 de enero de 2013]. Available from: http://anterior.cubaminrex.cu/Sociedad_Informacion/2009/Intervencion-RamiroValdes.html

MICROSOFT, 2002, MSF Risk Management Discipline. Microsoft Corporation. Report 602-i401a. United States. Online. [Cited: 10 de junio de 2013]. Avaivable from: http://www.uml.org.cn/softwareprocess/MSFRiskManagementDisciplinev.1.1.pdf

MICROSOFT, 2006, Modelado de amenazas Descubra los errores en el diseño de la seguridad con el método STRIDE. *MSDN Magazine* [online]. [Cited: 19 de enero de 2013]. P. 4–8. Available from: msdn.microsoft.com/es-es/magazine/cc163519.aspx

MICROSOFT, 2012, Descripción general de Microsoft Solutions Framework (MSF). [online]. [Cited: 21 de junio de 2013]. Available from: http://msdn.microsoft.com/es-es/library/jj161047.aspx

MOYA, Osiris Pérez, 2013, *Proceso para gestionar riesgos en los proyectos de desarrollo de software del Centro de Informatización Universitaria* [online]. Universidad de Ciencias Informáticas. [Cited: 10 de enero de 2013]. Available from: http://bibliodoc.uci.cu/RDigitales/2013/junio/11/Tdig_0028_13.pdf

OCHOA, Duque, 2010, *Metodologías de gestión de riesgos*. 2010. Universidad de Caldas : Facultad de Ingeniería. Colombia. [Cited: 19 de junio de 2013]. Avaivable from: http://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf

P.SALINI, 2011, A SURVEY ON SECURITY REQUIREMENTS ENGINEERING. *International Journal of Reviews in Computing*. 2011. Vol. 8, no. December, p. 2076–3328.

PALAREA, Anika, 2008, *Aplicación de un modelo de Gestión de Riesgos en el Proyecto Programa Nacional de Informatización del Conocimiento Geológico* [online]. Universidad de Ciencias Informáticas. [Cited: 4 de enero de 2013]. Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TD_1226_08/1/TD_1226_08.pdf

PCC, 2011, Lineamientos de la Política Económica y Social del Partido y la Revolución. 2011.

PMI, 2013, Guía del PMBOK. *Guía del PMBOK*. Project Management Institute, 2013. p. 317.

REYES, Yandielys, 2009, *Aplicación y mejora del Modelo de Gestión de Riesgos "MoGeRi" al proyecto "Captura y Catalogación de Medias"* [online]. Universidad de Ciencias Informáticas. [Cited: 4 de enero

de 2013]. Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TD_2768_09/1/TD_2768_09.pdf

RIASCOS, 2010, Herramientas TIC como apoyo a la gestión del talento humano *. *Cuadernos de Administración*. 2010. Vol. 27, no. 46, p. 1–2. [Cited: 13 de febrero de 2013]. Avaivable from: http://dintev.univalle.edu.co/revistasunivalle/index.php/cuadernosadmin/article/view/1554/2509

RIVERA, Sergio, 2010, *Modelo de un Sistema de Razonamiento Basado en Casos para el Análisis en la Gestión de Riesgos.* [online]. Universidad de Ciencias Informáticas. [Cited: 4 de enero de 2013]. Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TM_04806_11/1/TM_04806_11.pdf

SEI, 2006, *Security Quality Requirements Engineering (SQUARE): Case Study Phase III* [online]. Pittsburgh, Pennsylvania. [Cited: 4 de abril de 2013]. Available from: www.sei.cmu.edu/reports/06sr003.pdf

SEI, 2010, *CMMI® for Development, Version 1.3 CMMI-DEV, V1.3* [online]. Carnegie Mellon University. [Cited: 4 de abril de 2013]. Available from: http://www.sei.cmu.edu/reports/10tr033.pdf

SEI, 2012, *Mission Risk Diagnostic (MRD) Method Description* [online]. Pittsburgh. [Cited: 4 de abril de 2013]. Available from: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2012_004_001_15431.pdf

STONEBURNER, Gary, 2002, *Risk Management Guide for Information Technology Systems Recommendations of the National Institute of Standards and Technology*. [Cited: 12 de abril de 2013]. Available from: http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

TELANG, Rahul and WATTAL, Sunil, 2004, Impact of Software Vulnerability Announcements on the Market Value of Software Vendors – an Empirical. 2004. No. Wise 2004, p. 1–12.

UCI, 2012, *Ciclo de vida de proyectos de desarrollo de software*. Reporte técnico. Dirección de producción. Universidad de Ciencias Informáticas. La Habana.

VARGAS, Ricardo Viana, 2008, Basic Risk Identification Techniques. In : [online]. 2008. [Cited: 27 de mayo de 2013]. Available from: http://certifedpmp.wordpress.com/

YAZAR, Zeki, 2002, A Qualitative Risk Analysis And Management Tool-CRAMM. *SANS Institute InfoSec Reading Room*. 2002. Vol. Versión 1., p. 6–10.

ZULUETA, Yeleny, 2007, *Modelo de Gestión de Riesgos en Proyectos de Desarrollo de Software.* [online]. Universidad de Ciencias Informáticas. [Cited: 4 de enero de 2013]. Available from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TD_0924_07/1/TD_0924_07.pdf

BIBLIOGRAFÍA

A Case Study in Security Requirements Engineering for a High Assurance System. **Irvine, Cynthia, y otros. 2005.** California: United States : s.n., 2005.

A Qualitative Risk Analysis and Management Tool -CRAMM. **SANS. 2002.** s.l. : **SysAdmin Audit, Networking and Security Institute** - SANS Institute, 2002. Maryland. United States.

Salini, Kanmani *A survey on security requirements engineering.* **2011.** Puducherry: India : International Journal of Reviews in Computing , 2011, Vol. 8. 2076-3328.no 1.

Alexander, Ian. 2002. Modelling the Interplay of Conflicts Goals With Use and Misuse Cases, Londres: Inglaterra. Proceedings of 8th International Workshop on Requirements Engineering Foundation for Software Quality, 2002.

Allen, Julia, y otros. 2009. *Software Security Engineering A Guide for Project Managers.* s.l. : Addison-Wesley, Pittsburgh: United States. 2009.

Análisis y gestión de riesgos. PILAR. **Quintero Villarroya, José Luis. 2012.** Madrid : España. Asociación Española de Calidad, 2012.

Análisis y Modelado de Amenazas . **P.F, Daniel. 2006.** Oviedo : España. s.n., 2006. En línea [Cited: 12 de mayo de 2013] Avaivable from: http://fortinux.com/wp-content/uploads/2010/12/Analisis-y-Modelado-de-Amenazas.pdf

Aplicar el Modelo de Amenazas para incluir la Seguridad en el Modelado de Sistemas. **Castellaro, Castellaro, y otros. 2010.** Santa Fe: Argentina. Universidad Tecnológica Nacional, 2010.

CGR. 2011. *Resolución 60/2011.* La Habana :Cuba. Gaceta Oficial de la República de Cuba, 2011. No 013 Extraordinaria. ISSN 1682-7511.

Chrissis, Mary Beth, Konrad, Mike y Shrum, Sandy. 2009. *CMMI, Guía para la integración de procesos y la mejora de productos.* s.l. : Pearson Educación, 2009. 9788478290963.

ENISA. 2006. *Inventory of risk assessment and risk management methods. Agencia Europea de Seguridad de la Información y redes.* Cited: [4 de mayo de 2013] Avaivable from: https://www.enisa.europa.eu/act/rm/files/deliverables/inventory-of-risk-assessment-and-risk-management-methods/at_download/fullReport 2006.

Gasca Hurtado, Gloria Piedad. 2006. *Análisis de riesgos para el desarrollo de software seguro.* Madrid*:* España. Universidad Politécnica de Madrid, Facultad de Informática. 2006. Cited: [20 de febrero de 2013] Avaivable from: http://www.dlsiis.fi.upm.es/docto_lsiis/Trabajos20052006/Gasca.pdf

Gestión Automatizada de Requisitos de Seguridad para Proyectos de Desarrollo de Líneas de Producto Software. **Rodríguez, Mellado, y otros. 2009.** Congreso Iberoamericano de Seguridad Informática.

CIBSI 2009. Montevideo: Uruguay. Cited: [3 de abril de 2013] Avaivable from: http://www.criptored.upm.es/cibsi/cibsi2009/docs/Papers/CIBSI-Dia2-Sesion3(1).pdf

Hartong, Mark, Goel, Rajni y Wijesekera, Duminda. 2009. *Meta-models for Misuse Cases.* 2009. Washington: United States. Cited: [7 de febrero de 2013]. Avaivable from: http://www.csiir.ornl.gov/csiirw/09/CSIIRW09-Proceedings/Abstracts/Hartong-abstract.pdf

Incorporating Security Requirements Engineering into Standard Lifecycle Processes. **Mead, Nancy, Viswanathan, Venkatesh y Zhan, Justin. 2008.** 4, s.l. : International Journal of Security and Its Applications, IJSIA 2008, Vol. 2. no 4. Cited: [18 de abril de 2013] Avaivable from: http://www.sersc.org/journals/IJSIA/vol2_no4_2008/8.pdf

ISO/IEC 15408-2. 1999. Zúrich, Suiza : Organización Internacional para la Estandarización *Information technology - Security techniques -Evaluation criteria for IT security -- Part 2: Security functional requirements.* 1999.

J.D. Meier, y otros. 2010. Microsoft : Improving Web Application Security: Threats and Countermeasures, 2010.Cited [6 de marzo de 2013] Avaivable from: http://msdn.microsoft.com/en-us/library/ff649874.aspx

Lipner, Steve. 2005. Arizona. United States. *The Trustworthy Computing Security Development Lifecycle.* s.l. : Microsoft Corporation, Annual Computer Security Applications Conference 2005.

Matalobos Vega, Juan Manuel. 2009. Análisis de riesgos de seguridad de la información. *Universidad Politécnica de Madrid. España.* 2009. Cited: [4 de marzo de 2013] Avaivable from: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf

McGraw, Gary. 2006. Build Security In. *Risk Management Framework (RMF).* Cited: [21 de septiembre de 2013. Avaivable from: https://buildsecurityin.us-cert.gov/bsi/articles/best-practices/risk/250-BSI.html.

McGraw, Gary, Chess, Brian y Migues, Sammy. 2010. *Building Security In Maturity Model.* California : United States. s.n., 2010.

Mellado, Daniel. 2007. Un Proceso de Ingeniería de requisitos de seguridad en la práctica. : IEEE Latin American Transactions, 2007, Vol. 5. no 4 Cited: [3 de marzo de 2013]. Avaivable from: http://www.ewh.ieee.org/reg/9/etrans/ieee/issues/vol05/vol5issue4July2007/5TLA4_03Mellado.pdf

MIC. 2007. *REGLAMENTO DE SEGURIDAD PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN.* La Habana : Cuba. Ministerio de Informática y Comunicaciones, 2007.

Microsoft. 2012. Microsoft Solutiosn Frameworks (MSF). Cited [4 de octubre de 2013] Avaivable from:. http://msdn.microsoft.com/es-es/library/jj161047.aspx. ISBN 9780735623538.

Modelado de Amenazas, una herramienta para el tratamiento de la seguridad. **Feck, Carlos Ignacio. 2010.** s.l. Santa Fe, Argentina. Congreso Nacional de Estudiantes de Ingeniería en Sistemas de Información. CNEISI2010. Cited: [4 de febrero de 2013] Avaivable from:

http://www.frsf.utn.edu.ar/cneisi2010/archivos/22-Modelado_de_Amenazas_en_el_dise%C3%B1o_de_sistemas.pdf

NIST. 2010. *Recommended Security Controls for Federal Information Systems and Organizations.* Gaithersburg: United States. National Institute of Standards and Technology, 2010. SP 800-53.

Quintas Santiago, Joaquin. 2010. Patrones de diseño seguro para aplicaciones Web. *Maestría.* s.l. : UCI, La Habana, Cuba. 2010. Cited: [4 de octubre de 2013] Avaivable from: http://repositorio_institucional.uci.cu/jspui/bitstream/ident/TD_03928_10/1/TD_03928_10.pdf

Risk Methods and chance of practices. **Tóth, G.N y L, Berek. 2010.** 2, Hungary : Hungarian Journal of Industrial Chemistry Veszprém, 2010, Vol. 38. no 2. pp193-196. Veszprém:Hungary. Cited: [13 de noviembre de 2013] Avaivable from: http://konyvtar.uni-pannon.hu/hjic/HJIC38_193_196.pdf

SEI. 2010. CMMI for Development v1.3. Carnegie Mellon University, United States. Cited: [5 de noviembre de 2013] Avaivable from: http://www.sei.cmu.edu/reports/10tr033.pdf. CMU/SEI-2010-TR-033.

SEI. 2008. Requirements Elicitation Case Studies Using IBIS, JAD, and ARM. Carnegie Mellon University, United States. Cited: [22 de noviembre de 2013]. Avaivable from: https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/requirements-elicitation-case-studies-using-ibis-jad-and-arm.

SEI. 2008. *Requirements Elicitation Introduction.* Carnegie Mellon University, United States. Cited: [22 de noviembre de 2013] Avaivable from: https://buildsecurityin.us-cert.gov/articles/best-practices/requirements-engineering/requirements-elicitation-introduction

Sindre, Guttorm y Opdahl, Andreas. 2002. *Capturing Security Requirements through Misuse Cases.* 2002.Cited: [13 de octubre de 2013] Avaivable from: www.nik.no/2001/21-sindre.pdf

Software Security Requirements Checklist. **Mahtab, Alam. 2010.** 1, India : International Journal of Software Engineering, 2010, Vol. 3.no 1 Department of Computer Science,INMANTEC.

Solinas, Miguel. 2012. Elicitación y Trazabilidad de Requerimientos utilizando Patrones de Seguridad. *Maestría*. Universidad Nacional de La Plata : Argentina, 2012.

The Risk of e-Voting. **Lauer, Thomas. 2004.** 3, Oakland University, Rochester, USA : Electronic Journal of e-Governmen, 2004, Vol. 2. 1479-439X.

Threat Modeling as a Basis for Security Requirements. **Myagmar, Suvda, Lee, Adam y urcik, William. 2008.** Illinois. United States. National Center for Supercomputing Applications (NCSA).Cited: [8 de octubre de 2013] Avaivable from: http://www.craigchamberlain.com/library/security/Threat%20Modeling%20as%20a%20Basis%20for%20Security%20Requirements.pdf

UCI. 2011. *Políticas de seguridad informática para el desarrollo de software en la UCI.* : Dirección de Seguridad Informática, Universidad de Ciencias Informáticas. La Habana. 2011.

Using the Common Criteria to Elicit Security Requirements with Use Cases. **Ware, Michael, Bowles, John y Eastman, Caroline. 2005.** SoutheastCon, 2006. Proceedings of the IEEE. pp 273-278. Tennessee. United States. s.n., 2006.

Verdún, José Carrillo, y otros. 2007. *The risks analysis like a practice of secure software development. A revision of models and methodologies.*IFIP International Federation for Information Processing. Volumen 213, Network Control and Engineering for QoS, Security, and Mobility. Boston: Springer pp 27-39.

VI Congreso del Partido Comunista de Cuba. 2011. *Lineamientos de la política económica y social del partido y la revolución.* Cuba : s.n., 2011.

Vianca, Vega. 2008. *Ingeniería de Requerimientos para Productos Seguros. Resultados de un Análisis Bibliográfico*. Jornadas Chilenas de Computación 2008. Universidad Católica del Norte. Chile.

Viega, John y McGraw, Gary. 2001. *Building Secure Software: How to avoid security problems the right way.* s.l. : Addison- Wesley, 2001.

WASC. 2004. *Web Application Security Consortium: Clasificación de Amenazas.* 2004. [Cited: 2 de junio de 2013] Avaivable from: http:// projects.webappsec.org/f/WASC_TC-1.0.spa.pdf

ANEXOS

Anexo 1

Tabla 17. Encuesta aplicada a los expertos. Fuente elaboración propia

A continuación se relacionan un conjunto de sentencias junto a una escala de valoración. Le pedimos su cooperación valorando el grado de factibilidad en cada caso.

MA – Muy Adecuado (5)

BA - Bastante Adecuado (4)

A - Adecuado (3)

PA - Poco Adecuado (2)

I – Inadecuado (1)

No	Sentencias	Valoración
1	La guía para la gestión del riesgo tecnológico propuesto define actividades que se integran a las fases del proceso de desarrollo de software desde la Fase de Inicio.	
2	La guía define responsabilidades asociadas a roles que garantizan la ejecución de las actividades definidas.	
3	Se proponen recursos de soporte para la comprensión de la guía.	
4	La propuesta está sustentada en las tendencias de los referentes teóricos existentes para este fin.	
5	Se hace mención a los referentes teóricos en cada caso.	
6	Tiene en cuenta el uso de técnicas y herramientas para la realización de las actividades.	
7	La guía considera determinar el alcance que tendrá la gestión del riesgo tecnológico y posteriormente la identificación de las amenazas a los activos, determinación de controles o salvaguardas, actividades de seguimiento y control y la valoración del riesgo asociado a cada amenaza.	
8	El aprendizaje se integra como uno de los subprocesos que permite la mejora continua y la formalización de lecciones aprendidas.	
9	La comunicación se considera el eje del proceso de gestión de riesgos tecnológicos.	
10	La guía propuesta para la gestión del riesgo tecnológico tiene influencia en la seguridad del software.	

11	Las necesidades de seguridad del sistema que es objeto de análisis se plantean a través de objetivos de seguridad y en consecuencia estos se mapean a RF y RNF de seguridad.	
12	El desarrollo de CU seguros describe los controles o salvaguardas necesarias a partir de las amenazas potenciales que se identificaron para los activos del sistema.	
13	Las actividades de la guía propuesta se enmarcan en las fases iniciales del proceso de desarrollo del software de modo que se desarrolle la arquitectura del sistema en relación con los RF de seguridad.	
14	La implementación de los CU seguros garantiza la trazabilidad de la seguridad hasta el código fuente y facilita la verificación y prueba de los RF y RNF de seguridad.	
15	El diseño de escenarios y casos de prueba orientados al riesgo comprueba la eficacia de los CU seguros que se implementaron y determina la vulnerabilidad del sistema.	
16	Los artefactos propuestos resultantes de la ejecución de las actividades garantizan el seguimiento y control de la seguridad desde las Fases de Inicio hasta la Fase de Construcción.	
17	La evaluación de seguridad que propone el proceso permite cuantificar el riesgo de acuerdo al grado de vulnerabilidad de Confidencialidad, Integridad y Disponibilidad.	
18	Se valora la seguridad del sistema a través de la tolerancia ante los ataques realizados. (Pruebas de intrusión).	
19	Considera que la guía cuenta con las condiciones necesarias para ser aplicada.	
20	La guía propuesta cuenta con los mecanismos necesarios para que el equipo de dirección del proyecto obtenga las garantías objetivas de la seguridad del software.	
21	La guía contribuye a satisfacer las necesidades del cliente en el cumplimiento de los objetivos del software de forma fiable.	
22	La guía se alinea con las exigencias planteadas en relación a garantizar la seguridad del software desde su propio desarrollo.	
23	Cualquier otro criterio o recomendación para contribuir a la mejora de la guía sometida a su consideración.	

Anexo 2

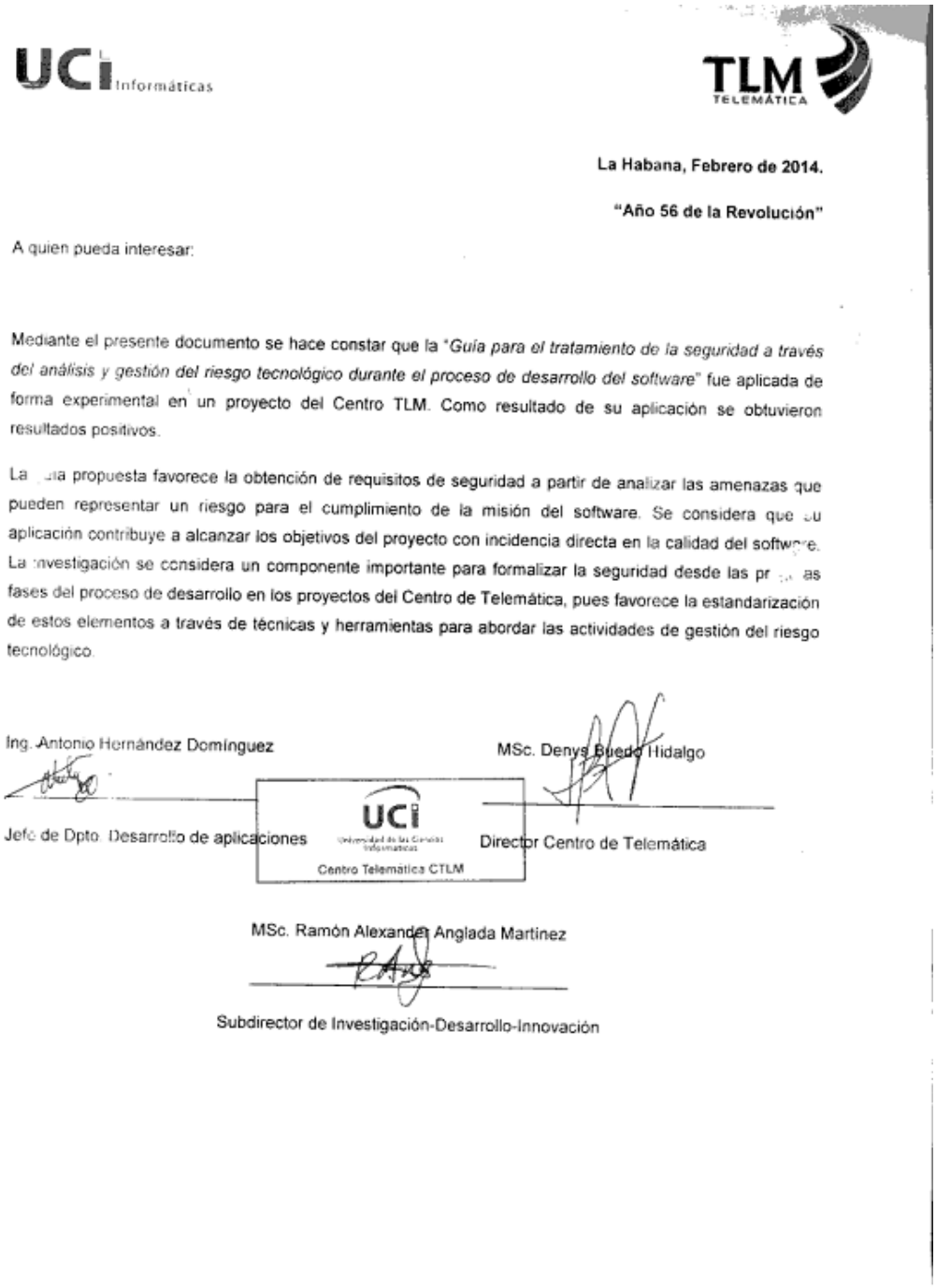
Tabla 18. Especialistas a los que se aplicó el instrumento de validación práctica. Fuente elaboración propia

Especialistas	**Rol**
Maydelin Piñero González	Jefe de proyecto
Erenio Ramos Medina	Arquitecto
Elaine López Rivero	Analista
Denis Henry Cruz Figueredo	Desarrollador
Adrián Hernández Yeja	Asesor de Seguridad
Rogfel Thompson Martínez	Analista de seguridad
Lourdes Veliz Méndez	Administrador de la Calidad
Yasser Azán Basallo	Desarrollador
Yaislenys Landabe Barbarú	Asesora de Calidad
Antonio Hernández Dominguez	Desarrollador
Dayan Trujillo Marquez	Desarrollador
Dayron Agüero Jiménez	Desarrollador
Erick Pérez Castillo	Desarrollador
Ernesto Melian Felpeto	Diseñador de IU
Ismaila López Sotolongo	Analista
Lex Karel Zayas Hernández	Desarrollador
Lianet Salazar Labrada	Analista
Gerardo Rodríguez Fernández	Desarrollador
Yeilin Pérez Martínez	Analista
Yordan Ernesto Estrada	Desarrollador
Wilfredo Rosales Romero	Desarrollador
David Rodríguez Rodríguez	Desarrollador
Katia Ramírez Bruzón	Administrador de la Calidad
Ramón A. Anglada Martínez	Desarrollador

Ernesto Jordán Borjas	Desarrollador
Arianna Pérez Carmenate	Analista
Yoanni Ordoñez Leyva	Arquitecto

Anexo 3

Figura 28. Aval de aplicación de la "Guía de gestión del riesgo tecnológico para el tratamiento de la seguridad durante el proceso de desarrollo del software"



UCI Informáticas

TLM TELEMÁTICA

La Habana, Febrero de 2014.

"Año 56 de la Revolución"

A quien pueda interesar:

Mediante el presente documento se hace constar que la "*Guía para el tratamiento de la seguridad a través del análisis y gestión del riesgo tecnológico durante el proceso de desarrollo del software*" fue aplicada de forma experimental en un proyecto del Centro TLM. Como resultado de su aplicación se obtuvieron resultados positivos.

La guía propuesta favorece la obtención de requisitos de seguridad a partir de analizar las amenazas que pueden representar un riesgo para el cumplimiento de la misión del software. Se considera que su aplicación contribuye a alcanzar los objetivos del proyecto con incidencia directa en la calidad del software. La investigación se considera un componente importante para formalizar la seguridad desde las primeras fases del proceso de desarrollo en los proyectos del Centro de Telemática, pues favorece la estandarización de estos elementos a través de técnicas y herramientas para abordar las actividades de gestión del riesgo tecnológico.

Ing. Antonio Hernández Domínguez
Jefe de Dpto. Desarrollo de aplicaciones

MSc. Denys Prado Hidalgo
Director Centro de Telemática

UCI Centro Telemática CTLM

MSc. Ramón Alexander Anglada Martínez
Subdirector de Investigación-Desarrollo-Innovación