Universidad de las Ciencias Informáticas

Facultad 3

Guía para la gestión del requisito no funcional seguridad en el desarrollo de aplicaciones web

Tesis en opción al título de
Máster en Calidad de Software

Autora: Ing. Yisel Niño Benitez

Tutores: Dr.C. Nemury Silega Martínez

Dr.C. Ana Marys Garcia Rodríguez

La Habana, 2018

Año 60 de la Revolución

AGRADECIMIENTOS

A Dios por ser mi faro en la tormenta, por la fuerza que me da, por la fe, por cada día de vida.

A Fidel por ser padre de un sueño hecho realidad. A la Universidad de las Ciencias Informáticas.

A mi hijo le debo las gracias porque es fuerza y reto. A él pido perdón por las horas de desvelo, las madrugadas a mi lado, por los cuentos que no leí en el afán de ser también ejemplo.

A mi familia por el aliento ante cada obstáculo, por la constancia y fuerza con que me nutren a cada paso, por el ejemplo que son, por estar junto a mí a pesar de las distancias. A mi mami Nena, mi eterno ángel guardián.

A mis tutores Nemury y Ana Marys, por la guía siempre certera, por su apoyo, por las horas dedicadas, por ser amigos invaluables más allá del compromiso científico. Ana, gracias por los innumerables consejos, los tirones de orejas, las horas de desvelo, las enseñanzas de vida, la complicidad, por todo el tiempo. Nemu, gracias por la compañía inicial, por los garabatos en la pizarra concretando las ideas para que la ciencia llenara una simple idea.

Al tribunal por las sugerencias y recomendaciones, por su tiempo.

Al claustro de profesores y a los estudiantes de la maestría de Calidad de Software.

Al centro CEIGE, por ser casi un hogar. A su consejo de dirección, por ser como familia. A mis colegas del departamento Desarrollo de Componentes, por ser un gran equipo más allá de los 0 y 1.

A mis amigos, los de aquí y los de allá, siempre al tanto del avance y animando en pos del éxito. Gracias infinitas por ser, por estar, aguantar mis locuras y los inesperados S.O.S. de ayuda materna cuando el tiempo no alcanza.

DEDICATORIA

Para Ernestico, que es risa, travesura, reguero, reto, fuerza y luz de mi vida…

RESUMEN

La gestión de la Seguridad Informática desde etapas tempranas del desarrollo de software evita que los mecanismos de seguridad deban ser ajustados dentro de un diseño ya existente, lo que introduce cambios que pueden generar vulnerabilidades en el software, aumentando el coste de desarrollo. Verificar la seguridad de forma temprana y frecuente en el desarrollo de aplicaciones web garantiza la disminución de las vulnerabilidades que pueda presentar el producto. Existen procesos definidos para la gestión y el desarrollo de los requisitos de software, sin embargo, no se gestiona de forma explícita el requisito no funcional Seguridad, ni se consideran tanto las pautas de la norma cubana ISO 25010:2016 para la Seguridad, como los riesgos que puedan estar presentes en el proceso de desarrollo. La presente investigación propone una guía para la gestión del requisito no funcional Seguridad para disminuir el número de vulnerabilidades en el desarrollo de aplicaciones web. Para ello se conciben actividades relacionadas con la gestión y trazabilidad del requisito no funcional Seguridad desde las primeras disciplinas de desarrollo de software y una lista de requisitos de seguridad que pueden ser utilizados por los equipos de proyectos. La validación de los resultados se logra, mediante el empleo de métodos científicos que corroboran la hipótesis y convergen en una alta satisfacción de los clientes con la propuesta.

Palabras claves: guía, requisito no funcional Seguridad, riesgo, seguridad informática, vulnerabilidad

ÍNDICE

INTRODUCCIÓN

El desarrollo de la Web se manifiesta en una gran cantidad de transformaciones, evolucionando de páginas sencillas con pocas imágenes y contenidos estáticos, a páginas complejas con contenidos dinámicos que provienen de bases de datos. Este progreso ha propiciado la creación de aplicaciones web, las cuales permiten la generación automática de contenido, la construcción de páginas personalizadas según el perfil del usuario, y el desarrollo del comercio electrónico [1-4]. Sin embargo, con la creciente demanda de las Tecnologías de la Información y la Comunicación (TIC), surgen dificultades asociadas a debilidades que estas tecnologías pueden presentar. Muchas entidades y personas son víctimas de fraudes o ataques informáticos por no cumplir con normas o requisitos de Seguridad Informática (SI) necesarios para prevenirlos [5; 6].

La SI tiene como objetivo garantizar que el material y los recursos de software y hardware de una organización se utilicen únicamente en los propósitos para los que fueron creados y dentro del marco previsto. Por su relevancia, es recomendable considerar la SI desde la concepción inicial de los sistemas de software y durante todo su ciclo de vida [2; 7; 8], cobrando vital importancia dentro de la Ingeniería de Software (IS), ya que trata de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada [9; 10].

Varios autores coinciden en la necesidad de aplicar mecanismos efectivos de IS proporcionando teorías, métodos y herramientas para construir sistemas de software que operen de manera confiable y con la calidad requerida [11-14]. Dentro de la IS, un área determinante para el éxito de un proyecto es la Ingeniería de Requisitos (IR), que identifica las características y propiedades del producto a desarrollar [14; 15]. Los requisitos del sistema se clasifican en Requisitos Funcionales (RF) y Requisitos No Funcionales (RNF) [14]. Los RF describen lo que un sistema debe hacer, mientras que los RNF son aquellos que no se refieren directamente a las funciones específicas del sistema, sino a las propiedades emergentes de este como fiabilidad, rendimiento, mantenibilidad, *seguridad*, portabilidad y estándares a utilizar [15]. La Norma Cubana (NC) ISO 25010: 2016 [16] relaciona las características de calidad de un producto y sus sub-características que se van a tener en cuenta a la hora de evaluar las propiedades de un producto software determinado y establece el sistema para la evaluación de la calidad del producto.

El RNF de Seguridad se define como grado de protección de los datos, software y/o plataforma tecnológica de posibles pérdidas, actividades no permitidas o uso para propósitos no establecidos previamente [9; 17; 18]. A diferencia de otros RNF como la fiabilidad y el rendimiento, la Seguridad no ha sido completamente integrada dentro del ciclo de vida de desarrollo y es considerada aún después que el sistema ha sido diseñado [19]. El RNF de Seguridad introduce no solo características de calidad, sino también restricciones de software, hardware y legales propias de la entidad cliente, bajo las cuales el sistema debe operar. Ignorar tales restricciones y los riesgos presentes en el entorno de explotación, durante el proceso de desarrollo podría acarrear problemas, que generalmente se traducen en vulnerabilidades del software, y conllevan a un incremento en los costos de presupuesto y tiempo para solventarlos una vez que han sido identificados [20; 21].

La Universidad de las Ciencias Informáticas (UCI) tiene como parte de su misión la producción de aplicaciones y servicios informáticos, a partir de la vinculación estudio-trabajo como modelo de formación para servir de soporte a la industria cubana de la informática [22]. Sus productos una vez finalizados son sometidos a pruebas de liberación por la Dirección de Calidad de Software (DCS). Dentro de este proceso de verificación y validación de la calidad del software, se ejecutan pruebas de seguridad para identificar algunas vulnerabilidades que pudieran estar presentes.

Según datos recolectados del año 2016 a partir de los Informes de Tendencia emitidos por la DCS, de un total de 48 pruebas realizadas se identificaron 58 vulnerabilidades, lo que corresponde aproximadamente a un 0.92 % del total de No Conformidades (NC) detectadas. En el año 2017 se identificaron 43 NC tipificadas como vulnerabilidad en las pruebas realizadas, siendo estas un 0.88 % del total de NC detectadas en ese propio año [23]. A pesar de que el porciento de NC es bajo numéricamente, el impacto de estas es crítico para los proyectos ya que las más frecuentes estaban relacionadas con vulnerabilidades Cross-site scripting (XSS), ausencia de la cabecera *anti-clickjacking X-Frame-Options*, cookies sin bandera *httponly* e información revelada: *Apache mod_status / server-status [24]*.

La tenencia de estas vulnerabilidades permite a atacantes remotos ejecutar scripts arbitrarios como otros usuarios, utilizar múltiples capas transparentes u opacos para engañar a un usuario para que haga clic en un botón o enlace en otra página cuando tenían la intención de hacer clic en la página de nivel superior, o divulgar de forma no autorizada determinado nivel de información [24]. Estos resultados demuestran que,

a pesar de tomar acciones para la detección de vulnerabilidades, aún no existe una conciencia en los proyectos de la importancia de las pruebas de seguridad y que la gestión del RNF de Seguridad es aún insipiente.

En encuestas aplicadas a diferentes roles, entre los que se encuentran: jefes de proyecto, analistas, desarrolladores, administradores de calidad, arquitectos, asesores y jefes de departamento, pertenecientes a diversos proyectos de los centros de desarrollo de la universidad, se identificó que de un total de 20 encuestados:

- el 90% conoce que se definen RNF de Seguridad y el 100% lo cree imprescindible para el desarrollo de las aplicaciones seguras.
- solamente el 30% considera la trazabilidad y gestión de la seguridad en todo el ciclo de vida del proceso de desarrollo del producto, sin embargo, no tienen en cuenta los riesgos que pueden dar lugar a vulnerabilidades, el 55% lo propone a partir de la disciplina Requisitos, sin embargo, de estos solo un 10% realiza el seguimiento hasta la disciplina de Análisis y Diseño, el resto no considera necesario el seguimiento en las disciplinas siguientes.
- el 95% de las personas conoce los inconvenientes de no hacer un tratamiento certero de la seguridad en el desarrollo e identifican como aspectos negativos en este sentido: penetración en los sistemas, uso indebido de los servidores y su información, uso indebido de credenciales de autenticación, inyecciones SQL, atraso en el cronograma de entrega del producto por la resolución de NC de seguridad en las pruebas de liberación y aumento del costo de desarrollo, imposibilidad de despliegue del producto en determinado entorno por no tener en cuentas las restricciones legales de seguridad del cliente y con ello la pérdida del prestigio de la entidad desarrolladora ante el cliente.
- el 92% de las personas encuestadas, independientemente de que reconocen la necesidad de la identificación y gestión del RNF de Seguridad, no consideran las sub-características de Seguridad definidas en la NC ISO 25010:2016.
- El 76% de los encuestados no tienen en cuenta los riesgos que puedan estar presentes en el proceso de desarrollo, relacionados con la identificación de las vulnerabilidades.

Por lo descrito anteriormente y teniendo en cuenta que "*la SI es un proceso continuo que necesita ser gestionado*" [25], se identificó el siguiente **problema de la investigación**: ¿cómo disminuir el número de vulnerabilidades en el desarrollo de aplicaciones web, considerando los riesgos y las sub-características de seguridad?

Se definió como **objeto de estudio**: los requisitos no funcionales de sistemas de software.

Para dar solución al problema planteado se trazó como **objetivo general:** elaborar una guía para la gestión del requisito no funcional Seguridad, teniendo en cuenta los riesgos y las sub-características de seguridad, para disminuir el número de vulnerabilidades en el desarrollo de aplicaciones web.

Del objetivo general se desglosan los siguientes **objetivos específicos:**

1. Construir el marco teórico referencial de la investigación en torno a la seguridad informática, la ingeniería de requisitos y el requisito no funcional Seguridad.
2. Elaborar una guía para la gestión del requisito no funcional Seguridad en el desarrollo de aplicaciones web.
3. Elaborar una lista de requisitos de seguridad como base para la disminución de las vulnerabilidades en el desarrollo de aplicaciones web.
4. Validar con el empleo de métodos científicos la contribución práctica de la guía para la gestión del requisito no funcional Seguridad en el desarrollo de aplicaciones web.

El **campo de acción** se enmarca en los requisitos no funcionales de Seguridad en el desarrollo de aplicaciones web.

Hipótesis: la aplicación de una guía para la gestión del requisito no funcional Seguridad en el desarrollo de aplicaciones web, contribuirá a disminuir el número de vulnerabilidades identificadas.

Métodos de investigación y técnicas utilizadas:

Métodos teóricos:

Histórico-lógico: utilizado en el estudio crítico de los documentos revisados y su uso como punto de referencia en la investigación.

Inducción-deducción: para la identificación de la problemática, así como sus variantes de solución.

Analítico-sintético: para la descomposición del problema en elementos que permitan su profundización con el fin de sintetizarlos en la solución propuesta.

Hipotético deductivo: para elaborar la hipótesis de la investigación, deducir sus consecuencias y verificar la veracidad de su enunciado.

Modelación: para el modelado de las actividades de los procesos propuestos en la guía para la gestión del requisito no funcional Seguridad.

Métodos empíricos:

Entrevista: para el desarrollo del diagnóstico inicial. Este método permitió obtener información sobre la problemática que se aborda en la investigación.

Encuesta: se empleó en la elaboración de la problemática de la investigación y para la definición de elementos a considerar en la elaboración de la Guía para el desarrollo del requisito no funcional Seguridad.

Análisis documental: para la revisión de la literatura con el objetivo de trazar la línea de investigación y definir la propuesta de requisitos no funcionales de Seguridad y las actividades como parte de la guía para su gestión.

Consulta a expertos: para la identificación de los requisitos no funcionales de Seguridad, y para validar los aportes fundamentales de la investigación.

Iadov: para evaluar y corroborar por usuarios potenciales, la factibilidad y pertinencia de la guía, así como los aportes fundamentales de la investigación.

Métodos estadísticos: se utilizó la modelación para el análisis de las encuestas aplicadas a expertos y a usuarios potenciales.

Aporte práctico:

La elaboración de una guía para la gestión del requisito no funcional Seguridad en el desarrollo de aplicaciones web, teniendo en cuenta los riesgos y las sub-características de seguridad.

Estructura del trabajo:

El documento está constituido por introducción, tres capítulos, conclusiones, recomendaciones y bibliografía. Como norma bibliográfica se utilizó APA 6th. Se incluyen figuras, tablas y anexos que facilitan la comprensión de la investigación. A continuación, se describen los principales elementos de los capítulos.

Capítulo1: Marco teórico referencial: se abordaron los elementos que conforman el marco teórico referencial y que componen el objeto de estudio de la investigación relacionado con la seguridad informática, la ingeniería de requisitos y el requisito no funcional Seguridad.

Capítulo 2: Guía para la gestión del requisito no funcional Seguridad en aplicaciones web: se describió el desarrollo de la guía para la gestión del requisito no funcional Seguridad en el desarrollo de aplicaciones web, en aras de ofrecer una solución al problema, tanto desde una perspectiva teórica-conceptual como desde su solución técnica. Se propuso, además, una lista de requisitos para facilitar la identificación de estos a partir del entorno propio de cada proyecto asociados a riesgos que puedan presentarse.

Capítulo 3: Validación de la investigación: se describió la validación de la guía y la propuesta de requisitos empleando el criterio de expertos, a partir de la contribución práctica de ambos resultados. Se validó la implementación de la solución en la disminución de las vulnerabilidades mediante un estudio de caso, y la validación de la aplicabilidad, utilidad y satisfacción de los usuarios de la guía, empleando la técnica de Iadov.

Finalmente se emitieron las **conclusiones** y **recomendaciones** del trabajo de investigación realizado; así como se listan las **referencias bibliográficas** y los **anexos** que proveen mayor información del trabajo realizado.

CAPÍTULO 1: MARCO TEÓRICO REFERENCIAL

1.1 Introducción

La evolución de las TIC y el creciente uso de las aplicaciones de software, trae consigo el manejo de altos volúmenes de información. Por tanto, es fundamental saber qué datos necesitan protección para así preservarlos. En el presente capítulo se abordan los elementos que conforman el marco teórico referencial y que componen el objeto de estudio de la investigación relacionado con la seguridad informática, la ingeniería de requisitos y el requisito no funcional Seguridad.

1.2 Seguridad informática

La SI tiene el objetivo de minimizar los riesgos asociados al acceso y utilización de determinado sistema de forma no autorizada y en general malintencionada[9; 16; 26-28]. Urbina [8] plantea que la SI es la "*disciplina que con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos a los que está expuesta, tanto físicos como lógicos*". Ruiz Larrocha [29] la concibe como un conjunto de métodos y técnicas para los propósitos antes mencionados, añadiendo a esto las herramientas necesarias que impiden la ejecución de operaciones no autorizadas de un sistema informático. Para la autora, la SI se enfoca en minimizar los riesgos existentes en el acceso y la utilización malintencionada de la información de los sistemas de software, con el fin de garantizar la integridad, confidencialidad y disponibilidad de la misma, haciendo uso de métodos y herramientas.

Viarios autores consideran preciso que los sistemas de software incorporen medidas de seguridad para protegerse de ataques maliciosos, lo que no significa que al hacerlo estén exentos de riesgos [7; 25; 30]. Ante esta situación, el desarrollador ya no sólo debe concentrarse únicamente en los usuarios y sus requisitos, sino también en los posibles ataques. Esto ha motivado cambios importantes en el proceso de diseño e implementación del software para incorporar la seguridad dentro de los requisitos críticos del sistema [31]. Para afrontar el establecimiento de un sistema de seguridad es necesario conocer [32]:

- Cuáles son los **elementos** que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables o directivos de la organización, para lo que previamente hay que realizar un estudio de los riesgos que puedan presentar.
- Cuáles son los **peligros** que afectan al sistema, accidentalmente o provocados. Estos datos se deducen de los aportados tanto por la organización como por el estudio y prueba del propio sistema.
- Cuáles son las **medidas** que deben adoptarse para conocer, prevenir, impedir, reducir y controlar los riesgos potenciales, definiendo los servicios y mecanismos necesarios para minimizarlos.

La SI se resume, por lo general, en cinco principios/características fundamentales [16; 26; 32]:

- **Integridad**: garantiza que los datos no sean modificados desde su creación sin autorización. Se debe asegurar que ningún intruso pueda capturar y modificar los datos en tránsito.
- **Confidencialidad**: avala que la información, almacenada en el sistema informático o transmitida por la red, solamente esté disponible para aquellas personas autorizadas a accederla, es decir, que sólo los individuos autorizados tengan acceso a los recursos que se intercambian, a la información o los activos informáticos pertinentes.
- **Disponibilidad**: garantiza el correcto funcionamiento de los sistemas de información y su disponibilidad en todo momento para los usuarios autorizados.
- **No repudio**: asegura la participación de las partes en una comunicación. El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, el usuario no puede negar dicha acción. En toda comunicación, existe un emisor y un receptor, por lo que se distinguen dos tipos de no repudio:

  a) no repudio en origen: garantiza que la persona que envía el mensaje no puede negar que es el emisor del mismo, ya que el receptor tendrá evidencias del envío,

  b) no repudio en destino: el receptor no puede negar que recibió el mensaje, porque el emisor tiene evidencias de la recepción del mismo.
- **Autenticación**: asegura que sólo los individuos autorizados tengan acceso a los recursos.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel. Para lograr este objetivo se necesitan estándares o normas que rijan aspectos imprescindibles a tener en cuenta en la implementación de un sistema de SI.

1.3 Estándares de Seguridad Informática

Ante la amenaza de ataques informáticos las organizaciones deben demostrar que realizan una gestión competente y efectiva de la seguridad de los recursos y datos que gestionan. Este aspecto hace necesario el uso de estándares o normas que orienten de forma estructurada, sistemática y coherente cómo proceder ante una situación de este tipo, fundamentalmente en su prevención.

1.3.1 Familia ISO 27000

Las normas ISO/IEC 27000 constituyen un conjunto de estándares de seguridad que proporciona un marco para la gestión de la seguridad. Contienen buenas prácticas para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización [33]. Un SGSI es *"esa parte del sistema de gestión general, basada en un enfoque de riesgo comercial, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión incluye la estructura organizativa, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos"* [34]. Algunas normas que forman parte de esta familia se presentan a continuación [25] [35], [36]:

ISO/IEC 27000: 2014 Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de la seguridad de la información – Generalidades y vocabulario: proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a estos y una breve descripción de los pasos para su establecimiento, monitorización, mantenimiento y mejora.

ISO/IEC 27001:2013 Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información - Requisitos: especifica los requisitos para el establecimiento,

implementación, operación, monitorización, revisión, mantenimiento y mejora continua de un SGSI dentro del contexto de la organización. Incluye requisitos para la evaluación y el tratamiento de *riesgos de seguridad* de la información adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. Este estándar constituye una norma certificable.

ISO/IEC 27002:2013 Tecnologías de la información – Técnicas de seguridad – Código de prácticas para los controles de seguridad de la información: no es certificable y abole la ISO/IEC 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Presenta un total de 14 Dominios, 35 Objetivos de Control y 114 Controles. Su implementación requiere de un trabajo de consultoría que adapte los requisitos de la norma a las necesidades de cada organización concretamente. Esta es la razón por la que una organización debe identificar sus requisitos de seguridad.

Existen tres fuentes principales de requisitos de seguridad, una fuente se deriva de **evaluar los riesgos para la organización**, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial. Otra fuente son los **requisitos legales**, **reguladores, estatutarios y contractuales** que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural. Y una tercera es el **conjunto particular de principios, objetivos y requisitos comerciales** para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

ISO/IEC 27003:2017 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información - Orientación: se centra en los aspectos críticos necesarios para el éxito del diseño e implementación de un SGSI de acuerdo con la norma ISO/IEC 27001:2013. Describe el proceso de especificación y diseño, desde el inicio hasta la elaboración de planes de ejecución y el de obtener la aprobación de la gestión para implementar un SGSI. Se define un proyecto para implementarlo y proporciona pautas para las normas de seguridad de la información organizacional y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y administración de controles teniendo en cuenta los entornos de riesgo de seguridad de la información de la organización.

ISO/IEC 27004:2016 Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la información - Monitoreo, medición, análisis y evaluación: proporciona directrices para ayudar a las organizaciones a evaluar el desempeño de la seguridad de la información y la eficacia de un SGSI para cumplir con los requisitos de ISO/IEC 27001: 2013. Establece el seguimiento y la medición de la eficacia de un SGSI, incluidos sus procesos y controles. Realiza el análisis y evaluación de los resultados de estas actividades.

ISO/IEC 27005:2011 Tecnología de la información - Técnicas de seguridad - Gestión del riesgo de seguridad de la información: normativa dedicada exclusivamente a la gestión de riesgos en SI. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de estos riesgos, como soporte al proceso de gestión de riesgos de la norma ISO/IEC 27001.

Esta familia, parece ser completa respecto a la gestión de los procesos de un SGSI, sin embargo, en algunos documentos aborda procesos y en otros controles. Además, su división en varios estándares dificulta su interpretación y puesta en práctica, y aunque realiza un análisis de riesgos, lo hace desde el punto de vista de la implementación de un SGSI y no teniendo en cuenta explícitamente las sub-características o propiedades de seguridad.

1.3.2 Modelo de madurez para la gestión de la seguridad informática (ISM3)

Este modelo puede ser certificable, tiene sus bases en la norma para Sistemas de gestión de la calidad - Requisitos ISO 9001:2000, y puede usarse por sí solo o para mejorar sistemas basados en ISO 27001, en Biblioteca de Infraestructura de Tecnologías de la Información (*ITIL*, por sus siglas en inglés), o en Objetivos de Control para Información y Tecnologías Relacionadas (*Cobit*, por sus siglas en inglés). Se enfoca en los procesos de SI que pueden ser comunes a todas las organizaciones.

ISM3 ve como objetivo de la seguridad de la información el garantizar la consecución de objetivos de negocio. Relaciona directamente los objetivos de negocio de una organización con los objetivos de seguridad de sus productos. Los procesos relacionados con la SI son descritos detalladamente, estableciendo objetivos y métricas que permitan establecer un sistema de calidad enfocado en la mejora continua del proceso, dado que existen criterios para medir la eficacia y eficiencia de los SGSI. El enfoque práctico y de medición, así como la orientación hacia los objetivos de negocio de la organización, es lo

que diferencia este modelo del resto de los estándares relacionados con la seguridad de la información [37].

Se adapta tanto a organizaciones maduras como a emergentes mediante sus cinco niveles de madurez, los cuales se adecuan a los objetivos de seguridad de la organización y a los recursos que están disponibles.

1.3.3 Proyecto de Seguridad de Aplicaciones Web Abiertas (OWASP)

El Proyecto de Seguridad de Aplicaciones Web Abiertas (*OWASP*, por sus siglas en inglés) es una organización sin fines de lucro a nivel mundial enfocada en mejorar la seguridad del software. Su misión es hacer visible la seguridad del software, para que las personas y las organizaciones sean capaces de tomar decisiones al respecto. OWASP está en una posición favorable para proporcionar información imparcial y práctica sobre aplicaciones seguras a individuos y organizaciones [38].

Emite herramientas de software y documentación basadas en el conocimiento sobre la seguridad de las aplicaciones [38]. Como parte de estas herramientas expone cada cierto tiempo el Top 10 de riesgos más críticos y el Top 10 de controles proactivos a tener en cuenta en las aplicaciones de software. El objetivo de estos programas es crear conciencia sobre la seguridad de la aplicación al describir las áreas de preocupación más importantes en las que los desarrolladores de software deben estar conscientes [7; 39].

En el Top 10 de Controles Proactivos [7; 39] se describe una lista de conceptos de seguridad que debe incluirse en cada proyecto de desarrollo de software de aplicaciones web. Los controles se ordenan por orden de importancia [7; 40].

1. Verificación de la seguridad temprana y frecuentemente
2. Parametrización de consultas
3. Codificación de datos
4. Validación de todas las entradas
5. Implementación de controles de identidad y autenticación
6. Implementación de controles de acceso apropiados

7. Protección de datos
8. Implementación del registro y la detección de intrusos
9. Aprovechamiento de los marcos de seguridad y bibliotecas
10. Tratamiento de errores y excepciones

La verificación de la seguridad temprana y frecuentemente (Control 1 del Top10 de Controles Proactivos) propone que desde el proceso de concepción del software se tengan en cuenta los requisitos de seguridad mientras se describen los requisitos del sistema, siempre teniendo en cuenta el resto de los controles propuestos. De igual manera propone verificar la seguridad con anticipación y a menudo en el proceso de desarrollo, ya sea a través de pruebas manuales o de pruebas y análisis automatizados.

Estos controles se encuentran relacionados con los riesgos definidos en el Top 10 de riesgos más críticos [41], y para minimizar las vulnerabilidades que provocan se definen requisitos que pueden estar presentes ante cada riesgo para cada uno de los controles.

	A1-Injection	A2-Broken Authentication and Session Management	A3-Cross-Site Scripting (XSS)	A4-Insecure Direct Object References	A5-Security Misconfiguration	A6-Sensitive Data Exposure	A7-Missing Function Level Access Control	A8-Cross-Site Request Forgery (CSRF)	A9-Using Components with Known Vulnerabilities	A10-Unvalidated Redirects and Forwards
C1: Verify for Security Early and Often	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C2: Parameterize Queries	✓									
C3: Encode Data	✓		✓							
C4: Validate All Inputs	✓		✓							✓
C5: Implement Authentication Controls		✓								
C6: Implement Appropriate Access Controls				✓			✓			
C7: Protect Data						✓				
C8: Implement Logging and IDs	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C9: Leverage Security Frameworks	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
C10: Error and Exception Handling	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Figura 1 Mapeo de los Controles Proactivos 2016 con el Top 10 de Riesgos.

Fuente: [39]

Teniendo en cuenta la criticidad de la SI en las organizaciones y las definiciones de las normas internacionales, se han aprobado estándares y resoluciones adaptadas al contexto nacional cubano. Estas regulaciones garantizan determinados aspectos de SI en el desarrollo de software.

1.4 Normas cubanas de seguridad informática

Los esfuerzos por informatizar esferas del desarrollo científico - técnico, económico, político y social, así como el surgimiento de nuevos riesgos asociados principalmente con el uso de las redes de datos de alcance global, ha propiciado que en Cuba se adopten medidas de tipo legal que permiten regular la SI.

La Oficina de Seguridad para las Redes Informáticas (OSRI), tiene como objeto social "*llevar a cabo la prevención, evaluación, aviso, investigación y respuesta a las acciones, tanto internas como externas, que afecten el normal funcionamiento de las tecnologías de la información del país*" [42]. Asegura el sistema de comunicaciones del país con los requisitos de máxima confiabilidad e independencia tecnológica, garantizando la infraestructura y los servicios para la seguridad y la defensa nacional.

Los sistemas informáticos pueden presentar dificultades y limitaciones a partir de las vulnerabilidades y debilidades que exterioricen. Para detectar y neutralizar oportunamente las posibles acciones enemigas en esta esfera, se estableció por el Ministerio de Comunicaciones (MINCOM) la Resolución 127: 2007, que instituye requisitos de seguridad en el empleo de las TIC a partir de criterios de racionalidad y utilidad. Dicho documento tiene por objetivo "*establecer los requisitos que rigen la seguridad de las TIC y garantizar un respaldo legal que responda a las condiciones y necesidades del proceso de informatización del país*" [30]. Estos requisitos son posibles de verificar y contribuyen a la disminución de los riesgos en la SI [30].

En Cuba, se cuenta además con la traducción normalizada por la Oficina Nacional de Normalización de la NC-ISO/IEC 27001: 2007. Esta fue elaborada por el Comité Técnico de Normalización NC/CTN 18 de Tecnología de la Información [43]. Es una adopción idéntica por el método de traducción de la Norma Internacional ISO/IEC 27001:2005 Information technology — Security techniques — Information security management systems — Requirements [43].

El Subcomité 7 – Ingeniería de Software y Sistemas (SC7) perteneciente al Comité Técnico Conjunto ISO/IEC No 1 (ISO/IEC JTC 1) – Tecnología de la Información, elaboró la Norma Ramal – Requisitos de la Calidad para Sistemas Informáticos y Productos de Software. Esta norma facilita la identificación de requisitos de seguridad y establece los requisitos mínimos a cumplir por los sistemas de software desarrollados en Cuba. El SC7 es integrante del Comité Técnico de Normalización No 18 – Tecnologías de la Información (CTN18).

El uso de estas normas, resoluciones y estándares, tanto nacionales como internacionales, contribuye a la definición de los requisitos para la implementación de un SGSI. En el desarrollo de software, atender la SI junto con los RF desde el inicio del proyecto, reduce los casos de conflicto, vulnerabilidades y encuentra formas de superarlos [19]. De esta manera se minimizan los riesgos asociados, en el proceso de desarrollo de software.

1.5 Ingeniería de software

Por su relevancia, es recomendable considerar la SI desde la concepción inicial de los sistemas de software y durante todo su ciclo de vida. En la definición de la IS destacan los siguientes conceptos:

- La aplicación práctica del conocimiento científico en el desarrollo y construcción de programas de computadoras y la documentación asociada requerida para desarrollar, operar y mantenerlos. [44]
- La disciplina tecnológica preocupada de la producción sistemática y mantenimiento de los productos de software que son desarrollados y modificados en tiempo y dentro del presupuesto definido [45]. En esta definición Fairley adiciona al concepto la sistematicidad dentro del proceso de desarrollo y la necesidad de hacerlo de una manera económica.
- La aplicación de un enfoque sistemático, disciplinado y cuantificable al desarrollo de operación y mantenimiento del software [46]. La IEEE coincide con Fairley en la sistematicidad del proceso y además añade la necesidad de cuantificarlo mediante la medición de indicadores.
- Es una disciplina o área de la informática o ciencia de la computación, que ofrece técnicas y métodos para desarrollar y mantener un software de calidad [47]. Pressman agrega a los anteriores conceptos el uso de herramientas y métodos para ejecutar los procesos con un enfoque de calidad [14].

En la IS se conoce como Ingeniería de Requisitos (IR), al acto de formalizar las actividades relacionadas con lograr la obtención, análisis, especificación, validación y gestión de los requisitos del sistema a desarrollar [14; 15]. La IR es crítica respecto al éxito o fracaso de numerosos proyectos informáticos y su gestión inadecuada incide negativamente en los costos y el cumplimiento de las fechas de entrega [48].

1.6 Ingeniería de requisitos

La Ingeniería de Requisitos (IR) es el conjunto de procesos, tareas y técnicas que permiten la definición y gestión de los requisitos de un producto, de un modo sistemático [15]. Incluye las actividades relacionadas con la determinación de las necesidades o de las condiciones a satisfacer para hacer un software nuevo o modificado. Varios autores consideran que es una colección estructurada de actividades, mediante las

cuales se obtienen, validan y mantienen documentados los requisitos del usuario y del sistema [14; 15; 49].

Pressman [14] plantea que un proceso sólido de IR ayuda a garantizar que se ha especificado un sistema que recoge las necesidades del cliente y cumple con sus expectativas. Identifica como parte de este proceso siete tareas fundamentales: inicio (identificación de la necesidad u oportunidad de negocio), elicitación, elaboración, negociación, especificación, validación y administración de requisitos [14].

Para Sommerville [15], la IR es el proceso de desarrollar una especificación del software que comunique las necesidades del sistema del cliente a los desarrolladores. Describe la IR en cuatro pasos, estos tratan de la evaluación de si el sistema es útil para el negocio (estudio de viabilidad); el descubrimiento de requisitos (obtención y análisis); la transformación de estos requisitos en formularios estándar (especificación), y la verificación de que los requisitos realmente definen el sistema que quiere el cliente (validación).

A partir de lo antes expuesto, se comprende para la investigación la IR como la disciplina que facilita los métodos y técnicas apropiados para entender las necesidades del cliente. Estas son analizadas confirmando su viabilidad, a través de una negociación razonable, especificada sin ambigüedad, y validada por las partes interesadas [50].

La parte más difícil de construir un sistema es precisamente saber qué construir, y establecer los requisitos técnicos detallados, incluyendo todas las interfaces con personas, máquinas y otros sistemas [14]. El término requisito puede conceptualizarse según lo planteado en la traducción certificada de la ISO 9000: 2000 como "*necesidad o expectativa establecida, generalmente implícita u obligatoria*" [13] de un cliente sobre el contenido, la forma o la funcionalidad de un producto. Pueden ser generados por las diferentes partes interesadas [12; 13].

Sommerville plantea que "*los requisitos para un sistema son la descripción de los servicios proporcionados por el sistema y sus restricciones operativas. Reflejan las necesidades de los clientes de un sistema que ayude a resolver algún problema como el control de un dispositivo, hacer un pedido o encontrar información*" [15; 51].

El Instituto de Ingeniería de Software (*SEI:* Software Engineering Institute) plantea como parte del glosario del Modelo de Madurez y Capacidad Integrado (*CMMI* por sus siglas en inglés) que un requisito es: (1) una condición o capacidad necesitada por un usuario para solucionar un problema o lograr un objetivo. (2) Una condición o capacidad que debe cumplir o poseer un producto o componente de producto para satisfacer un contrato, un estándar, una especificación u otros documentos impuestos formalmente. (3) Una representación documentada de una condición o capacidad como en (1) o en (2) [52].

"Los requisitos se asignan a las funciones del producto y a los componentes de productos, incluyendo objetos, personas y procesos" [52]. Varios autores realizan la clasificación de requisitos atendiendo a niveles y categorías.

1.6.1 Clasificaciones de requisitos

Sommerville clasifica los requisitos atendiendo a niveles y categorías. Los niveles atendiendo al grado de abstracción y las categorías de acuerdo a las característica o cualidades del sistema. Dichas categorías también están detalladas en la Guía del Cuerpo de Conocimiento de Ingeniería de Software (*SWEBOK*, por sus siglas en inglés) [15; 53]:

Requisitos del usuario: declaraciones, en lenguaje natural y en diagramas, de los servicios que se espera que el sistema proporcione y de las restricciones bajo las cuales debe funcionar. Son requisitos de un alto nivel de abstracción.

Requisitos del sistema: establecen con detalle las funciones, servicios y restricciones operativas del sistema. El documento de requisitos del sistema (algunas veces denominado especificación funcional) debe ser preciso y decir exactamente qué es lo que se va a implementar.

RF: especifican acciones que el sistema debe ser capaz de realizar, sin tomar en consideración ningún tipo de restricción física. Describen el comportamiento de entrada y salida del sistema y surgen de la razón fundamental de la existencia del producto. Indican características y restricciones sobre la funcionalidad del software. Definen el comportamiento interno del sistema.

RNF: son propiedades o cualidades que el producto debe tener, también son conocidos como requisitos o atributos de calidad. Debe pensarse en estas propiedades como las características que hacen al producto atractivo, usable, rápido o confiable; normalmente están vinculados a RF.

Los RF y los RNF, pueden expresarse en términos del cliente y pueden ser descripciones no técnicas [52]. Algunas de las categorías de RNF son: apariencia o interfaz externa, usabilidad, rendimiento, soporte, portabilidad, **seguridad**, privacidad, legales, confiabilidad, ayudas y documentación en línea, y hardware [54]. Estas categorías son relacionadas como características de calidad junto a sus sub-características dentro del modelo de calidad del producto que formaliza la ISO 25010 [16].

Los requisitos de seguridad, por su parte, son identificados según varios autores mediante una evaluación metódica de los **riesgos** de seguridad [7; 41; 43; 55]. Existen tres fuentes principales de requisitos de seguridad, una se deriva de **evaluar los riesgos**, teniendo en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial. Otra fuente son los **requisitos legales**, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural. Y una tercera es **el conjunto particular de principios, objetivos y requisitos comerciales** para el procesamiento de la información desarrollada por una organización para sostener sus operaciones [43].
Los requisitos de seguridad se derivan de los estándares de la industria, las leyes aplicables y un historial de riesgos y vulnerabilidades pasadas. Definen nuevas funciones o adiciones a las funciones existentes para resolver un problema de seguridad específico o eliminar una vulnerabilidad potencial. Proporcionan una base de la funcionalidad de seguridad vetada para una aplicación [5; 7; 56]. El alcance específico de la seguridad debe estar claramente definido por los interesados en términos de los activos a los que se aplica la seguridad y las vulnerabilidades contra las que se evalúa [57].
Para la adecuada gestión de los requisitos de software ya sean RF o RNF son utilizados normas y estándares. Estos rigen los procesos asociados a la IR durante todo el ciclo de vida del proyecto.

1.7 Estándares y normas para la gestión de requisitos

Los estándares y normas relacionados con los procesos de IR, establecen terminologías, técnicas y herramientas que contribuyen a una adecuada gestión de los requisitos de software. Pueden ser aplicables durante el ciclo de vida de un proyecto de software y en dependencia del modelo o metodología utilizada.

ISO 29148 – Ingeniería de sistemas y software - Procesos del ciclo de vida - Ingeniería de requisitos [58]: contiene prácticas para los procesos y productos relacionados con la IR a lo largo del ciclo de vida de proyectos de software que son de utilidad para la investigación. Define la construcción de un requisito, proporcionando atributos y características, y analiza la aplicación iterativa de los procesos de IR. Facilita una orientación adicional en la aplicación de los procesos de IR y la gestión de las actividades relacionadas en la norma ISO 15288.

ISO 15288 - Ingeniería de sistemas y software: procesos del ciclo de vida del sistema [59]: establece un marco común de procesos para describir el ciclo de vida de la IS y la terminología asociada desde un punto de vista ingenieril. Estos procesos se pueden aplicar en cualquier nivel de la estructura jerárquica de un sistema.

IEEE 830-1998 Prácticas recomendadas para la especificación de requisitos de software [60]: describe el contenido y las cualidades de una especificación de requisitos. Puede ser aplicada para ayudar en la selección de productos de software internos y comerciales. Define como características de una especificación de requisitos, que debe ser: correcto, sin ambigüedad, completo, consistente, clasificado por importancia y/o estabilidad, verificable, modificable, y traceable. Estas características son de utilidad para la investigación y necesarias para la gestión del ciclo de vida RNF de Seguridad, sobre todo ante la necesidad de mantener la trazabilidad hasta el fin del ciclo de vida del producto.

IEEE 1233-1998 Guía para desarrollar especificaciones de requisitos de sistema [61] proporciona una guía para el desarrollo de las especificaciones de requisitos, incluyendo su identificación, organización, presentación y modificación. De interés para la investigación, aborda las condiciones para incorporar conceptos operativos, restricciones de diseño y requisitos de configuración de diseño en la especificación. Esta guía también cubre las características y cualidades necesarias de los requisitos individuales y el conjunto de todos los requisitos.

NC ISO/IEC 25010:2016 Ingeniería de software y sistemas – Requisitos de la calidad y evaluación de software – Modelos de la calidad de software y sistemas (ISO/IEC 25010: 2011, IDT): define seis características de calidad y describe un modelo de proceso de evaluación del producto de software. La Seguridad se ha añadido como una característica, en lugar de una sub-característica de la Funcionalidad, con las sub-características de confidencialidad, integridad, no repudio, responsabilidad y autenticidad [62].

Esta norma es de un alto valor para la investigación ya que define las sub-características que se tienen en cuenta para la identificación del RNF de Seguridad.

Las normas ISO e IEEE son considerados estándares con alto grado de complejidad y se encuentran desagregadas en varios documentos [63], lo que dificulta la comprensión para su implementación por parte de los interesados, conllevando a un aumento en los esfuerzos y costos para preparar la documentación e implantación de los sistemas. Estos estándares especifican qué hacer en materia de la gestión de requisitos sin definir el cómo y no tienen en cuenta el tratamiento de los RNF de Seguridad, excepto la ISO 25010, que aporta sub-características en las que se pueden clasificar los RNF de Seguridad.

1.7.1 Modelo de Madurez y Capacidad Integrado (CMMI)

El modelo CMMI, es una colección de buenas prácticas que ayuda a las organizaciones a mejorar sus procesos. El mismo es desarrollado por equipos con miembros procedentes de la industria, del gobierno y del SEI. Las buenas prácticas del modelo se centran en las actividades para desarrollar productos y servicios de calidad con el fin de cumplir las necesidades de clientes y usuarios finales [52].

CMMI define 22 áreas de procesos concentradas en cuatro grandes grupos [52]: Gestión de procesos, Gestión de proyectos, Ingeniería y Soporte. Las áreas de proceso de Ingeniería cubren las actividades de desarrollo y mantenimiento que se utilizan en las disciplinas ingenieriles y se aplican al desarrollo de cualquier producto [52]:

- Integración del Producto (PI).
- Desarrollo de Requisitos (RD).
- Solución Técnica (TS).
- Validación (VAL).
- Verificación (VER).

Entre las áreas de Gestión de proyectos se encuentra Administración de Requisitos (*REQM*, por sus siglas en inglés), importante también en la IR y estrechamente relacionada con las del grupo ingenieril [52]. El proceso REQM trata directamente la planificación, el monitoreo, las inconsistencias y la trazabilidad de los

requisitos [52; 64]. De las áreas de procesos del grupo Ingeniería, es relevante para la investigación el RD por las definiciones hechas para la descripción y el desarrollo de los requisitos [52; 65].

Administración de requisitos REQM

El propósito de REQM es [52; 66] “gestionar los requisitos de los productos y los componentes de producto del proyecto, y asegurar la alineación entre esos requisitos, los planes y los productos de trabajo del proyecto”. Los procesos de REQM gestionan los requisitos recibidos o generados por el proyecto, incluyendo tanto los técnicos como los no técnicos, así como los impuestos al proyecto por la organización [63]. En particular si se implementa el área de proceso RD, sus procesos generan requisitos de producto y de componentes de producto que también son gestionados por REQM. El proceso REQM tiene una meta con cinco prácticas específicas [52]:

SG 1 Gestionar los requisitos.

SP 1.1 Comprender los requisitos.

SP 1.2 Obtener el compromiso sobre los requisitos.

SP 1.3 Gestionar los cambios a los requisitos.

SP 1.4 Mantener la trazabilidad bidireccional de los requisitos.

SP 1.5 Asegurar el alineamiento entre el trabajo del proyecto y los requisitos.

Este proceso es de relevancia para la investigación, ya que permite mediante su aplicación: gestionar los cambios a los requisitos a medida que evolucionan e identificar inconsistencias que ocurren entre los planes, los productos de trabajo y los requisitos. Mantiene la trazabilidad bidireccional entre los requisitos con los componentes del producto y otros productos de trabajo.

Desarrollo de requisitos RD

El propósito de RD es educir, analizar y establecer los requisitos de cliente, de producto y de componente de producto [52; 67]. Esta área de proceso tiene tres metas a cumplir y diez prácticas específicas [52]:

SG 1 Desarrollar los requisitos de cliente.

SP 1.1 Educir las necesidades.

SP 1.2 Trasformar las necesidades de las partes interesadas en requisitos de cliente.

SG 2 Desarrollar los requisitos de producto.

SP 2.1 Establecer los requisitos de producto y de componente de producto.

SP 2.2 Asignar los requisitos de componente de producto.

SP 2.3 Identificar los requisitos de interfaz.

SG 3 Analizar y validar los requisitos.

SP 3.1 Establecer los conceptos y los escenarios de operación.

SP 3.2 Establecer una definición de la funcionalidad y de los atributos de calidad requeridos.

SP 3.3 Analizar los requisitos.

SP 3.4 Analizar los requisitos para conseguir un equilibrio.

SP 3.5 Validar los requisitos.

El RD incluye las siguientes actividades [52]:

- Educción, análisis, validación y comunicación de las necesidades, expectativas y restricciones para obtener los requisitos priorizados del cliente.
- Recopilación y coordinación de las necesidades de las partes interesadas.
- Desarrollo de los requisitos en el ciclo de vida del producto.
- Establecimiento de los requisitos iniciales de producto y de componente de producto, consistentes con los requisitos de cliente.
- Establecimiento de los RF y de los RNF.

Como parte del proceso de mejora continua por el que apuesta, la actividad productiva de la UCI fue certificada con el nivel 2 de madurez de CMMI. Actualmente se encuentra en la definición y piloto de las áreas del nivel 3 para su posterior evaluación.

Por el análisis realizado en la investigación se ha confirmado la importancia que se le confiere a la identificación temprana de los requisitos de seguridad y su seguimiento durante el ciclo de vida del proyecto. Teniendo en cuenta que la actividad productiva de la UCI está certificada con el nivel 2 de madurez de CMMI y la utilidad de las definiciones para las áreas de procesos REQM y RD, se propone su uso para la elaboración de una guía que permita la gestión del RNF de Seguridad en el desarrollo de aplicaciones web. Para la propuesta de los requisitos se analizaron las definiciones de la ISO 25010 para la característica de calidad Seguridad [16] y el Top 10 de los diez riesgos más críticos en Aplicaciones Web de OWASP [41].

1.8 Conclusiones parciales del capítulo

En el presente capítulo se hace una revisión de términos y conceptos que son utilizados en la investigación, a partir de los cuales se arriban a las siguientes conclusiones:

- A partir del análisis de estándares internacionales y nacionales definidos en materia de SI, se corrobora la importancia de la identificación temprana de los requisitos de seguridad y el seguimiento de estos durante todo el desarrollo del ciclo de vida del proyecto.
- La correcta evaluación de los riesgos y los requisitos legales reguladores, estatutarios y contractuales que tienen que satisfacer una organización, son necesarios para una correcta identificación de los requisitos de seguridad.
- El análisis de las definiciones para las áreas de procesos REQM y RD, corroboró que no se analiza de forma explícita la gestión del RNF de Seguridad. Las responsabilidades de los roles no formalizan las tareas propias a desarrollar como parte de la gestión del RNF de Seguridad. No se tiene en cuenta dentro de las entradas y actividades de determinados procesos la documentación legal de la entidad referente a las políticas de SI, los riesgos y vulnerabilidades que puedan existir en su entorno y las sub-características de seguridad.
- La correcta interpretación de las sub-características de calidad y la identificación de los riesgos que puedan estar presentes en la actividad productiva, constituyen elementos relevantes que deben ser considerados en la identificación del RNF de Seguridad.

CAPÍTULO 2: GUÍA PARA LA GESTIÓN DEL REQUISITO NO FUNCIONAL SEGURIDAD EN APLICACIONES WEB

2.1 Introducción

Desde una perspectiva de seguridad, un sistema confiable es un sistema que cumple con requisitos de seguridad específicos [57]. En el presente capítulo se describe la guía desarrollada para la gestión del RNF de Seguridad, teniendo en cuenta las actividades que se deberán realizar en las disciplinas ingenieriles dentro del ciclo de vida de un proyecto, sus roles y artefactos. Se propone, además, una lista de requisitos para facilitar su identificación a partir del entorno de cada proyecto, asociados a riesgos que puedan presentarse y a las sub-características de seguridad de la ISO 25010.**2.2 Guía para la gestión del requisito no funcional Seguridad en el desarrollo de aplicaciones web**

La Mejora de Procesos de Software (MPS) tiene un carácter sistémico para mejorar el rendimiento de un sistema de procesos existente, a partir de desarrollar un conjunto de acciones que se manifiestan en modificaciones del proceso de desarrollo de software [68-70]. A continuación, se describe el proceso ingenieril teniendo en cuenta las definiciones hechas como parte del modelo CMMI para las áreas de procesos relacionadas, aunque para el alcance de la investigación solo se tendrán en cuenta las áreas REQM y RD.

2.2.1 Propósito

"*El propósito del grupo de Ingeniería es llevar a cabo el desarrollo de la solución, desde la obtención de los requisitos hasta la integración del producto y la entrega del mismo. Este grupo está integrado por las áreas de proceso Desarrollo de Requisitos (RD), Solución Técnica (TS), Integración de Producto (PI), Verificación (VER) y Validación (VAL)"* [52; 64; 67; 71]. Aunque REQM pertenece al grupo de gestión del proyecto, su propósito es "*es gestionar los requisitos de los productos y los componentes de producto del proyecto y asegurar la alineación entre esos requisitos, los planes y los productos de trabajo del proyecto*" [52; 63; 67; 71].

2.2.2 Roles

Como parte de las definiciones para la elaboración de la guía para la gestión de los RNF de Seguridad se analizaron los roles definidos en el grupo Ingenieril. Las responsabilidades de algunos de estos roles

fueron modificadas para lograr una adecuada gestión del RNF de Seguridad. Los roles definidos para estas actividades se describen a continuación [63; 67].

Analista:

- Participa con el cliente y el usuario final recopilando las entradas de los involucrados relevantes.
- Captura las necesidades de los clientes y las transforma en requisitos del cliente y del producto y define sus prioridades.
- Realiza la especificación de requisitos.
- Lleva a cabo las actividades del análisis.
- Desarrolla el modelo de análisis del sistema.
- Documenta el flujo de análisis.
- Participa en el diseño de la solución.
- Diseña las pruebas.
- Realiza el seguimiento de los requisitos durante todo el desarrollo del proyecto.
- Crea y actualiza las matrices de trazabilidad.
- Elabora el glosario de términos y el manual de usuario.

Además, asociado a la gestión del RNF de Seguridad este rol realiza las siguientes acciones:

- Participa en la elaboración del Plan de Administración de Requisitos.
- Determina los proveedores válidos de requisitos.
- Analiza los documentos legales de la entidad y el Plan de SI.

Proveedor de requisitos:

- Participa en los encuentros coordinados por los miembros del proyecto.
- Acepta la especificación de requisitos de software.

Además, asociado a la gestión del RNF de Seguridad este rol realiza las siguientes acciones:

- Provee los requisitos a los miembros del proyecto.
- Valida la especificación de requisitos de software.
- Participa en la definición de las prioridades, costo, tiempo y alcance de los requisitos de software.

Es necesario incluir al especialista en SI de la entidad cliente dentro de los involucrados relevantes, pues esta persona es la que domina los riesgos existentes del entorno y las posibles vulnerabilidades que se

deban mitigar en el sistema que se desarrollará. De igual manera validará que el sistema a desarrollar cumple con lo establecido en el Plan de SI.

Algunas de las competencias que debe cumplir un especialista de SI para ser considerado como proveedor de requisitos sobre temas de SI son: evaluar los riesgos de SI, y basado en estos diseñar, ejecutar y mantener políticas, medidas y sistemas de SI para su entidad; proveer un marco metodológico o políticas estandarizadas sobre SI para la entidad y sus proyectos; analizar y detectar amenazas de seguridad y desarrollar técnicas para su prevención [72; 73].

Arquitecto de información:

- Identifica la visión, misión y objetivos del producto, equilibrando las necesidades de la organización patrocinadora y la de su público.
- Realiza el estudio de homólogos para conocer el estado del arte del producto que se quiere desarrollar.
- Realiza la organización y representación de los contenidos a través de: definición de la taxonomía, diseño del sistema de navegación y diseño del sistema de etiquetado para el sistema de navegación.
- Realiza diagramación de diagramas tipos.

Además, asociado a la gestión del RNF de Seguridad este rol realiza las siguientes acciones:

- Realiza auditoría de información identificando las entidades de recursos de información conociéndose como: servicios, fuentes, sistema, contenidos.

Arquitecto de software:

- Define las herramientas, bibliotecas, componentes, marcos de trabajo y otros componentes que permitan acelerar y mejorar el trabajo del proyecto.
- Elabora el documento de arquitectura de software.
- Define de conjunto con el jefe de proyecto el flujo de desarrollo basado en las herramientas identificadas.
- Vela por el cumplimiento de los requisitos de hardware.
- Identifica componentes horizontales de la aplicación.
- Determina de conjunto con los diseñadores las interfaces de integración tanto internas como externas.

Además, asociado a la gestión del RNF de Seguridad este rol realiza las siguientes acciones:

- Analiza las vulnerabilidades de las posibles tecnologías a utilizar antes de aprobarlas.
- Define todos los elementos bases de la arquitectura del proyecto.
- Vela por la integración de los componentes del sistema.
- Identifica todos los posibles escenarios de despliegue de la aplicación.
- Analiza las vulnerabilidades de los posibles escenarios de despliegue.

Administrador de la calidad:

- Elabora el Plan de Aseguramiento de la Calidad.
- Participa en la elaboración del Plan de Monitoreo y en el monitoreo y análisis de las áreas de procesos.
- Guía el diseño y ejecución de las pruebas internas.
- Participa en el análisis y recolección de los datos para las mediciones.
- Coordina y colabora con las pruebas de liberación externa al proyecto.
- Crea una cultura de calidad en el proyecto.
- Guía, diseña y mantiene informados a los involucrados sobre el desarrollo de las pruebas.
- Revisa los defectos detectados por cada probador e informa al jefe de proyecto al terminar cada iteración.
- Concilia los defectos declarados “No Procede” con el Jefe de Proyecto, al finalizar cada iteración.
- Archiva la documentación generada en el proceso de prueba en la herramienta de gestión documental.
- Coordina y colabora con las pruebas de liberación externa al proyecto.
- Monitorea la solución de las no conformidades y solicitudes de cambio.

Además, asociado a la gestión del RNF de Seguridad este rol realiza las siguientes acciones:

- Elabora los planes de prueba.
- Participa en las revisiones técnicas formales de los artefactos.
- Participa en las revisiones con el cliente de los entregables.
- Vela por el cumplimiento de las políticas de la organización y reglas bases del proyecto.
- Realiza las revisiones de inconsistencias y monitorea las no conformidades hasta su cierre.

Administrador de la configuración:

- Planea junto al Jefe de proyecto el proceso de Administración de la configuración.
- Despliega la Administración de la configuración.
- Crea la Línea base.
- Revisa que las Solicitudes de cambios de mejora que llegan al proyecto no se hayan emitido anteriormente por otros interesados.
- Analiza el impacto de una solicitud de cambio de mejora.
- Agrega a la Solicitud de cambio de mejora emitida anteriormente el nombre del interesado.
- Registra las Solicitudes de cambios de mejora.
- Actualiza el estado de las Solicitudes de cambios de mejora.
- Informa a los interesados acerca del estado de la Solicitud de cambio de mejora.
- Comunica el estado de la configuración a los interesados.

Además, asociado a la gestión del RNF de Seguridad este rol realiza las siguientes acciones:

- Asegura la infraestructura para la Administración de la configuración.
- Identifica los elementos de configuración y líneas Base.

Jefe de proyecto:

- Desarrolla el Plan de desarrollo de software.
- Administra recursos.
- Participa en la legalización del proyecto.
- Realiza las estimaciones del proyecto.
- Define la organización del proyecto.
- Participa en las RTF.
- Participa en las revisiones de los entregables con el cliente.
- Participa en las revisiones con la alta gerencia.
- Administra la capacitación interna al proyecto.
- Evalúa a los miembros del proyecto según su desempeño.
- Gestiona las interacciones con clientes y usuarios.
- Genera y asigna acciones correctivas.
- Monitorea las acciones correctivas hasta su cierre.
- Realiza las pruebas de aceptación

Además, asociado a la gestión del RNF de Seguridad este rol realiza las siguientes acciones:

- Participa en la fase de estudio preliminar (visión general del proyecto, análisis de factibilidad, proyecto técnico).
- Aprueba la tecnología a usar en el desarrollo del proyecto.
- Monitorea la adherencia a procesos.
- Guía el proceso de identificación y mitigación de los riesgos.

Equipo de Desarrollo: se encarga de implementar los componentes de producto de acuerdo a los diseños realizados.

2.2.3 Guía para la gestión del Requisito No Funcional de Seguridad en el desarrollo de aplicaciones web

La guía para la gestión del RNF de Seguridad es un documento que contiene actividades, preferentemente basadas en modelos o procesos. Aporta documentos o artefactos de apoyo referentes a la SI y su fin está dirigido a la disminución de vulnerabilidades en el desarrollo de aplicaciones web, a través de una correcta gestión del RNF de Seguridad.

Las actividades que se proponen como parte de la guía se encuentran acorde al ciclo de vida de un proyecto de desarrollo de aplicaciones web. Las fases o disciplinas que se tienen en cuenta para la gestión del RNF de Seguridad llegan hasta las Pruebas de liberación, teniendo en cuenta que una vulnerabilidad detectada en el entorno de aceptación del cliente implicaría un aumento de los costes en su resolución. El escenario ideal sería tratar las vulnerabilidades en el momento de su aparición, es decir lograr con ellas una contención de fase.

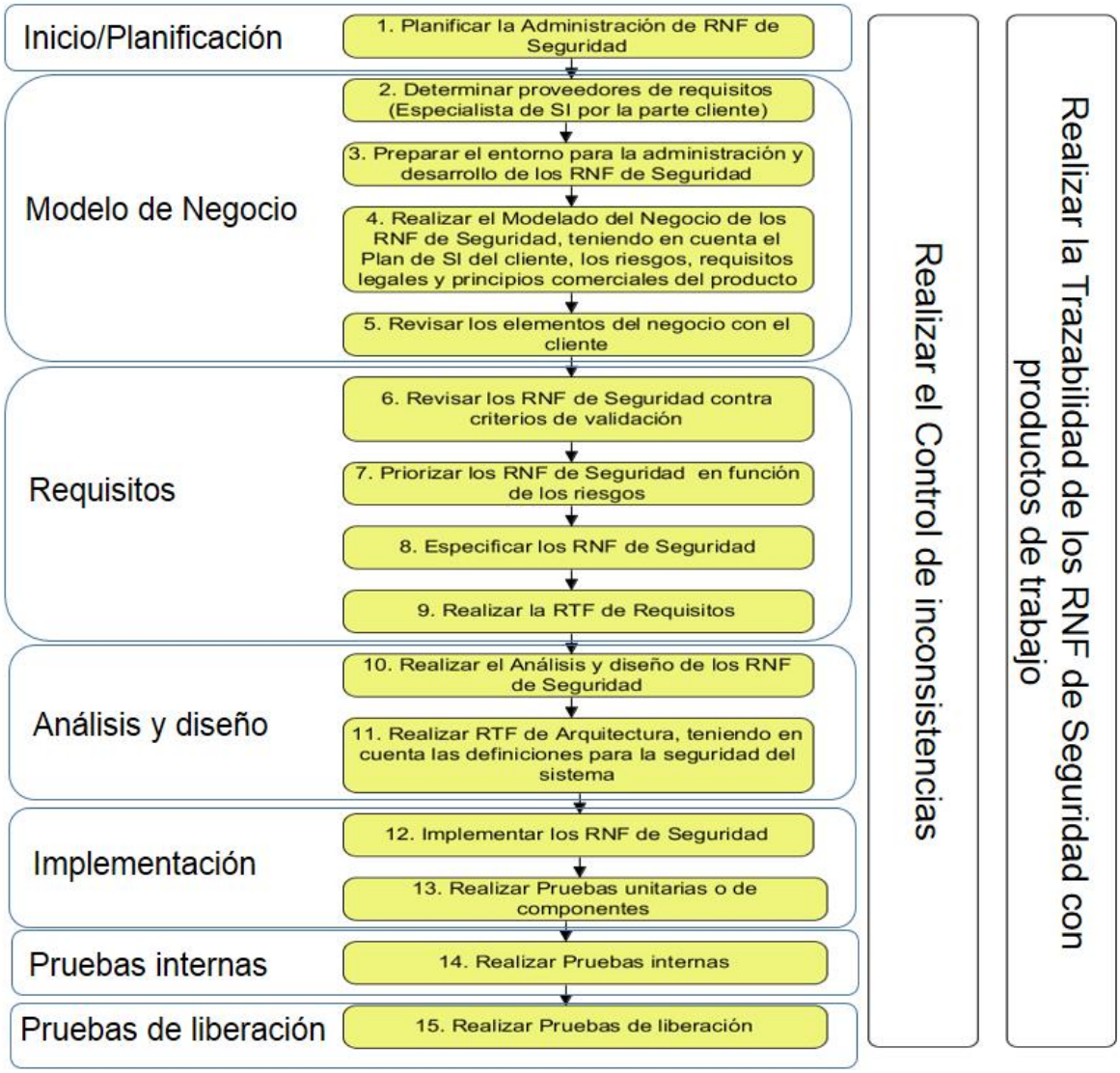


Figura 2 Guía para la gestión del RNF de Seguridad.
Fuente: Elaboración propia.

Tabla 1 Descripción de la guía para la gestión del RNF de Seguridad en aplicaciones web.
Fuente: Elaboración propia.

Etapa	Rol	Entrada	Actividad	Salida
Inicio / Planificación	Jefe de proyecto /	Acta de inicio del proyecto	1. Planificar la Administración de RNF de Seguridad.	Cronograma y Plan de

	Analista / Planificador		Actualiza las actividades concernientes a la administración de requisitos en el Cronograma de proyecto y las referentes a la capacitación del equipo de proyecto con respecto a los temas de SI necesarios para su gestión.	capacitación
Modelado de negocio	Jefe de proyecto / Analista / Proveedor de requisitos	Registro de proveedores de requisitos	2. Determinar proveedores de requisitos (Especialista de SI por la parte cliente). El cliente debe facilitar un catálogo de proveedores de requisitos. Nota: se debe tener en cuenta que es imprescindible que participe la persona encargada de los recursos informáticos del cliente o la persona responsable del **Plan de SI** o del SGSI entre los proveedores. Esta persona debe conocer qué **elementos** componen el entorno de despliegue, las **amenazas** y **riesgos** que lo pueden afectar y las **medidas** que se deben ejecutar para prevenirlas.	Registro de proveedores de requisitos
	Jefe de proyecto / Analista / Proveedor de	Plan de desarrollo de software	3. Preparar el entorno para la administración y desarrollo de los RNF de Seguridad. Se deben coordinar reuniones con el cliente (Jefe de Proyecto, Proveedor	Herramientas instaladas y configuradas. Plan de desarrollo de software.

	requisitos		de requisitos). Se debe facilitar el aseguramiento de los encuentros con el cliente. Preparar las herramientas, documentación y todo lo necesario para el entorno de gestión de los RNF de Seguridad. Las herramientas seleccionadas para el desarrollo deben tener una evaluación si son seguras o al menos identificadas las vulnerabilidades que presentan.	
	Analista / Proveedor de requisitos / Arquitectos	Registro de proveedores de requisitos Documentación del negocio entregada por el cliente (Plan de SI, riesgos de SI, requisitos legales, conjunto de principios, objetivos y requisitos comerciales) y **Lista de RNF**	4. Realizar el Modelado del Negocio teniendo en cuenta los RNF de Seguridad. Se debe recibir como insumo de la actividad la documentación del negocio si el cliente la proporciona (Analista, Proveedor de requisitos). Nota: entre la documentación de negocio entregada por el cliente al analista, se debe entregar por parte del especialista de SI, el Plan de SI del cliente, los riesgos, requisitos legales y principios comerciales del producto y las características tecnológicas del entorno de despliegue.	Modelo de negocio con CU Reglas de negocio Comedlo conceptual Glosario de términos

		de Seguridad propuesta para la guía.		
	Jefe de proyecto / Analista / Proveedor de requisitos	Descripción de procesos de negocio o Modelo de negocio con CU, Reglas del negocio, Modelo Conceptual o Mapa de procesos	5. Revisar los elementos del negocio con el cliente teniendo en cuenta la descripción del RNF de Seguridad. Se realiza la reunión para obtener la conformidad del cliente con los elementos del negocio. Se especifica en la Minuta de reunión si hay cambios sugeridos por parte del proveedor de requisitos. Si los cambios son de gran impacto para el proyecto se debe tramitar a través de una Solicitud de cambio.	Minuta de reunión Acta de aceptación del negocio.
Requisitos	Jefe de proyecto / Analista	Especificación de requisitos de software	6. Revisar los RNF de Seguridad contra criterios de validación. Se analizan los requisitos teniendo en cuenta los criterios de validación tanto para los requisitos del cliente como los requisitos del producto.	Criterios para validar los requisitos del cliente y del producto actualizados.
	Jefe de proyecto / / Analista / Arquitecto	Especificación de requisitos de software / Riesgos de seguridad	7. Priorizar los RNF de Seguridad en función de los riesgos Se deben priorizar los RNF de Seguridad teniendo en cuenta: Probabilidad*Impacto=Prioridad [74]	Especificación de requisitos de software
	Analista	Criterios para validar los requisitos del	8. Describir los RNF de Seguridad Se deben describir los RNF de Seguridad.	Especificación de requisitos de software

		cliente y del producto actualizados Especificación de requisitos de software.		actualizada.
	Analista / Equipo de revisores	Especificación de requisitos de software Lista de comprobación	9. Realizar Revisiones Técnicas Formales (RTF) de Requisitos Para la RTF se emplearán listas de comprobación que medirán la completitud técnica de los requisitos, y que no existan inconsistencias con los artefactos con que se relacionan.	Lista de comprobación Lista de defectos de los requisitos
Análisis y Diseño	Analista / Arquitectos	Especificación de requisitos de software	10. Realizar el Análisis y diseño de los RNF de Seguridad El diseño de la seguridad a nivel de sistema tiene que tomar en consideración, los servicios externos y las interconexiones entre sistemas.	Modelo de diseño
	Analista / Arquitectos / Equipo de revisores	Modelo de diseño Vistas de arquitectura	11. Realizar RTF de Arquitectura, teniendo en cuenta las definiciones para la seguridad del sistema. Para la RTF se emplearán listas de comprobación que medirán la completitud técnica de los diagramas del diseño y las vistas de arquitectura, especialmente las cuestiones referidas a los RNF de Seguridad.	Lista de comprobación Lista de defectos de los requisitos

Implementación	Equipo de proyecto / Arquitecto/ Administrador de configuración	Diagramas del diseño Estándares de codificación Entorno de desarrollo	12. Implementar los RNF de Seguridad El ambiente de desarrollo tiene que ser seguro, eso incluye las estaciones de trabajo, los servidores, dispositivos de red y repositorios de código.	Componentes codificados del producto
Pruebas unitarias	Analista / Desarrolladores / Administrador de calidad	Componentes codificados del producto	13. Realizar Pruebas unitarias o de componentes.	Lista de vulnerabilidades Componentes del producto actualizados
Pruebas internas	Analista / Desarrolladores / Equipo de pruebas	Componentes integrados del producto	14. Realizar Pruebas internas. El objetivo de las pruebas y el proceso de evaluación es verificar que el sistema desarrollado cumple con los requisitos funcionales y de seguridad.	Lista de vulnerabilidades Componentes del producto actualizados
Pruebas de liberación	Analista / Desarrolladores / Equipo de pruebas	Componentes integrados del producto	15. Realizar Pruebas de liberación. El objetivo de las pruebas y el proceso de evaluación es verificar que el sistema desarrollado cumple con los requisitos funcionales y de seguridad.	Lista de vulnerabilidades Componentes del producto actualizados

2.3 Propuesta de requisitos de seguridad para aplicaciones web

Los requisitos de seguridad proporcionan una base para la seguridad de una aplicación. Es preciso tener en cuenta para su correcta definición riesgos, requisitos legales y el conjunto particular de principios, objetivos y requisitos comerciales que son proporcionados por el cliente.

Se decide proponer un conjunto de requisitos de seguridad a tener en cuenta en el desarrollo de aplicaciones web. Para ello se tuvieron en consideración: los resultados de encuestas aplicadas a diversos roles inmersos en el desarrollo de software pertenecientes a varias áreas de la UCI, lo planteado por la Norma Ramal (NR) 2-1 Requisitos de la Calidad para Sistemas Informáticos y Productos de Software [75], los Diez riesgos más críticos en Aplicaciones Web de OWASP [41], y el Estándar de Verificación de Seguridad en Aplicaciones de OWASP [76]. Los requisitos fueron agrupados de acuerdo a los principales objetivos de seguridad o sub-características analizadas en la investigación [2].

Para la validación de los requisitos se utilizó la técnica de grupo focal. Esta técnica consiste en la realización de un análisis por grupos pequeños de personas, donde se expresan libre y espontáneamente acerca un tema [69].

En su aplicación se crearon dos pequeños grupos y se realizaron dos sesiones de trabajo. El debate fue guiado por un moderador y se registraron todos los criterios emitidos. Las guías de los encuentros se pueden consultar en el Anexo 2. Las sesiones de trabajo tuvieron como objetivo validar la lista de RNF de Seguridad propuesto a partir del análisis de los riesgos identificados por OWASP [41] y las sub-características de seguridad definidas en la ISO 25010 [16]. En la primera sesión el moderador presentó la propuesta de 35 requisitos identificados previamente teniendo en cuenta la bibliografía consultada y el resultado de las encuestas utilizadas en el diagnóstico inicial de la investigación. En esta sesión cada grupo refinó las propuestas de los RNF de Seguridad y realizaron recomendaciones al respecto. En la segunda sesión ambos grupos se reunieron para llegar a acuerdos sobre la propuesta de forma conjunta. Como resultado de este encuentro se decidió mantener los 35 requisitos propuestos a partir del análisis bibliográfico y agregar los siguientes dos requisitos, teniendo en cuenta las recomendaciones de los expertos:

- Cerrar automáticamente la sesión de un usuario cuando ha estado inactivo durante un cierto lapso de tiempo
- Destruir el identificador de sesión luego de salir o cerrar el sistema

Integridad:

- RNFS 1: utilizar marcos de trabajo que automáticamente previenen los ataques XSS (Cross-Site Scripting o inyección de código malicioso).
- RNFS 2: validar los datos que se reciben y velar por la integridad de los datos que se devuelven.
- RNFS 3: prevenir los ataques *CSRF* (del inglés Cross-Site Request Forgery o falsificación de petición en sitios cruzados).
- RNFS 4: evitar las inyecciones de código.
- RNFS 5: utilizar LIMIT y otros controles SQL para evitar la fuga masiva de datos en caso de inyecciones SQL.
- RNFS 6: realizar validaciones para la entrada de datos al servidor utilizando “listas blancas”.
- RNFS 7: cifrar los datos sensibles que sean almacenados.

Confidencialidad:

- RNFS 8: proteger las conexiones autenticadas o que involucren funciones o información relevante.
- RNFS 9: no mostrar referencias hacia objetos internos de la aplicación.
- RNFS 10: no se deben mostrar mensajes con información que ayude a recopilar información sobre el producto o las configuraciones del servidor.
- RNFS 11: evitar la elevación de privilegios en las cuentas de usuarios.
- RNFS 12: todos los elementos de la infraestructura deben ser revisados para asegurarse de que no contienen ninguna vulnerabilidad conocida, así como las herramientas administrativas usadas para el mantenimiento de los diferentes componentes.
- RNFS 13: no almacenar datos sensibles de manera innecesaria.
- RNFS 14: deshabilitar el almacenamiento en caché de datos sensibles.

Disponibilidad:

- RNFS 15: realizar estudio sobre las posibles vulnerabilidades que se puedan presentar en la tecnología a utilizar en el desarrollo.
- RNFS 16: utilizar tecnologías seguras para el desarrollo.
- RNFS 17: cumplir los requisitos exclusivos de los límites de negocio de las aplicaciones.
- RNFS 18: controlar el receptor de escucha de las Bases de Datos.

- RNFS 19: garantizar que el servidor no envíe directrices o cabeceras de seguridad a los clientes o que se encuentren configurados con valores inseguros.
- RNFS 20: actualizar las configuraciones apropiadas de la tecnología usada de acuerdo a las advertencias de seguridad y seguir un proceso de gestión de parches.
- RNFS 21: utilizar una herramienta para mantener un inventario y control de versiones de los componentes
- RNFS 22: utilizar componentes únicamente de orígenes oficiales y utilizando los canales seguros.
- RNFS 23: analizar riesgos y vulnerabilidades del entorno de despliegue del cliente atendiendo a sus características.

No repudio:

- RNFS 24: cifrar todos los datos en tránsito utilizando protocolos seguros.
- RNFS 25: identificar o firmar de forma única los mensajes intercambiados.
- RNFS 26: almacenar los mensajes intercambiados en ficheros logs para su posterior consulta.

Autenticación o Autenticidad:

- RNFS 27: no mantener contraseñas creadas por defecto, débiles o muy conocidas especialmente en el caso de los administradores del sistema.
- RNFS 28: definir mecanismos de autenticación personalizado para todos los usuarios del sistema.
- RNFS 29: no se deben utilizar cuentas suministradas por defecto.
- RNFS 30: no permitir ataques de fuerza bruta y/o ataques automatizados.
- RNFS 31: utilizar controles contra contraseñas débiles.
- RNFS 32: alinear la política de longitud, complejidad y rotación de las contraseñas establecidas.
- RNFS 33: limitar el tiempo de respuesta de cada intento fallido de inicio de sesión.
- RNFS 34: controlar el ciclo de vida de las contraseñas.
- RNFS 35: un usuario estándar (no administrador) no debe tener acceso a modificar sus privilegios en la aplicación o los de otro usuario con su mismo rol.
- RNFS 36: cerrar automáticamente la sesión de un usuario cuando ha estado inactivo durante un cierto lapso de tiempo.
- RNFS 37: destruir el identificador de sesión luego de salir o cerrar el sistema.

A continuación, se muestran las relaciones entre los requisitos y los riesgos identificados por un equipo de investigadores de OWASP [41] en el Top 10 - Los diez riesgos más críticos en Aplicaciones Web del año 2017 (Ver Tabla 5). Aunque se definen requisitos que no se encuentran directamente relacionados con los riesgos, mitigan la aparición de vulnerabilidades que pueden estar presentes en el desarrollo de las aplicaciones web y atentar contra la seguridad del producto final.

Tabla 2 Relación entre riesgos/vulnerabilidades y requisitos.

Fuente: Elaboración propia.

Riesgos/Vulnerabilidades	**Requisitos que se relacionan**
Inyección	RNFS 1, RNFS 2, RNFS 3, RNFS 4, RNFS 5, RNFS 6
Pérdida de autenticación	RNFS 27, RNFS 28, RNFS 29, RNFS 30, RNFS 31, RNFS 32, RNFS 33, RNFS 34, RNFS 35, RNFS 36, RNFS 37
Exposición de datos sensibles	RNF 7, RNFS 13, RNFS 14
Entidades externas XML	RNFS 6
Pérdida de control de acceso	RNFS 11, RNFS 17, RNFS 35
Configuración de seguridad incorrecta	RNFS 15, RNFS 16, RNFS 19, RNFS 20, RNFS 22
Ataques de XSS (Cross-Site Scripting)	RNFS 1, RNFS 2,
Uso de componentes con vulnerabilidades conocidas	RNFS 19, RNFS 20, RNFS 21, RNFS 22, RNFS 23

Con la identificación preliminar de los requisitos expuestos en la investigación, se pretende que el uso de estos contribuya a elevar el conocimiento en materia de SI y la calidad en el desarrollo de aplicaciones web. La gestión del RNF de Seguridad se garantiza desde etapas tempranas del desarrollo del producto, gracias a la tipificación de riesgos y/o vulnerabilidades que pueden estar presentes tanto en el entorno del cliente como en el equipo de desarrollo.

Para una correcta identificación de los RNF de Seguridad se tienen en cuenta aspectos legales que igualmente deben garantizarse y que se pueden ver reflejados en los requisitos presentados en la investigación. Los requisitos propuestos deben formar parte de los resultados obtenidos desde la concepción de los procesos de negocio, mantener la trazabilidad con los elementos que se relacionan, y

monitoreados a medida que el desarrollo del sistema evolucione. Estas acciones contribuyen a la disminución de las posibles vulnerabilidades que pudiera tener el producto final.

2.4 Adaptación de la guía para la gestión del RNF de Seguridad a los procesos definidos en la Universidad de las Ciencias Informáticas

Teniendo en cuenta la MPS y las definiciones realizadas para las áreas de procesos de REQM y RD en la Universidad de las Ciencias Informáticas, se decidió adaptar la guía para la gestión del RNF de Seguridad para su aplicación en el desarrollo de aplicaciones web. En la aplicación de la adaptación de la guía, se consideran los riesgos [41] y las sub-características de seguridad [16] y se modifican los procesos REQM y RD, agregando entradas y salidas a determinadas actividades en función de lograr una adecuada gestión de los RNF de Seguridad [2].

A continuación, se detallan las modificaciones realizadas a determinadas actividades de los subprocesos de las áreas REQM y RD que corresponden de manera específica a la gestión de los RNF de Seguridad en el desarrollo de aplicaciones web en la UCI [2].

Tabla 3 Modificaciones al IPP Administración de Requisitos.
Fuente: Elaboración propia.

IPP Administración de Requisitos		
Criterios de entrada	Firma del Acta de Inicio del proyecto o servicio y Oferta o Ficha técnica.	
Criterios de salida	Firma del Acta de terminación del Proyecto.	
Actividad	Descripción	Salidas
2. Determinar proveedor de requisitos.	El cliente debe facilitar un catálogo de proveedores de requisitos. (Proveedor de requisitos) Nota: se debe tener en cuenta que es imprescindible que participe la persona encargada de los recursos informáticos del cliente o la persona responsable del Plan de SI o del SGSI entre los proveedores. También se debe contar con personal que pertenezca a departamentos o grupos importantes en la definición de los requisitos, como: clientes, usuarios finales, políticas, normativas,	Registro de proveedores de requisitos

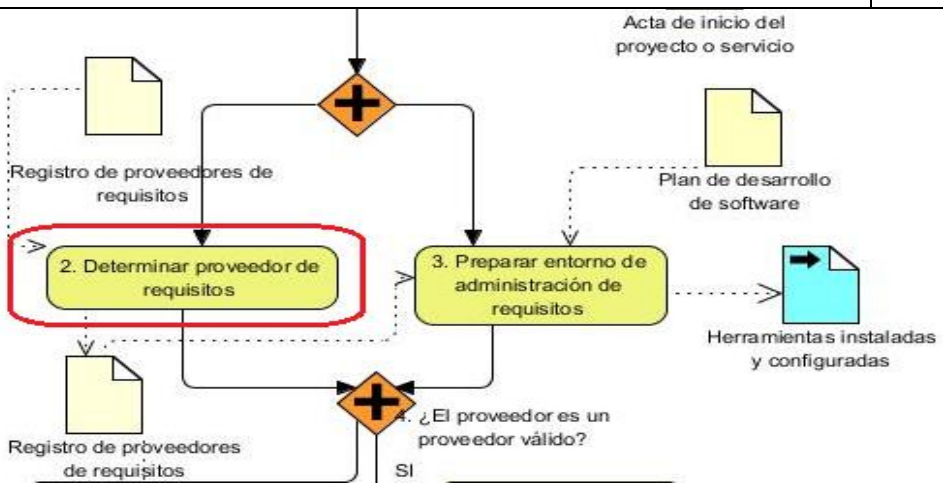
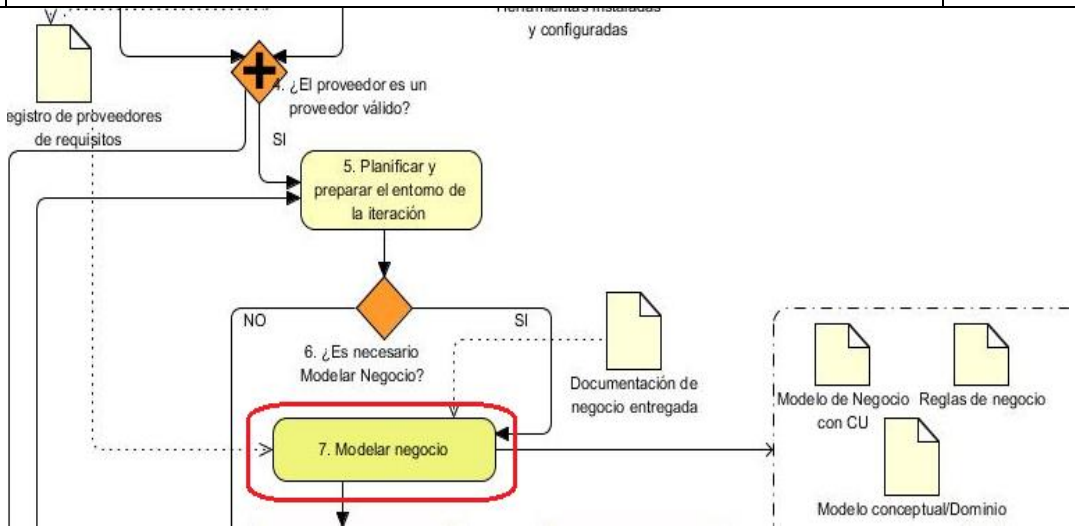
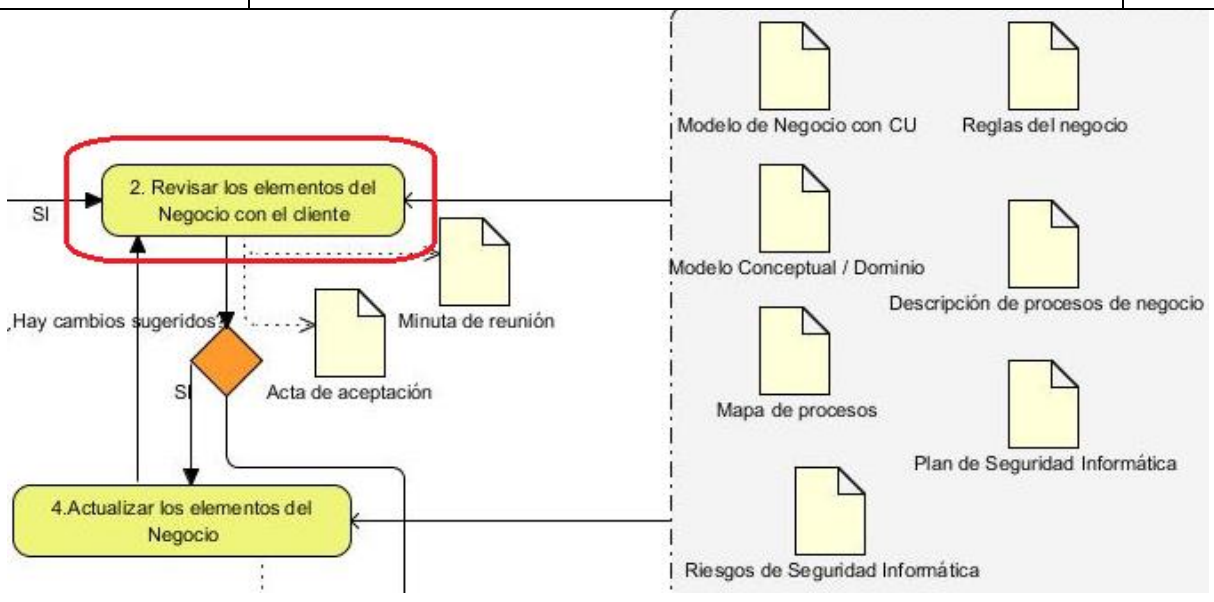
	grupos de sistemas, grupos de calidad.	
		
7. Modelar negocio	Recibir documentación del negocio si el cliente la proporciona. (Analista, Proveedor de requisitos) Nota: entre la documentación de negocio entregada por el cliente al analista, se debe entregar por parte del especialista de SI, el Plan de SI y las características tecnológicas y posibles riesgos y vulnerabilidades que pueda presentar el entorno de despliegue.	Modelo de negocio con CU Modelo conceptual /Dominio Reglas de negocio Glosario de términos
		

Tabla 4 Modificaciones al IPP Entendimiento y compromiso.
Fuente: Elaboración propia.

IPP Entendimiento y compromiso		
Criterios de entrada	Descripción de procesos de negocio o Modelo de negocio con CU /Modelo conceptual/dominio/Reglas de negocio/Especificación de requisitos de software/Descripción de requisitos/Especificación de CU, Plan de SI, Lista de riesgos/vulnerabilidades de SI del cliente, Lista de RNF de Seguridad propuestos.	
Criterios de salida	Acta de Aceptación/Minuta de reunión.	
Actividad	Descripción	Salidas
2. Revisar elementos del negocio con el cliente.	Se revisan los elementos de negocio con el cliente teniendo como entradas: Descripción de procesos de negocio o Modelo de negocio con CU, Reglas del negocio, Modelo conceptual/dominio -Mapa de proceso, Plan de SI, Lista de riesgos/vulnerabilidades de SI del cliente, Lista de RNF de Seguridad propuestos.	Minuta de reunión Acta de aceptación (firmada)

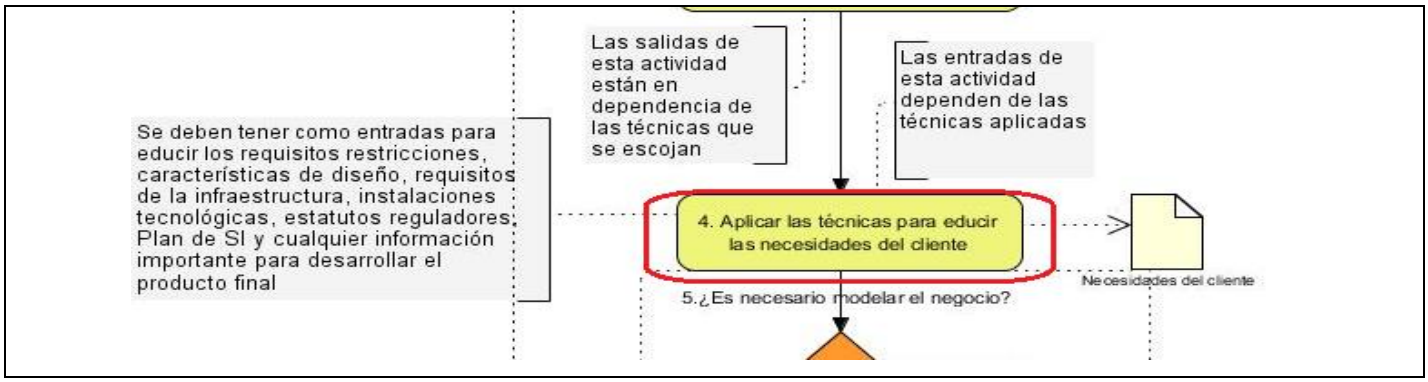


A los subprocesos IPP Traceo e IPP Control de inconsistencias [67] no es necesario modificarles ninguna entrada, actividad o salida, pues las que se encuentran descritas son adecuadas para complementar la gestión del RNF de Seguridad. Específicamente en el caso del proceso de Traceo, se encuentran definidas matrices que relacionan los requisitos con artefactos del proyecto, requisitos con conceptos, requisitos con casos de uso del negocio, requisitos con procesos de negocio, requisitos con casos de uso del sistema, requisitos con historias de usuario, requisitos con diagramas de clases del diseño, requisitos con diseños de casos de pruebas, requisitos con paquetes funcionales codificados, requisitos con componentes. Al estar estas matrices enfocadas a los requisitos de forma general, aplican para el seguimiento del RNF de Seguridad.

Así como se hacen ajustes a determinados elementos de las definiciones del área REQM, se varían aspectos en el área de proceso RD, específicamente en el IPP Gestión de requisitos del cliente.

Tabla 5 Modificaciones al IPP Gestión de requisitos del cliente.
Fuente: Elaboración propia.

IPP Gestión de requisitos del cliente		
Criterios de entrada	Acta de inicio del proyecto. Documento de educción de necesidades del cliente. Necesidades del cliente. Catálogo de proveedores.	
Criterios de salida	Cronograma de proyecto. Necesidades del cliente. Criterios para validar requisitos del cliente. Registro de proveedores de requisitos. Prioridad de requisitos del cliente.	
4. Aplicar las técnicas para educir las necesidades del cliente	Entrevistar a las partes interesadas, haciendo mayor énfasis en los proveedores que resultaron aceptados, y aplicar las técnicas para recopilar las necesidades, expectativas, restricciones, características de diseño, requisitos de la infraestructura, instalaciones tecnológicas, estatutos reguladores, Plan de SI y cualquier información importante para desarrollar el producto final. (Analista, Arquitecto de software, Arquitecto de Información).	Necesidades del cliente



2.5 Conclusiones parciales del capítulo

En el presente capítulo se concluye que:

- Se elaboró la guía para la gestión del RNF de Seguridad, teniendo en cuenta las fases del ciclo de vida del software y detallando las entradas y salidas para cada una de las actividades definidas, para beneficiar la gestión del RNF de Seguridad y lograr una disminución de las vulnerabilidades en el desarrollo de aplicaciones web.
- La correcta interpretación de las sub-características de seguridad definidas en la ISO 25010 y los riesgos más críticos propuestos por OWASP en el año 2017, favorecieron la identificación de una lista de RNF de Seguridad que contribuye a disminuir las vulnerabilidades en los desarrollos de aplicaciones web
- A partir de las definiciones hechas en las áreas de procesos de REQM y RD del modelo CMMI para la UCI, se realizaron las modificaciones necesarias para lograr una correcta gestión del RNF de Seguridad y así lograr una disminución de las vulnerabilidades en el desarrollo de aplicaciones web.
- La elaboración de una guía para la gestión del RNF de Seguridad en las aplicaciones web, a partir de los procesos de REQM y RD, favorece la gestión del RNF de Seguridad en los proyectos de desarrollo de la UCI.

CAPÍTULO 3: VALIDACIÓN DE LA INVESTIGACIÓN

3.1 Introducción del capítulo

En el capítulo se describe el proceso de validación diseñado y los resultados alcanzados. El proceso de validación de la solución se constituye por: la aplicación del método de expertos Delphi para valorar la contribución de la guía propuesta en la solución del problema, el análisis de los resultados del efecto de la implementación de la guía a partir de un estudio de caso y la aplicación de la técnica de Iadov para medir el grado de satisfacción del cliente respecto a la guía desarrollada para la gestión del RNF de Seguridad, así como de los requisitos propuestos, su utilidad y aplicabilidad en entornos reales.

3.2 Proceso de validación

El problema de la investigación parte de la necesidad de gestionar los RNF de Seguridad con el fin de disminuir el número de vulnerabilidades en las aplicaciones web desarrolladas en la UCI, considerando los riesgos y las sub-características de seguridad. La solución propuesta se centra en la elaboración de una guía para la gestión del RNF de Seguridad y se presenta una lista de RNF de Seguridad que facilita la identificación de estos requisitos en los proyectos de desarrollo de aplicaciones web. Para comprobar la hipótesis de la investigación, se realizó la validación de la guía y los requisitos propuestos, utilizando el método Delphi, un estudio de caso y la técnica Iadov.

Los métodos de validación para investigaciones científicas en la rama de la informática, se enfocan en demostrar la relevancia del problema que resuelve y el rigor con que fueron construidos [77-79], para garantizar la incorporación de una contribución científica al sustento de la propuesta [69]. Una vez demostrada la valía de la investigación, es importante valorar la satisfacción de los clientes para con la propuesta [69; 80; 81]. En la validación de la presente investigación los métodos empleados también fueron utilizados en tesis doctorales y de maestría relacionadas con SI y calidad de software [25; 69; 82-84] que proponen el empleo de: encuestas, consultas a expertos y técnica Iadov. El proceso de validación de la investigación se concibió de la siguiente manera:

- Encuesta a expertos mediante el método Delphi para obtener las consideraciones sobre la contribución de la guía y la propuesta de los RNF de Seguridad, con el fin de disminuir el número de vulnerabilidades en las aplicaciones web desarrolladas en la UCI.

- Estudio de caso para obtener las diferencias a partir de la comparación del número de vulnerabilidades en un proyecto, antes y después de la aplicación de la guía para la gestión del RNF de Seguridad y la lista de requisitos propuestos para ello.
- Encuesta a los clientes y técnica de Iadov para valorar la aplicabilidad y utilidad de la de la guía y la propuesta de los RNF de Seguridad en entornos reales y medir la satisfacción de los clientes.

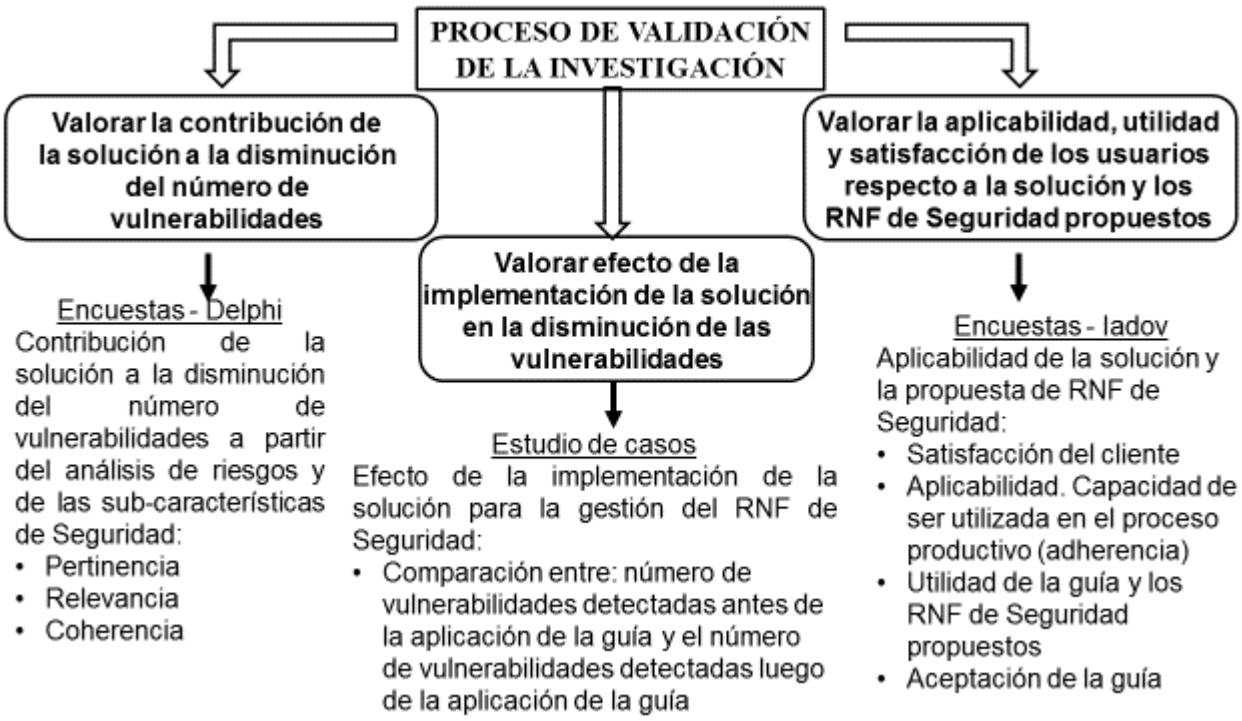


Figura 3 Proceso de validación de la investigación.
Fuente: Elaboración propia.

3.2.1 Contribución de la solución a la disminución del número de vulnerabilidades en las aplicaciones web desarrolladas en la UCI

La valoración de la contribución de la solución a la disminución del número de vulnerabilidades en las aplicaciones web desarrolladas en la UCI, mediante el uso del análisis de riesgos y de las sub-características de seguridad, se realizó aplicando los métodos Delphi y encuesta, para obtener el criterio de los expertos. El método Delphi consiste en la selección de un grupo de expertos a los que se le pregunta su opinión sobre cuestiones referidas a acontecimientos futuros. Este procedimiento extrae y

maximiza las ventajas que presentan los métodos basados en grupos de expertos y minimiza sus contratiempos [85; 86].

En la aplicación del método se tuvieron en cuenta expertos que tuviesen al menos 5 años de experiencia en la industria del software, de modo que contaran con la capacidad de hacer recomendaciones, detectar insuficiencias y valorar los aspectos de la propuesta de solución.

Para la selección de los expertos se siguieron los siguientes pasos:

1. Determinar las áreas del conocimiento que deben dominar los expertos: los expertos deben tener conocimientos sobre las áreas de procesos REQM y RD, SI, riesgos que afectan la SI y las sub-características de seguridad.
2. Elaborar la lista de expertos candidatos: a partir de las áreas del conocimiento que deben dominar los expertos se identifican los candidatos.
3. Obtener el compromiso de participación de los candidatos a expertos: la muestra del grupo de candidatos a expertos estuvo conformada inicialmente por 15 personas de las cuales 13 acordaron participar en la validación.
4. Determinar el coeficiente de experticia: se aplicó una encuesta de autovaloración. El coeficiente de experticia (K) se determina por la opinión del encuestado acerca de su nivel de conocimiento en al área de conocimiento que se evalúa [86; 87], lo cual se refleja en la ecuación 1:

$$K = \frac{k_c + k_a}{2} \quad (1)$$

Donde:

K = coeficiente de experticia.

k_c = coeficiente experticia o conocimiento que tiene el experto en el tema.

k_a = coeficiente de argumentación o fundamentación de los criterios del experto.

El resultado del coeficiente K se analiza de la siguiente forma:

- Si 0,8 ≤ K < 1,0 el coeficiente de experticia es alto.
- Si 0,5 ≤ K < 0,8 el coeficiente de experticia es medio.
- Si K < 0,5 el coeficiente de experticia es bajo.

A partir de los resultados obtenidos durante la encuesta de autovaloración se determinó que de los 13 encuestados, 9 cumplían la condición de experticia requerida para la validación del tema, desechándose aquellos que tenían experticia baja en al menos un área de conocimiento. Se aceptaron los que tuvieron experticia media en una sola área de conocimiento (como máximo) y experticia alta en el resto. Los resultados de este análisis se muestran en el Anexo 3.

Entre los expertos seleccionados figuran personas que estuvieron involucradas en el diagnóstico inicial de la investigación, personal de la Dirección de Calidad de Software (DCS) y de la Dirección de Seguridad Informática (DSI) de la UCI. Una vez identificados los expertos se procedió a aplicar la encuesta de validación del proceso (ver Anexo 4). Los resultados del procesamiento de las encuestas de validación se muestran a continuación.

En cuanto a la **relevancia** de la guía propuesta, el criterio de los expertos para cada uno de los aspectos que se evaluó en el rango de Muy Adecuado (MA), Bastante Adecuado (BA) y Adecuado (A), la media de estos valores fue de: 87.6%, 11,0%, 1.4% respectivamente.

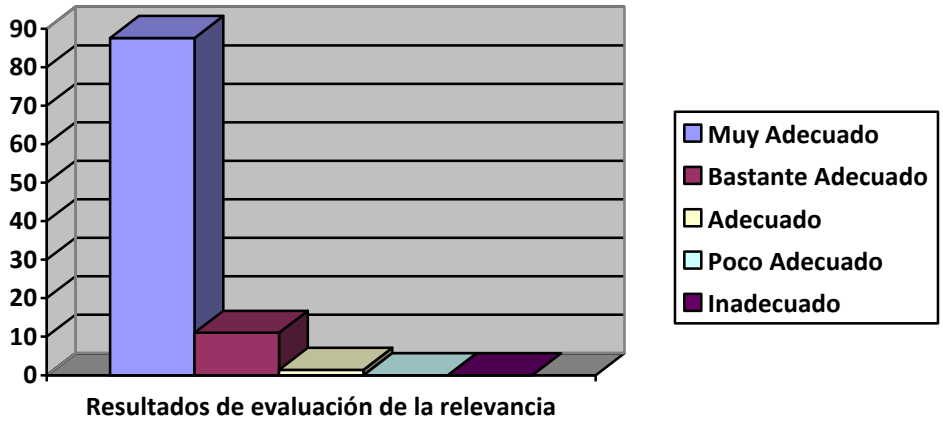


Figura 4 Resultados de la evaluación de la relevancia.

Fuente: Elaboración propia.

En el caso de la **pertinencia** de la guía las evaluaciones fueron 89% Muy Adecuado y un 11% Bastante Adecuado. Los resultados obtenidos en la validación de la pertinencia del proceso se muestran a continuación.

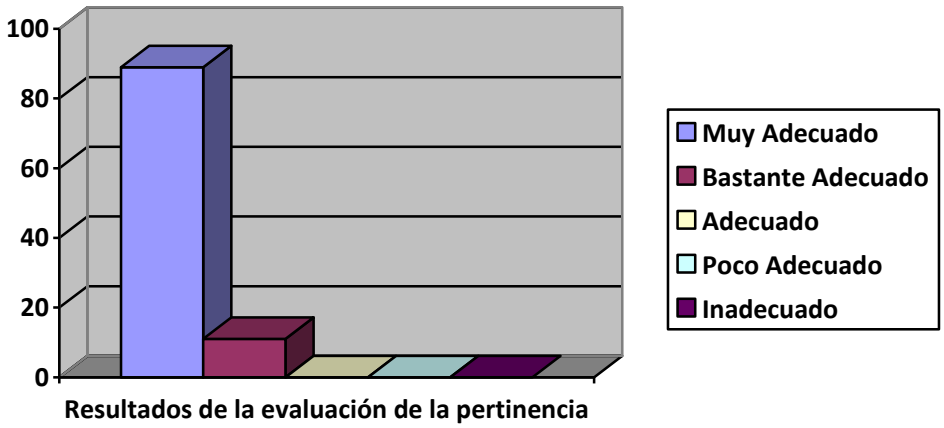


Figura 5 Resultados de la evaluación de la pertinencia.
Fuente: Elaboración propia.

Respecto a la **coherencia**, las evaluaciones para Muy Adecuado y Bastante Adecuado fueron del 100,00% (87,50% y 12,50% respectivamente). Los resultados obtenidos en la validación de la coherencia del proceso se muestran a continuación.

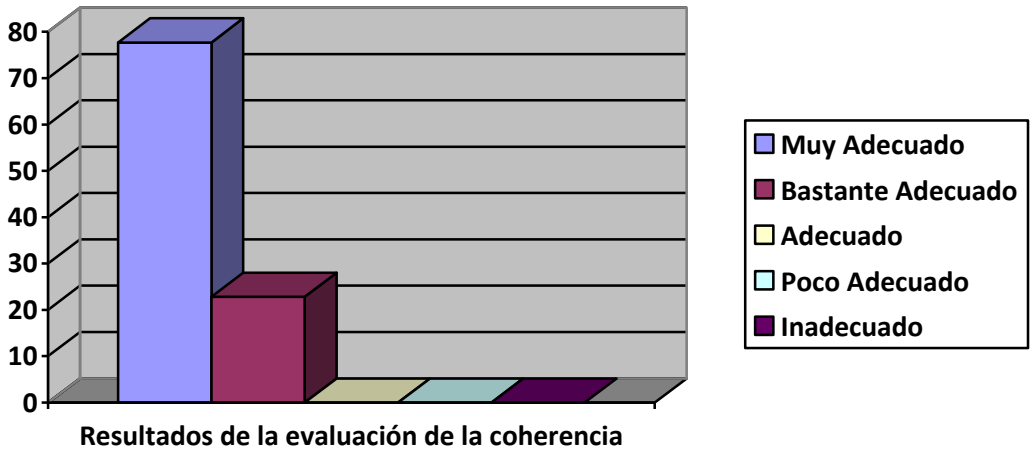


Figura 6 Resultados de la evaluación de la coherencia.
Fuente: Elaboración propia.

Entre los criterios emitidos por los expertos como resultado de la pregunta 4 de la encuesta, se señalaron como elementos positivos:

- La inclusión del especialista de SI dentro de las personas que figuran como proveedores de requisitos, contribuye a que los aspectos relacionados con los riesgos y las vulnerabilidades del entorno sean tenidas en cuenta para la identificación de los RNF de Seguridad.
- Tener en cuenta como parte de las entradas para el Modelado de Negocio los documentos legales del cliente y aquellos que norman las políticas de SI, favorece la identificación de los RNF de Seguridad.
- Como parte de los documentos entregados por el cliente se cuenta con una lista de riesgos y vulnerabilidades existentes en el entorno del cliente final, lo que facilita la identificación de RNF de Seguridad.
- Se analizan las sub-características de seguridad y sus definiciones según la norma ISO 25010, lo que contribuye a la clasificación de los RNF de Seguridad.
- Las modificaciones hechas a los procesos de REQM y RD beneficia la gestión de los RNF de Seguridad.

Así como se emitieron criterios positivos sobre la guía, se identificaron las siguientes sugerencias y recomendaciones por parte de los expertos:

- Identificar métricas de SI que permitan realizar análisis sobre indicadores de interés para la organización, teniendo en cuenta las vulnerabilidades más frecuentes.
- Desarrollar una herramienta que implemente métricas relacionadas con la SI y contribuya a la toma de decisiones de la organización.

3.2.2 Valorar el efecto de la implementación de la guía en la disminución de las vulnerabilidades

Se decidió aplicar un estudio de caso en el proyecto Desarrollo de Sistema de Planificación de Actividades XIPAC 3.0 del Centro de informatización de Entidades (CEIGE), para valorar el efecto de la implementación de la guía. Este análisis permitió obtener las diferencias respecto al número de vulnerabilidades identificadas en diferentes iteraciones, a partir de la comparación del número de NC resultante en el proceso de pruebas de liberación a nivel de centro. En una primera iteración del desarrollo no se tuvo en cuenta la aplicación de la guía. En la segunda iteración del proyecto se aplicó la guía para la

gestión del RNF de Seguridad y la lista de requisitos propuestos, en el desarrollo de las nuevas funcionalidades definidas por el cliente para el alcance de esta iteración.

El Sistema de Planificación de Actividades (SIPAC) está destinado a facilitar la gestión de las actividades a todos los niveles organizacionales en el proceso de Planificación por Objetivos. Permite interrelacionar objetivos de trabajo y actividades en tiempo real; garantizando el seguimiento y cumplimiento de los objetivos y actividades en las entidades. Lleva a cabo la planeación estratégica y operativa mediante la gestión de planes, áreas de resultados claves, objetivos y actividades, y su proceso de aprobación-conciliación durante la concepción o ejecución de la planificación. Se basa en principios de independencia tecnológica, implementando funcionalidades generales de los procesos asociados a la planificación por objetivos, pero desde las particularidades de un modelo cubano de planificación.

Para la primera iteración de esta versión del producto no se tuvo en cuenta la guía para la gestión del RNF de Seguridad ni la lista de requisitos propuestos. Al realizar el proceso de pruebas de liberación interna por el equipo de calidad del CEIGE se identificaron un total de 387 NC, de ellas17 NC fueron clasificadas como vulnerabilidades.

A partir de la implementación de las funcionalidades planificadas en el alcance de la segunda iteración del proyecto, y las solicitudes de cambio realizadas por el cliente en la primera iteración, se decidió por parte de la dirección del centro, aplicar la guía y la definición de los requisitos propuestos en el proceso de desarrollo. La aplicación de la guía permitió velar por la definición, gestión, desarrollo, seguimiento y trazabilidad del RNF de Seguridad en el proyecto desde fases tempranas del desarrollo hasta las pruebas de liberación.

Una vez culminado el desarrollo de la segunda iteración, el producto se sometió a pruebas de liberación por el equipo de calidad del CEIGE. Las pruebas se realizaron por las personas que fueron responsables de realizar el mismo proceso a la primera iteración. Al concluir el proceso de pruebas de liberación interna se obtuvieron un total de 258 NC, de este total 7 fueron clasificadas como vulnerabilidades. Algunas de las vulnerabilidades disminuidas en el proceso de pruebas respecto a la iteración anterior fueron:

- Un usuario puede acceder al sistema y modificar los permisos de otro rol sin tener los permisos requeridos.
- Las contraseñas de acceso al sistema son débiles.
- Los usuarios no son bloqueados después de varios intentos fallidos de entrada al sistema.

- Se puede acceder al sistema desde varias estaciones de trabajo por el mismo usuario indistintamente.
- No está deshabilitado el almacenamiento de datos sensibles en la caché.

El impacto de las vulnerabilidades disminuidas en SIPAC se valoró como crítico, teniendo en cuenta que el mismo implementa la Instrucción 1 del Consejo de Estado y de Ministros, para la planificación de los objetivos y actividades en los Órganos de la Administración Central del Estado (OACE). Para esta valoración se tuvo en cuenta que la mayoría de las vulnerabilidades estaban relacionadas con el riesgo de pérdida de autenticación y exposición de datos sensibles.

A través de estas vulnerabilidades, los atacantes podrían robar o modificar los datos del sistema que se encontraran protegidos inapropiadamente. Las consecuencias sociales de la existencia de una fuga de datos personales, y sobre todo de datos del gobierno, se pueden analizar desde el punto de vista que propicia al atacante la suplantación de la identidad de un usuario. Además, el atacante puede realizar fraudes que causarían daños en las diferentes estructuras de los OACE que gestionan sus objetivos y planes de trabajo en el sistema.

De igual forma esto causaría grandes daños económicos y morales a la economía y estabilidad del país al modificar los planes y sus objetivos o apropiarse de información confidencial y utilizarla malintencionadamente. Los costes de estas vulnerabilidades se pueden medir a través del impacto económico-social que tengan en dependencia de la entidad víctima del ataque, más los costos del mantenimiento del sistema.

El análisis de los resultados de los dos procesos de liberación interna evidenció una disminución de un 59% de la cantidad de vulnerabilidades identificadas. Este dato confirma que la aplicación de la guía para la gestión del RNF de Seguridad en aplicaciones web desarrolladas en la UCI, contribuye a disminuir el número de vulnerabilidades identificadas.

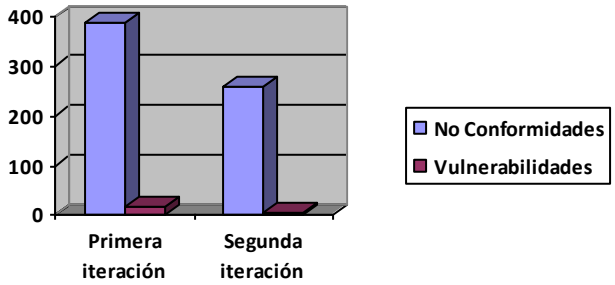


Figura 7 Resultados de los procesos de liberación interna del proyecto SIPAC 3.0.
Fuente: Elaboración propia.

3.2.3 Aplicabilidad de la guía y la propuesta de RNF de Seguridad

Para evaluar la satisfacción del cliente respecto a la utilidad y aplicabilidad de la guía (teniendo en cuenta la adherencia de los procesos a partir de las modificaciones realizadas, con las prácticas específicas del modelo CMMI), se aplicó la técnica Iadov. Esta técnica permite el estudio del grado de satisfacción del personal involucrado en un proceso determinado objeto de análisis [69; 88; 89].

Para la identificación y selección de los expertos que participaron en esta técnica desempeñándose como clientes, se consideró que los mismos tuvieran al menos cinco años de su desempeño laboral vinculados en el desarrollo de aplicaciones web, empleándose la encuesta de autovaloración de expertos para evaluar la satisfacción del cliente (ver Anexo 5).

La aplicación de la encuesta y el procesamiento de los datos para finalizar la selección de los expertos fue similar a la selección de los expertos para la valoración de la guía. Se identificaron 10 expertos, entre los que figuran miembros de varios centros de desarrollo de la UCI y personas de la DSI.

La técnica Iadov se compone de cinco preguntas claves: tres cerradas y dos abiertas, las cuales se formulan en la investigación para valorar el grado de satisfacción y utilidad de los clientes con la guía y los requisitos propuestos. Una vez establecidas las preguntas se conforma el “cuadro lógico de Iadov” y el número resultante de la interrelación de las tres preguntas, indica la posición de los sujetos en la escala de satisfacción [68; 69; 89]. La escala de satisfacción está dada por los criterios:

1. Clara satisfacción.
2. Más satisfecho que insatisfecho.
3. No definida.
4. Más insatisfecho que satisfecho.
5. Clara insatisfacción.
6. Contradictoria.

A continuación, se muestra el cuadro lógico de Iadov obtenido con la aplicación de la encuesta entregada a los expertos (ver Anexo 6)

Tabla 6 Cuadro lógico de Iadov
Fuente: Elaboración propia

¿La guía y la lista de requisitos propuestos teniendo en cuenta los riesgos y las sub-características de seguridad, satisface sus expectativas para gestionar los RNF de Seguridad?	¿Considera usted que es irrelevante la gestión del RNF de Seguridad desde el inicio del desarrollo del software?								
	No			No sé			Sí		
	¿Considera usted útil la gestión de los RNF de Seguridad la identificación de los requisitos no funcionales de Seguridad a partir de los riesgos y las sub-características de seguridad?								
	Sí	No sé	No	Sí	No sé	No	Sí	No sé	No
Me gusta mucho	1	2	6	2	2	6	6	6	6
No me gusta mucho	2	2	3	2	3	3	6	3	6
Me da lo mismo	3	3	3	3	3	3	3	3	3
Me disgusta más de lo que me gusta	6	3	6	3	4	4	3	4	4
No me gusta nada	6	6	6	6	4	4	6	4	6
No sé qué decir	2	3	6	3	3	3	6	3	4

Las preguntas abiertas que se formularon fueron:

- ¿Considera la guía propuesta y los requisitos identificados según los riesgos y las sub-características de seguridad aplicables al entorno productivo de la UCI para lograr la disminución de las vulnerabilidades en el desarrollo de aplicaciones web?
- ¿Qué elemento(s) usted agregaría a la guía y los requisitos propuestos?

Los resultados de la satisfacción individual según las categorías empleadas fueron los siguientes:

Tabla 7 Resultados de la técnica de Iadov.
Fuente: Elaboración propia.

Nivel de satisfacción	Cantidad	%
Máxima satisfacción	9	90,00
Más satisfecho que insatisfecho	1	10,00
No definida	0	0,00

Al analizar las respuestas recopiladas de la aplicación de las encuestas en el cuadro lógico de Iadov, se obtiene un grado de satisfacción grupal de **0,90**, lo cual se traduce en una clara satisfacción con el uso guía para la gestión del RNF de Seguridad y la lista de requisitos propuestos. En el criterio de los expertos respecto a la utilidad de la guía, hubo una concordancia de un 100,00% con la calificación *"Muy Adecuado"*. Respecto a la aplicabilidad de la guía y los requisitos propuestos existió una concordancia de un 90,00% con la calificación *"Muy Adecuado"* y el otro 10,00% lo calificó como *"Bastante Adecuado"*.

Las preguntas abiertas que formaron parte del ejercicio, permitieron la recopilación tanto de aspectos positivos como de recomendaciones, que sirven para enfocar futuras investigaciones hacia la mejora de esta área de investigación:

- Los analistas vinculados en diferentes centros de desarrollo, destacan las modificaciones hechas a los procesos de REQM y RD que favorecen la gestión del RNF de Seguridad.
- Los arquitectos y jefes de proyectos reconocen el beneficio que reporta en la identificación de los RNF de Seguridad, la lista de los requisitos propuestos.
- Los encuestados reconocen el uso de la guía y los requisitos definidos para incidir en la disminución de las vulnerabilidades.
- Hacer de dominio público para la actividad de desarrollo-producción de la UCI la lista de los riesgos más frecuentes y así como las vulnerabilidades que más afectan el desarrollo de software, a través de lecciones aprendidas.

La aplicación de la técnica de Iadov aportó datos importantes respecto al grado de satisfacción de los clientes. Los resultados obtenidos y los criterios emitidos validan la fortaleza de la propuesta, reflejándose una opinión muy positiva respecto a la satisfacción del cliente.

3.2.4 Triangulación metodológica de los métodos científicos utilizados

Luego de haber aplicado los métodos Delphi, un estudio de caso, y la técnica Iadov para validar la propuesta de solución, se realiza la triangulación metodológica de los resultados. La triangulación metodológica es "la combinación de múltiples métodos en un estudio del mismo objeto o evento para abordar mejor el fenómeno que se investiga" [90]. Con ello, se pretende corroborar los resultados para identificar coincidencias y discrepancias en el proceso de validación [91; 92].

Tabla 8 Resultados de la triangulación metodológica.
Fuente: Elaboración propia.

Objetivo a evaluar	**Métodos cualitativos**	**Métodos cuantitativos**	**Conclusión**
Elaborar una guía para la gestión del RNF de Seguridad, teniendo en cuenta los riesgos y las sub-características de seguridad, para disminuir el número de vulnerabilidades en el desarrollo de aplicaciones web.	**Grupo focal:** para la validación de los RNF de Seguridad. Luego de agregarse dos nuevos requisitos a la lista inicial, se obtuvo la conformidad con los requisitos propuestos.	**Método de Delphi:** para obtener las consideraciones sobre la contribución de la guía y la propuesta de los RNF de Seguridad. Se obtuvo un alto porciento de evaluación en el rango de Muy Adecuado para la relevancia, pertinencia y coherencia de la guía y los requisitos propuestos. **Estudio de caso**: para obtener las diferencias a partir de la comparación del número de vulnerabilidades en un proyecto, antes y después de la aplicación de la guía. Se obtuvo como resultado una disminución del 59% de vulnerabilidades entre una iteración y otra. **Técnica de Iadov**: para evaluar	Validez de la guía para la gestión del RNF de Seguridad en el desarrollo de aplicaciones web teniendo en cuenta los riesgos y las sub-características de seguridad, y así como de la lista de requisitos de seguridad. Se corroboró la conformidad con la lista de requisitos propuestos, una alta concordancia respecto a la relevancia, pertinencia y coherencia de la propuesta por parte de expertos. Además, se demostró la

		la satisfacción de los clientes respecto a la utilidad y aplicabilidad de la guía. Se obtuvo un índice de satisfacción grupal de un **0.9%.**	disminución de las vulnerabilidades en un estudio de caso luego de aplicada la propuesta, y se evidenció una alta satisfacción por parte de los usuarios del resultado de la investigación.

3.3 Conclusiones parciales del capítulo

Las principales conclusiones que se pueden señalar del presente capítulo son:

- La guía y los requisitos propuestos, fueron validados mediante criterios recopilados a través de encuestas a los expertos seleccionados. Se tuvo en cuenta la contribución del análisis de riesgos y de las sub-características de seguridad, demostrando el efecto positivo de la guía para la disminución de vulnerabilidades en el desarrollo de aplicaciones web, así como el alto nivel de satisfacción de los clientes, obtenido de la aplicación de la técnica de Iadov.
- La utilización de la guía, favorece la disminución del número de vulnerabilidades identificadas en el desarrollo de aplicaciones web. El criterio de los expertos avala la coherencia y pertinencia de la guía, siendo consecuente con las exigencias del problema de investigación.
- Los resultados de la aplicación de la técnica de Iadov evidenciaron un alto nivel de satisfacción por parte de clientes potenciales, resaltando aspectos positivos de la guía y los requisitos propuestos con respecto a la disminución de vulnerabilidades en el desarrollo web.

CONCLUSIONES GENERALES

Sobre los resultados obtenidos en el desarrollo de la investigación se concluye lo siguiente:

1. El análisis de las definiciones, normas y estándares relacionados con la Seguridad Informática evidenciaron la necesidad de tener en cuenta los riesgos y las sub-características de seguridad para la gestión de los requisitos no funcionales de seguridad.
2. La guía propuesta para la gestión del requisito no funcional de seguridad en las aplicaciones web desarrolladas en la Universidad de las Ciencias Informáticas, contribuye a la disminución del número de vulnerabilidades a partir de la consideración de los riesgos identificados y las sub-características de seguridad.
3. La lista de requisitos de seguridad propuesta, teniendo en cuenta riesgos y las sub-características de seguridad, facilita de esta forma su identificación para la disminución de las vulnerabilidades en los desarrollos de aplicaciones web.
4. La guía y los requisitos propuestos, fueron validados mediante métodos científicos a través de encuestas a los expertos seleccionados, estudio de caso y á técnica de Iadov para medir la satisfacción de los clientes. Se tuvo en cuenta la contribución del análisis de riesgos y de las sub-características de seguridad, demostrando el efecto positivo de la guía para la disminución de vulnerabilidades en el desarrollo de aplicaciones web mediante un estudio de caso como método activo, así como el alto nivel de satisfacción de los clientes.

RECOMENDACIONES

1. Identificar métricas de Seguridad Informática e implementarlas en una solución que permita realizar análisis sobre indicadores de interés para la organización y contribuya a la toma de decisiones de la organización.
2. Hacer de dominio público para la actividad de desarrollo-producción de la Universidad de las Ciencias Informáticas la lista de los riesgos más frecuentes y así como las vulnerabilidades que más afectan el desarrollo de software, a través de lecciones aprendidas.

REFERENCIAS BIBLIOGRÁFICAS

[1] Martín, A. R. andMartín, M. J. R. (2014). *Aplicaciones web*: Ediciones Paraninfo, SA.

[2] Niño Benitez, Y. andSilega Martínez, N. (2018). Requisitos de Seguridad para aplicaciones web. *Revista Cubana de Ciencias Informáticas, 12*, 205-221.

[3] Luján Mora, S. (2016). Programación de aplicaciones web. Historia. Principios básicos y clientes web. Luján Mora, Sergio.

[4] Sierra, Y. andYury, Y. (2018). *Aplicación web para el control de inventario y facturación de la empresa Binacom Sys SA.*

[5] Avilés, G. G. (2015). *Seguridad en Bases de Datos y Aplicaciones Web*: IT Campus Academy.

[6] Sánchez, M. (2018). Origen y evolución de internet. *Contribuciones a las Ciencias Sociales*(marzo).

[7] Anton, K.; Manico, J. andBird, J. (2018). OWASP Top 10 Proactive Controls 2018. 40.

[8] Urbina, G. B. (2016). *Introducción a la seguridad informática*: Grupo Editorial Patria.

[9] Gil Vera, V. D. andGil Vera, J. C. (2017). Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas. *Scientia et technica, 22*(2).

[10] Tucta, G. andAlejandro, R. (2017). *Sistema de Gestión de Seguridad de la información basado en la Norma ISO/IEC 27001 para el Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación.* Universidad Técnica de Ambato. Facultad de Ingeniería en Sistemas, Electrónica e Industrial. Carrera Ingeniería en Sistemas Computacionales e Informáticos.

[11] Naur, P. andRandell, B. (1968). Software Engineering: Report of a conference sponsored by the NATO Science Committee, Garmisch, Germany, 7th-11th October 1968.

[12] Radatz, J.; Geraci, A. andKatki, F. (1990). IEEE standard glossary of software engineering terminology. *IEEE Std, 610121990*(121990), 3.

[13] ISO. (2000). *ISO 9000:2000 Sistemas de gestión de la calidad — Conceptos y vocabulario*.

[14] Pressman, R. S. andMaxim, B. R. (2015). *Ingeniería de Software. Un enfoque práctico* (8th ed.).

[15] Sommerville, I. (2011). *Ingeniería de software* (9na ed.): Addison-Wesley.

[16] ISO/IEC, N. (2016). INGENIERÍA DE SOFTWARE Y SISTEMAS – REQUISITOS DE LA CALIDAD Y EVALUACIÓN DE SOFTWARE (SQuaRE) – MODELOS DE LA CALIDAD DE SOFTWARE Y SISTEMAS
(ISO/IEC 25010: 2011, IDT).

[17] Losavio, F. andEsteves, Y. (2016). *Modelado del Negocio como Técnica Centrada en la Calidad del Software para el Análisis del Dominio del Aprendizaje Electrónico.* Paper presented at the IV Simposio Científico y Tecnológico en Computación/SCTC 2016/ISBN: 978-980-12-8407-9. Universidad Central de Venezuela, Caracas, Venezuela.

[18] Valle Rojo, S. d. andOliveros, A. (2014). Elicitación y especificación de requerimientos no funcionales para aplicaciones web.

[19] Rosado, D. G.; Blanco, C.; Sánchez, L. E. andMedina, E. F. (2009). La Seguridad como una asignatura indispensable para un Ingeniero del Software. La Mancha.

[20] Anderson, R. J. (2010). *Security engineering: a guide to building dependable distributed systems*: John Wiley & Sons.
[21] Taylor, R. W.; Fritsch, E. J. andLiederbach, J. (2014). *Digital crime and digital terrorism*: Prentice Hall Press.
[22] UCI. (2018). Universidad de las Ciencias Informáticas. *Universidad de las Ciencias Informáticas.* Retrieved 15 de Octubre, 2018, from http://www.uci.cu
[23] UCI, D. d. C. d. S. (2018). Informe de Tendencias. Retrieved enero 2018, 2018, from https://excriba.prod.uci.cu/page/site/direccin-de-calidad/documentlibrary#filter=path%7C%2F01-%2520Direccion%2520de%2520Calidad%2F0103-%2520Expediente%2520Direccion%2520de%2520Calidad%2FTendencias%2FInforme_de_tendencias%7C&page=1
[24] Dayana Leticia López Chávez, P. A. R. (2018). PRUEBAS DE SEGURIDAD UTILIZANDO HERRAMIENTAS PARA LA DETECCIÓN DE VULNERABILIDADES., 7.
[25] Montesino Perurena, R. (2012). *Modelo para la gestión automatizada e integrada de Controles de seguridad informática.* (Doctorado en Ciencias Técnicas Tesis doctoral), Universidad de las Ciencias Informáticas.
[26] Garfinkel, S.; Spafford, G. andRiverol, M. C. (1999). *Seguridad y comercio en el Web*: McGraw-Hill.
[27] Vieites, Á. G. (2011). *Enciclopedia de la seguridad informática* (Vol. 6): Grupo Editorial RA-MA.
[28] Estrada, Y.; Alba, W. andMartín, A. (2012). Fundamentos para implementar y certificar un Sistema de Gestión de la Seguridad Informática bajo la Norma ISO/IEC 27001. *Serie Científica de la Universidad de las Ciencias Informáticas, No. 10, Vol. 5*, 10.
[29] Larrocha, E. R. (2017). *Nuevas tendencias en los sistemas de información*: Editorial Centro de Estudios Ramón Areces S. A.
[30] RESOLUCION No. 127 /2007 (2007).
[31] Asteasuain, F. andSchmidt, L. A. (2005). Aplicación de la Programación Orientada a Aspectos como Solución a los Problemas de la Seguridad en el Software. 15.
[32] ISO/IEC. (2013). ISO/IEC 27002: 2013 Information technology — Security techniques — Code of practice for information security management.
[33] Arora, V. (2010). Comparing different information security standards: COBIT v s. ISO 27001. *Qatar: Carnegia Mellon University*.
[34] ISO/IEC. (2005). ISO/IEC 27001 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos: Switzerland.
[35] ISO (Producer). (2017, marzo 12). El portal de ISO 27001 en Español. *El portal de ISO 27001 en Español*. Retrieved from http://www.iso27000.es/iso27000.html
[36] Mentor, A. (Producer). (2017, marzo 12). Aula Mentor. *Aula Mentor. Seguridad informática. Normas ISO sobre gestión de seguridad de la información*. Retrieved from http://descargas.pntic.mec.es/mentor/visitas/demoSeguridadInformatica/normas_iso_sobre_gestin_de_seguridad_de_la_informacin.html

[37] Proença, D. andBorbinha, J. (2018). *Information Security Management Systems-A Maturity Model Based on ISO/IEC 27001.* Paper presented at the International Conference on Business Information Systems.
[38] OWASP (Producer). (2017, 03 21). OWASP. *OWASP*. Retrieved from https://www.owasp.org/index.php/Main_Page
[39] OWASP. (2016). OWASP Top 10 controles proactivos 2016. 28.
[40] Brito, H. R. G. (Producer). (2017, 03 20). Behique Digital. *Behique Digital*. Retrieved from https://henryraul.wordpress.com/2016/10/11/owasp-top-10-proactive-controls-2016/
[41] OWASP. (2017). OWASP Top 10 - 2017 Los diez riesgos más críticos en Aplicaciones Web.
[42] (OSRI), O. d. S. d. R. I. (2018). Oficina de Seguridad de Redes Informática. Retrieved 29/03/2018, 2018, from http://www.mincom.gob.cu/?q=node/311
[43] Normalización, N. O. N. d. (2016). ISO/IEC 27001: 2007 TECNOLOGÍA DE LA INFORMACIÓN—TÉCNICAS DE SEGURIDAD—SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN—REQUISITOS (ISO/IEC 27001: 2005, IDT): Cuban National Bureau of Standards.
[44] Boehm, B. (1976). *Economía de la Ingeniería del Software*.
[45] Fairley, R. E. (1985). *Software Engineering Concepts*.
[46] IEEE. (1990). *IEEE Terminología estándar de ingeniería de software*.
[47] Pressman, R. S. (2005). *Ingenieria de software. Un enfoque práctico* (Vol. 5ta Edición).
[48] Huebe, M. d. L. P. (2005). *Ingeniería de sistemas.* Universidad Autónoma del Estado de Hidalgo. , Pachuca.
[49] Jacobson, I.; Booch, G. andRumbaugh, J. (2000). *El proceso unificado de desarrollo de software/The unified software development process*: Pearson Educación.
[50] Litvak, C. S.; Hadad, G. D. S. andDoorn, J. H. (2015). *Procesamiento de Lenguaje Natural para Estudiar Completitud de*
Requisitos.
[51] Sommerville, I. (2005). *Ingeniería del software*: Pearson Educación.
[52] SEI. (2010). CMMI® para Desarrollo, Version 1.3: Carnegie Mellon University.
[53] ISO/IEC. (2005). Ingeniería de Software - Guía del Cuerpo de Conocimiento de Ingeniería de Software (SWEBOK).
[54] Thaureaux, D. D. (2009). *Uso de la Metodología DoRCU en la ingeniería de requisitos para el desarrollo de Software de Salud centrada en el usuario, por Especialistas Funcionales del MINSAP.* (Mestría), Universidad de las Ciencias Informáticas, La Habana.
[55] Sherman, A. T.; DeLatte, D.; Neary, M.; Oliva, L.; Phatak, D.; Scheponik, T.; Herman, G. L. andThompson, J. (2018). Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia, 42*(4), 337-377.
[56] Carpentier, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas*: Ediciones ENI.
[57] NIST; ROSS, R.; McEVILLEY, M. andOREN, J. C. (2016). INGENIERÍA DE SEGURIDAD DE SISTEMAS - Consideraciones para un Enfoque Multidisciplinario en la Ingeniería de Sistemas Confiables Confiables.

[58] ISO/IEC/IEEE. (2011). *Ingeniería de software y de sistemas - Procesos del ciclo de vida - Ingeniería de requisitos*.
[59] ISO. (2015). ISO/IEC/IEEE 15288:2015 Systems and software engineering -- System life cycle processes. Retrieved 25 de junio, 2017, from https://www.iso.org/standard/63711.html
[60] IEEE. (1998). *IEEE Std 830-1998 Práctica recomendada para especificaciones de requisitos de software*.
[61] IEEE. (1998). *IEEE Guía para desarrollar especificaciones de requisitos del sistema*.
[62] Normalización, O. N. d. (2016). *INGENIERÍA DE SOFTWARE Y SISTEMAS – REQUISITOS DE LA CALIDAD Y EVALUACIÓN DE SOFTWARE (SQuaRE) – MODELOS DE LA CALIDAD DE SOFTWARE Y SISTEMAS (ISO/IEC 25010: 2011, IDT)*. La Habana, Cuba.
[63] Blanco, K. R. (2013). *Proceso Base de Ingeniería de Requisitos para las pequeñas y medianas empresas de desarrollo de software.* (Tesis en opción al título de Máster en Calidad de Software), Universidad de las Ciencias Informáticas, La Habana
[64] Alharbi, E. T. andQureshi, M. R. J. (2014). Implementation of risk management with SCRUM to achieve CMMI requirements. *International Journal of Computer Network and Information Security, 6*(11), 20.
[65] Demirel, S. T. andDas, R. (2018). *Software requirement analysis: Research challenges and technical approaches.* Paper presented at the Digital Forensic and Security (ISDFS), 2018 6th International Symposium on.
[66] UCI, G. d. I. (2017). Mejora de Procesos de Software. Retrieved 20 de noviembre, 2018, from http://mejoras.prod.uci.cu/
[67] Ingeniería, U. G. d. (2017). Mejora de Procesos de Software. Retrieved 20 de noviembre, 2018, from http://mejoras.prod.uci.cu/
[68] Trujillo-Casañola, Y.; Febles-Estrada, A. andLeón-Rodríguez, G. (2014). Modelo para valorar las organizaciones al iniciar la mejora de procesos de software. *Ingeniare. Revista chilena de ingeniería, 22*(3), 412-420.
[69] García, A. M. (2018). *Modelo de recomendación de escenarios al iniciar la mejora de procesos de software.* (Doctor en Ciencias Técnicas Doctoral), Universidad de las Ciencias Informáticas, La Habana.
[70] Muñoz, M.; Gasca, G. andValtierra, C. (2014). Caracterizando las necesidades de las pymes para implementar mejoras de procesos software: Una comparativa entre la teoría y la realidad. *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação*(SPE1), 1-15.
[71] Wood, P. B. andVickers, D. (2018). *Anticipated impact of the capability maturity model integration (CMMI®) V2. 0 on aerospace systems safety and security.* Paper presented at the 2018 IEEE Aerospace Conference.
[72] Portantier, F. (2012). *Seguridad informática*: USERSHOP.
[73] Salazar, D. (2009). PERFILES PROFESIONALES PARA SEGURIDAD INFORMÁTICA. Un enfoque práctico. Retrieved 02/12/2018, 2018, from https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&ved=2ahUKEwjZqc6Uy4HfAhXM1lkKHRXwBT0QFjADegQIBxAC&url=https%3A%2F%2Fwww.monografias.c

om%2Ftrabajos-pdf2%2Fperfiles-profesionales-seguridad-informatica-practico%2Fperfiles-profesionales-seguridad-informatica-practico.pdf&usg=AOvVaw3qMbAWDkWOrWVHBUBSbGmB

[74] Estupiñan, A. d. C. A.; Pulido, J. A. andJaime, J. A. B. (2013). Análisis de Riesgos en Seguridad de la Información. *Ciencia, innovación y tecnología, 1*, 40-53.

[75] CALISOFT, C. N. d. C. d. S. (2018). Norma Ramal – Requisitos de la Calidad para Sistemas Informáticos y Productos de Software. Retrieved 23/05/2018, 2018, from http://subcomite7.cubava.cu/2017/02/10/norma-ramal-requisitos-de-la-calidad-para-sistemas-informaticos-y-productos-de-software/

[76] OWASP; Manico, J.; Stock, A. v. d. andCuthbert, D. (2017). Estándar de Verificación de Seguridad en Aplicaciones 3.0.1.

[77] Friedman, C. P. andWyatt, J. C. (2013). *Evaluation methods in medical informatics*: Springer Science & Business Media.

[78] Niu, N.; Da Xu, L. andBi, Z. (2013). Enterprise information systems architecture—Analysis and evaluation. *IEEE Transactions on Industrial Informatics, 9*(4), 2147-2154.

[79] Vaishnavi, V. K. andKuechler, W. (2015). *Design science research methods and patterns: innovating information and communication technology*: Crc Press.

[80] Palinkas, L. A.; Horwitz, S. M.; Green, C. A.; Wisdom, J. P.; Duan, N. andHoagwood, K. (2015). Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research, 42*(5), 533-544.

[81] Martínez, N. S. (2014). *MÉTODO PARA LA TRANSFORMACIÓN AUTOMATIZADA DE MODELOS DE PROCESOS DE NEGOCIO A MODELOS DE COMPONENTES PARA SISTEMAS DE GESTIÓN EMPRESARIAL.* (Doctor en Ciencias Técnicas Doctoral), Universidad de las Ciencias Informáticas, La Habana.

[82] Cutiño, R. Y. V. (2011). *Guía metodológica para implementar la seguridad durante el desarrollo de aplicaciones informáticas.* (Máster en Informática Aplicada), Universidad de las Ciencias Informáticas, La Habana.

[83] Muñoz, M. S. (2014). *Modelo para la evaluación de la seguridad del Control de Acceso de los Sistemas de Información de centros productivos de la Universidad de las Ciencias Informáticas.* (Máster en Informática Aplicada Maestría), Universidad de las Ciencias Informáticas, La Habana.

[84] Baryolo, O. G. (2012). *CAEM: MODELO DE CONTROL DE ACCESO PARA SISTEMAS DE INFORMACIÓN EN ENTORNOS MULTIDOMINIOS.* (Tesis presentada en opción al grado científico de Doctor en Ciencias Técnicas), Universidad de las Ciencias Informáticas.

[85] Landeta, J. (1999). *El método Delphi. Una técnica de previsión del futuro*: Ariel.

[86] Ramírez, M. andVásquez, J. (2018). Emergence and development of the Delphi method: A scientometric perspective [Surgimiento y desarrollo del método Delphi: Una perspectiva cienciométrica].

[87] López-Gómez, E. (2018). El método Delphi en la investigación actual en educación: una revisión teórica y metodológica. *Educación XX1, 21*(1), 17-40.

[88] Pineda, E. B.; de Alvarado, E. L. andde Canales, F. H. (1994). *Metodología de la investigación: manual para el desarrollo de personal de salud*: OPS.

[89] González, M. V. (2017). *Estrategia para la obtención de los requisitos de software de portales web para el centro CIDI de la Universidad de las Ciencias Informáticas.* (Máster en Calidad de Software Maestría), Universidad de las Ciencias Informáticas, La Habana.

[90] Cowman, S. (1993). Triangulation: a means of reconciliation in nursing research. *Journal of Advanced Nursing, 18*(5), 788-792.

[91] Aguilar Gavira, S. andBarroso Osuna, J. M. (2015). La triangulación de datos como estrategia en investigación educativa. *Pixel-bit. Revista de medios y educación, 47*, 73-88.

[92] Samaja, J. (2018). La triangulación metodológica (Pasos para una comprensión dialéctica de la combinación de métodos). *Revista Cubana de Salud Pública, 44*, 431-443.

ANEXOS

Anexo 1. Materiales y resultados del diagnóstico

Encuesta: Para evaluar la necesidad de la investigación

Con este cuestionario se pretender evaluar la necesidad de desarrollar una investigación para la elaboración de una guía que gestione el Requisito No Funcional (RNF) de Seguridad en el desarrollo de aplicaciones web en la Universidad de las Ciencias Informáticas (UCI), con el fin de disminuir el número de vulnerabilidades identificadas. Se le asegura confidencialidad y anonimato a su respuesta.

Rol: _____ Años de experiencia _____ Tipo de proyectos en los que ha trabajo _____

1. Conoce si en su proyecto se definen requisitos de seguridad:
   ____ Si Cómo _____ ____No
2. ¿Cree importante definir requisitos de seguridad en su proyecto?: ____ Si _____No
3. ¿En qué momento del ciclo de vida del proyecto sugiere la gestión de los requisitos de seguridad?
   _____ Modelado de negocio _____ Requisitos _____ Análisis y diseño _____ Implementación _____ Pruebas de Liberación
4. Conoce las consecuencias que provoca que no se tengan en cuenta los requisitos de seguridad en los proyectos:
   ____ Si Cuáles: _____ ____ No
5. Tienen en cuenta los miembros de su proyecto las tecnologías para el desarrollo seguro de aplicaciones: ____ Si _____No
6. Conoce si se encuentran identificadas lecciones aprendidas con las vulnerabilidades más frecuentes encontradas en una tecnología similar a la que usa su proyecto:
   ____ Si Cuál: _____ ____ No
7. Sabe si se ejecutan pruebas de seguridad en su proyecto: ____ Si _____No
8. Conoce las vulnerabilidades más frecuentes: ____ Si Cuáles: _____ _____No
9. Conoce cuál es el costo de certificación de un proyecto por una entidad certificadora en el país, como Segurmática: ____ Si _____No
10. Diga al menos tres aspectos que considere de vital importancia en función de la seguridad de la aplicación.

Anexo 2 Materiales y resultados de grupo focal para Buenas Prácticas y recomendaciones

Guía del Grupo focal

No de participantes: 7 expertos en el desarrollo de software.

Fecha: 20 de septiembre del 2018 Lugar: Laboratorio 10, Docente 1 Producción Hora: 2:00 p.m.

Nombre del moderador: Yisel Niño Benitez

Nombre del observador: Dannel Jiménez Torres

Objetivo de la investigación: validar la lista de RNF de Seguridad propuesto a partir del análisis de los riesgos identificados por OWASP y las sub-características de Seguridad definidas en la ISO 25010.

Descripción del grupo focal: el análisis de la bibliografía consultada en materia de Seguridad Informática promueve la identificación temprana de los requisitos no funcionales (RNF) de Seguridad y reconoce como importante su gestión y seguimiento durante el ciclo de vida del proyecto. Para darle solución a esta necesidad se realizó una guía para la gestión del RNF de Seguridad, como valor agregado a la guía se definición de una lista de requisitos de Seguridad con el objetivo de facilitar su identificación en los proyectos de desarrollo de aplicaciones web. El **objetivo del grupo focal** es validar los requisitos propuestos y realizar recomendaciones al respecto.

Descripción de los participantes: 7 personas, de ellas 2 especialistas de CEIGE seleccionados, de ellos 1 asesor de tecnología y SI, 2 miembros de la Dirección de Calidad de Software, 2 especialistas de CEIGE y 1 miembro de la Dirección de Seguridad Informática.

Guía de la actividad

- Describir lo que constituye un grupo focal
- Explicar el objetivo de la reunión
- Explicar procedimiento, confidencialidad
- Presentación de cada participante, implica que se le pedirá a cada participante que se presente y que aborde en un minuto su experiencia en la MPS.
- Presentación de la lista de la propuesta inicial de los RNF de Seguridad (Ver epígrafe 2.3 Propuesta de requisitos de seguridad para aplicaciones web).

- Ejecución del debate
- Conclusiones

Guía de preguntas

- ¿Qué importancia le confiere a la identificación de los RNF de Seguridad?
- ¿Considera adecuadas las sub-categorías propuestas en la definición de los requisitos?
- ¿Qué requisitos considera que sean necesarios además de los ya definidos?
- ¿Considera que los requisitos propuestos puedan disminuir las vulnerabilidades en el desarrollo de aplicaciones web?

Anexo 3. Resultados del procesamiento para la selección de expertos

Nivel de experticia en la temática: Administración de Requisitos y Desarrollo de Requisitos

Tabla 9 Experticia en la temática: Administración de Requisitos y Desarrollo de Requisitos. Fuente: Elaboración propia.

Candidato	K_c	K_a	K	Nivel
1	0,80	0,80	0,80	Alto
2	0,90	0,90	0,90	Alto
3	0,50	0,50	0,50	Bajo
4	0,80	0,80	0,80	Alto
5	0,50	0,40	0,45	Bajo
6	0,90	6,00	0,75	Medio
7	0,90	0,80	0,85	Alto
8	0,60	0,40	0,50	Bajo
9	0,90	0,80	0,85	Alto
10	0,90	0,70	0,80	Alto
11	1,00	0,90	0,95	Alto
12	0,90	0,70	0,80	Alto
13	0.70	0.60	0.65	Medio

Nivel de experticia en la temática: Seguridad Informática y las sub-características de Seguridad

Tabla 10 Experticia en la temática: Seguridad Informática y las sub-características de Seguridad.
Fuente: Elaboración propia

Candidato	K_c	K_a	K	Nivel
1	0,90	0,90	0,90	Alto
2	0,90	0,70	0,80	Alto
3	0,60	0,50	0,55	Medio
4	0,80	0,80	0,80	Alto
5	0,70	0,30	0,50	Bajo
6	1,00	0,90	0,95	Alto
7	0,90	0,70	0,80	Alto
8	0,30	0,40	0,35	Bajo
9	0,90	0,80	0,85	Alto
10	0,70	0,70	0,70	Medio
11	0,80	0,70	0,75	Medio
12	1,00	0,70	0,85	Alto
13	0,50	0,50	0,50	Bajo

Nivel de experticia en la temática: Riesgos que afectan la Seguridad Informática

Tabla 11 Experticia en la temática: Riesgos que afectan la Seguridad Informática.
Fuente: Elaboración propia.

Candidato	K_c	K_a	K	Nivel
1	0,90	0,80	0,85	Alto
2	0,90	0,80	0,85	Alto
3	0,50	0,30	0,40	Bajo
4	0,90	0,80	0,85	Alto
5	0,50	0,50	0,50	Medio
6	0,90	0,80	0,85	Alto
7	0,80	0,50	0,65	Medio
8	0,50	0,40	0,45	Bajo
9	0,80	0,70	0,75	Medio
10	0,80	0,80	0,80	Alto
11	0,80	0,80	0,80	Alto
12	0,60	0,50	0,55	Medio
13	0,50	0,30	0,40	Bajo

Anexo 4 Contribución de la guía y la propuesta de los Requisitos No Funcionales de Seguridad

Compañero (a):

La validación de la guía para la gestión del Requisito No Funcional de Seguridad y la propuesta de requisitos identificados a partir de los riesgos y las sub-características de Seguridad, se llevará a cabo a partir del juicio de valor que Ud. emita respecto a la relevancia, pertinencia y coherencia del mismo donde:

Relevancia: La influencia de cada uno de los elementos de la guía propuesta en las organizaciones.

Pertinencia: La estructura del proceso es congruente con los objetivos del mismo y consideran las exigencias de las organizaciones.

Coherencia: Existe coherencia e interrelación entre los componentes del proceso.

1. Para evaluar la **relevancia** de la guía propuesta, valore, según la escala que se muestra a continuación, la influencia que tiene cada uno de los elementos que se mencionan, en la disminución de las vulnerabilidades.
   a) Muy Adecuado (MA)
   b) Bastante Adecuado (BA)
   c) Adecuado (A)
   d) Poco Adecuado (PA)
   e) Inadecuado (I)

No	Aspectos	Evaluación
1	Roles y sus responsabilidades definidas en la ejecución de los procesos.	
2	Modificaciones realizadas a los procesos de REQM y RD para la gestión del RNF de Seguridad.	
3	Definición de la lista de RNF de Seguridad teniendo en cuenta las sub-características de Seguridad.	
4	Identificación de riesgos que afectan las SI.	
5	Identificación de la relación existente entre los requisitos definidos y los riesgos identificados.	
6	Facilidad de comprensión de la guía y los requisitos propuestos.	
7	Efectividad de la guía para el cumplimiento del objetivo propuesto.	
8	Utilidad de la guía para la gestión del RNF de Seguridad teniendo en cuenta	

	los riesgos y las sub-características de seguridad, para disminuir el número de vulnerabilidades en las aplicaciones web.	

2. Para emitir su criterio acerca de la **pertinencia** de la estructura de la guía propuesta, las actividades, entradas y salidas modificadas en los procesos REQM y RD y la lista de RNF de Seguridad propuesta, marque con una (X) en la casilla correspondiente al valor asignado por usted, teniendo como referencia la escala siguiente:
   a) Muy Adecuado (MA) ☐
   b) Bastante Adecuado (BA) ☐
   c) Adecuado (A) ☐
   d) Poco Adecuado (PA) ☐
   e) Inadecuado (I) ☐
3. Sobre la **coherencia** e interrelación existente entre los roles, actividades, entradas y salidas de la guía propuesta, y la relación entre los RNF de Seguridad, las sub-características y los riesgos, marque con una (X) en la casilla que corresponda, según su criterio, teniendo en cuenta la escala de referencia siguiente:
   a) Muy Adecuado (MA) ☐
   b) Bastante Adecuado (BA) ☐
   c) Adecuado (A) ☐
   d) Poco Adecuado (PA) ☐
   e) Inadecuado (I) ☐
4. De considerarlo necesario, emita las observaciones, sugerencias y/o recomendaciones que pudieran contribuir, según su criterio, al perfeccionamiento de la guía propuesta y los RNF de Seguridad identificados.

   _____

   _____

Anexo 5 Encuesta de autovaloración de expertos para evaluar la satisfacción del cliente

Compañero(a):

Se desea someter a la valoración de un grupo de expertos la satisfacción del cliente respecto a la utilidad y aplicabilidad de la guía para la gestión del requisito No Funcional de Seguridad en aplicaciones web. Para ello se necesita conocer el grado de dominio que usted posee en el desarrollo de software y sus años de experiencia en esta área del conocimiento. Con ese fin se necesita que responda lo siguiente:

1. Marque con una cruz (X) el grado de conocimiento que usted tiene sobre la temática mejora de procesos de software, donde 0 corresponde al valor mínimo y 10 al máximo:

0	1	2	3	4	5	6	7	8	9	10

2. Especifique del 0 al 10 la influencia de las fuentes indicadas como fundamento de su conocimiento en las temáticas de Seguridad Informática e Ingeniería de Requisitos, donde 0 corresponde al valor mínimo y 10 al máximo:

No.	Fuente de argumentación	Fundamentación
1	Años de experiencia en el tema	
2	Conocimientos teóricos adquiridos en análisis bibliográfico	
3	Experiencia práctica	
4	Participación en eventos científicos	
5	Publicaciones en revistas referenciadas y en memorias de eventos	

3. Especifique años de experiencia en el área del conocimiento mejora de procesos de software: ___

Anexo 6 Encuesta para valorar la satisfacción de los clientes

La medida de la satisfacción del cliente con respecto a la guía propuesta y los Requisitos No Funcionales (RNF) de Seguridad, así como su utilidad y aplicabilidad en entornos reales, se llevará a cabo a partir del juicio que usted emita. Según su criterio, responda las siguientes preguntas:

1. ¿La guía y la lista de requisitos propuestos teniendo en cuenta los riesgos y las sub-características de Seguridad, satisface sus expectativas para gestionar los RNF de Seguridad? Especifique el grado de satisfacción:

   Me gusta mucho: _____

   No me gusta mucho: _____

   Me da lo mismo: _____

   Me disgusta más de lo que me gusta_____

No me gusta nada: _____

No sé qué decir: _____

2. Especifique el grado en que usted valora que la guía propuesta resulte útil para la disminución del número de vulnerabilidades en el desarrollo de las aplicaciones web, siendo *Muy Adecuado* la mayor puntuación e *Inadecuado* la menor.

Muy Adecuado	Bastante Adecuado	Adecuado	Poco Adecuado	Inadecuado

3. ¿Considera usted que es irrelevante la gestión del RNF de Seguridad desde el inicio del desarrollo del software?

____Sí ____No ____No sé

4. Especifique el grado en que usted valora que la guía propuesta y los requisitos identificados según los riesgos y las sub-características de Seguridad aplicables al entorno productivo de la UCI para lograr la disminución de las vulnerabilidades en el desarrollo de aplicaciones web, siendo *Muy Adecuado* la mayor puntuación e *Inadecuado* la menor.

Muy Adecuado	Bastante Adecuado	Adecuado	Poco Adecuado	Inadecuado

5. ¿Recomendaría este sistema a otras organizaciones?

___ Sí ___ No ___ No sé