UNIVERSIDAD ESTATAL DE MILAGRO

FACULTAD CIENCIAS DE LA INGENIERIA

TRABAJO DE TITULACIÓN DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERIO EN SISTEMAS COMPUTACIONALES

PROPUESTA PRÁCTICA DEL EXAMEN DE GRADO O DE FIN DE CARRERA (DE CARÁCTER COMPLEXIVO)

INVESTIGACIÓN DOCUMENTAL

TEMA: MODELO DE SISTEMA BASADO EN EL CONOCIMIENTO PARA EL DISEÑO DE SOFTWARE EN EL DOMINIO DE SEGURIDAD DE LA APLICACIÓN

Autores:

Edison José Villavicencio Sánchez

Bryan Lenin González Irrasabal

Acompañante:

Ing. Mirella Azucena Correa Peralta

Milagro, 24 de Mayo 2018

ECUADOR

DERECHOS DE AUTOR

Ingeniero.
Fabricio Guevara Viejó, PhD.
RECTOR
Universidad Estatal de Milagro
Presente.

Nosotros, **VILLAVICENCIO SÁNCHEZ EDISON JOSÉ, GONZÁLEZ IRRASABAL BRYAN LENIN** en calidad de autores y titulares de los derechos morales y patrimoniales de la propuesta práctica de la alternativa de Titulación – Examen Complexivo: Investigación Documental, modalidad presencial, mediante el presente documento, libre y voluntariamente procedo a hacer entrega de la Cesión de Derecho del Autor de la propuesta practica realizado como requisito previo para la obtención de mi Título de Grado, como aporte a la Temática **KNOWLEDGE BASED SYSTEM PARA DISEÑO DE SOFTWARE** del Grupo de Investigación **TICS Y DESARROLLO DE SOFTWARE** de conformidad con el Art. 114 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, concedo a favor de la Universidad Estatal de Milagro una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos. Conservo a mi favor todos los derechos de autor sobre la obra, establecidos en la normativa citada.

Así mismo, autorizo a la Universidad Estatal de Milagro para que realice la digitalización y publicación de esta propuesta practica en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

El autor declara que la obra objeto de la presente autorización es original en su forma de expresión y no infringe el derecho de autor de terceros, asumiendo la responsabilidad por cualquier reclamación que pudiera presentarse por esta causa y liberando a la Universidad de toda responsabilidad.

Milagro, a los 24 días del mes de Mayo de 2018.

VILLAVICENCIO SÁNCHEZ EDISON JOSÉ
CI: 030295478-9

GONZÁLEZ IRRASABAL BRYAN LENIN
CI: 094209641-3

APROBACIÓN DEL TUTOR DE LA INVESTIGACIÓN DOCUMENTAL

Yo, **CORREA PERALTA MIRELLA AZUCENA** en mi calidad de tutor de la Investigación Documental como Propuesta práctica del Examen de grado o de fin de carrera (de carácter complexivo), elaborado por los estudiantes **VILLAVICENCIO SÁNCHEZ EDISON JOSÉ, GONZÁLEZ IRRASABAL BRYAN LENIN**, cuyo título es **MODELO DE SISTEMA BASADO EN EL CONOCIMIENTO PARA EL DISEÑO DE SOFTWARE EN EL DOMINIO DE SEGURIDAD DE LA APLICACIÓN**, que aporta a la Línea de Investigación **CICLO DE VIDA DE UN PROYECTO DE SOFTWARE, METODOLOGÍAS Y PLATAFORMAS** previo a la obtención del Grado **INGENIERO EN SISTEMAS COMPUTACIONALES**; considero que el mismo reúne los requisitos y méritos necesarios en el campo metodológico y epistemológico, para ser sometido a la evaluación por parte del tribunal calificador que se designe, por lo que lo APRUEBO, a fin de que el trabajo sea habilitado para continuar con el proceso de titulación de la alternativa de Examen de grado o de fin de carrera (de carácter complexivo) de la Universidad Estatal de Milagro.

En la ciudad de Milagro, a los 24 días del mes de mayo de 2018.

CORREA PERALTA MIRELLA AZUCENA

Tutor
C.I.: 091961590-6

APROBACIÓN DEL TRIBUNAL CALIFICADOR

El tribunal calificador constituido por:

MIRELLA AZUCENA CORREA PERALTA

LISSETT MARGARITA AREVALO GAMBOA

DENIS DARIO MENDOZA CABRERA

Luego de realizar la revisión de la Investigación Documental como propuesta practica, previo a la obtención del título (o grado académico) de INGENIERO EN SISTEMAS COMPUTACIONALES presentado por el señor EDISON JOSÉ VILLAVICENCIO SÁNCHEZ.

Con el título: **MODELO DE SISTEMA BASADO EN EL CONOCIMIENTO PARA EL DISEÑO DE SOFTWARE EN EL DOMINIO DE SEGURIDAD DE LA APLICACIÓN.**

Otorga a la presente Investigación Documental como propuesta práctica, las siguientes calificaciones:

Investigación documental	[80]
Defensa oral	[20]
Total	[100]

Emite el siguiente veredicto: (aprobado/reprobado) APROBADO

Fecha: 24 de mayo del 2018.

Para constancia de lo actuado firman:

	Nombres y Apellidos	Firma
Presidente	MIRELLA AZUCENA CORREA PERALTA	
Secretario /a	DENIS DARIO MENDOZA CABRERA	
Integrante	LISSETT MARGARITA AREVALO GAMBOA	

APROBACIÓN DEL TRIBUNAL CALIFICADOR

El tribunal calificador constituido por:

MIRELLA AZUCENA CORREA PERALTA

LISSETT MARGARITA AREVALO GAMBOA

DENIS DARIO MENDOZA CABRERA

Luego de realizar la revisión de la Investigación Documental como propuesta practica, previo a la obtención del título (o grado académico) de INGENIERO EN SISTEMAS COMPUTACIONALES presentado por el señor BRYAN LENIN GONZÁLEZ IRRASABAL.

Con el título: **MODELO DE SISTEMA BASADO EN EL CONOCIMIENTO PARA EL DISEÑO DE SOFTWARE EN EL DOMINIO DE SEGURIDAD DE LA APLICACIÓN.**

Otorga a la presente Investigación Documental como propuesta práctica, las siguientes calificaciones:

Investigación documental	[80]
Defensa oral	[20]
Total	[100]

Emite el siguiente veredicto: (aprobado/reprobado) APROBADO

Fecha: 24 de mayo del 2018.

Para constancia de lo actuado firman:

	Nombres y Apellidos	Firma
Presidente	MIRELLA AZUCENA CORREA PERALTA	
Secretario /a	DENIS DARIO MENDOZA CABRERA	
Integrante	LISSETT MARGARITA AREVALO GAMBOA	

DEDICATORIA

Dedico el presente trabajo a Dios, por darme iluminación y enseñarme grandes lecciones de fe, por darme una familia extraordinaria y algo caótica, por permitirme alcanzar a unos de los momentos más importantes de mi formación profesional.

A mi madre, su apoyo incondicional, cariño y consejo, enseñándome el valor del sacrificio y constancia, a pesar de momentos difíciles que se haya pasado. A mi padre, por la confianza, por apoyarme siempre en las ideas y metas propuestas, a pesar de nuestras enormes diferencias de pensamiento, perennemente pendiente de mi estudio.

A mi abuelita Laura, a pesar de sus tediosas expresiones, siempre dispuesta a aconsejar, dialogar y ayudar en cualquier momento.

A mi abuelito Mauro, que desde el cielo me cuida y llena de prosperidades.

A mis catedráticos, que se convirtieron en buenos amigos y siempre allí con los consejos académicos y de vida.

A mis amigos, compañeros y conocidos, pudiese nómbralos a cada uno de ustedes, pero debo de hacer espacio para la dedicatoria de mi amigo, sino se va a molestar conmigo.

Edison José Villavicencio Sánchez

Dedico este trabajo a Dios, por su infinita sabiduría, por permitirme llegar a este momento especial y memorativo en mi vida, mi nueva etapa como profesional.

A mis padres, a quienes amo por apoyarme en todo ámbito, valorando sus consejos y esfuerzos, brindándome los recursos necesarios sabiéndolos aprovechar, con mucho cariño a mis hermanos, han sido parte de mis estudios, en haberme ayudado en muchas circunstancias.

A mis abuelitas, por el amor que me brindan, siendo concejeras en el transcurso de mis estudios; a mi abuelito por su apoyo, alentándome a continuar mis estudios y a mis tíos por haberme depositado confianza en mí en especial a mi tío Carlos que con estas palabras junto a mi hermano, marcaron mi vida: "estudien mijos, yo no quiero que sean como yo, sean mejores", hoy no estas presente en esta tierra pero si estas en nuestros corazones.

A mí enamorada Angélica por ser parte de muchos momentos a mi lado y la motivación que me da para seguir adelante con mis estudios.

A mis amigos, y amigos docentes que han sido parte de mis estudios e inconvenientes el cual todo estudiante pasa; me han apoyado y alentando para seguir triunfando.

Bryan Lenin González Irrasabal

AGRADECIMIENTO

A Dios, por darme fuerzas en los momentos difíciles, por darme salud, inteligencia y disciplina para culminar esta formación profesional.

A mis padres, por la confianza y apoyo brindado, demostrándome su amor con una taza de café o agua aromática en cada malanoche que he tenido durante la carrera, por apagar el foco de mi cuarto cuando me quedaba dormido como gato, por corregirme en mis faltas y ser un ejemplo de vida, de lucha, superación y sacrificio.

A Mirella Correa Peralta, mi tutora y profesora, a quién considero como una mamá, debido a su buen corazón, sus conocimientos y consejos académicos que me ha transmitido, por el tiempo dedicado en este proyecto y por supuesto, por las veces que se ha gozado de las escrituras que hemos presentado.

A mis hermanos, Marcel y Joel, a pesar momentos inmemoriales y discusiones que se tiene, siempre están con ideas para estudiar e importunar.

A mis amigos, quienes a pesar de penas y alegrías, siempre han estado allí con sus ocurrencias e ideas.

Edison José Villavicencio Sánchez

Agradezco a Dios, por darme las fuerzas y la sabiduría necesaria para poder culminar este trabajo, por la gran bendición en darme a los padres más buenos, siendo pilares fundamentales en mi vida me han apoyado en todo y siempre estaré agradecido, a mis hermanos, abuelitos, tíos, mi enamorada, y amigos que han formado parte de mi vida profesional a las que me encantaría agradecerles su amistad, consejos y apoyo.

A mi institución Universidad Estatal de Milagro por haber permitido estudiar y ser parte de esta evolución académica, a mis docentes por haberme enseñado lo necesario para enfrentarme al mundo laboral y en especial a mi tutora Ingeniera Mirella Correa por guiarme en este trabajo y haberme tenido mucha paciencia.

Gracias a todos por todo lo que me han brindado y por todas sus bendiciones estaré siempre agradecido.

Bryan Lenin González Irrasabal

ÍNDICE GENERAL

DERECHOS DE AUTOR II
APROBACIÓN DEL TUTOR DE LA INVESTIGACIÓN DOCUMENTAL III
APROBACIÓN DEL TRIBUNAL CALIFICADOR IV
DEDICATORIA VI
AGRADECIMIENTO VII
ÍNDICE GENERAL VIII
ÍNDICE DE FIGURAS IX
ÍNDICE DE TABLAS X
RESUMEN 1
ABSTRACT 2
INTRODUCCIÓN 3
PROBLEMA DE INVESTIGACIÓN 5
MARCO TEÓRICO CONCEPTUAL 8
METODOLOGÍA 15
DESARROLLO DEL TEMA 17
CONCLUSIONES 26
REFERENCIAS BIBLIOGRÁFICAS 28

ÍNDICE DE FIGURAS

Figura N° 1: Representación conceptual de las áreas involucradas en el SBC 9

Figura N° 2: Propósitos que destacan el SBC 9

Figura N° 3: Adaptado de Carreto Arellano, 2014. 11

Figura N° 4: Metodología empleada en la Investigación Propuesta. 15

Figura N° 5: Ventajas de la investigación bibliográfica documental. 16

Figura N° 6: Desventajas de la investigación bibliográfica documental. 16

Figura N° 7: Cybersecurity Workforce Framework en base al conocimiento de seguridad cibernética y su arquitectura. 19

Figura N° 8: Plataforma de análisis predictivo de CPSI – ONWATCH para administración de información energética en infraestructuras. 20

Figura N° 9: Esquema gráfico de las fases fundamentadas en el conocimiento de la seguridad de aplicaciones frente a ataques u vulnerabilidades del proyecto de aplicación web de código abierto OWASP. 22

Figura N° 10: Detalle de las funciones principales de la herramienta de modelado libre Archi para la arquitectura de software establecido en conocimiento y peritaje en la toma de decisiones. 23

Figura N° 11: Transformación de habilidades de un equipo de desarrollo de software en conocimiento y experiencia. 24

ÍNDICE DE TABLAS

Tabla 1. Diferencia entre investigación documental e investigación bibliográfica. 15

Tabla 2. Desarrollo de software infalible en base al conocimiento de seguridad cibernética y su arquitectura. 18

Tabla 3. Comparación entre medidas de recomendación de seguridad y la relación del conocimiento en la seguridad del software. 20

Tabla 4. Análisis, métodos y neutralización de vulnerabilidades basados en el conocimiento de la seguridad de aplicaciones. 21

Tabla 5. Método de evaluación y estrategias de arquitecturas en el desarrollo del diseño de aplicaciones basadas en el conocimiento de seguridad. 23

Tabla 6. Experiencias, requisitos e incorporación de conocimientos en seguridad y la relación de las habilidades de seguridad con el diseño y desarrollo de software. 25

Modelo Knowledge Based System para el diseño de software en el dominio de la seguridad de las aplicaciones

RESUMEN

El diseño de software fundamentado en el dominio de seguridad de aplicaciones abarca un sin número de metodologías instituidas en buenas prácticas de desarrollo de software, arquitecturas, experiencias y habilidades establecidas en el conocimiento de seguridad informática; al mismo tiempo de puntualizar investigaciones en delineaciones de diseño y dominio en protección de datos e información, se demuestra la interacción de aplicaciones basadas en conocimiento para cumplir los requerimientos de defensa ante fallos críticos u vulnerabilidades, apreciando diversos aspectos en relación a los datos de ataques, procesos o criterios de análisis en la estructura de predicción o monitoreo. Se efectuó una investigación bibliográfica y documental realizando una búsqueda en repositorios de revistas, artículos y ensayos científicos como Scopus, Redalyc y ScienceDirect. Se asimilaron diversas evaluaciones y técnicas basadas en conocimiento de seguridad de información enfocadas a la arquitectura del software, vulnerabilidades y amenazas en el código e implementación, desplegando ciertos aspectos de innovación en el procedimiento de clasificación: normas de reconocimiento, impactos de riesgos en directorios u registros, entre otros; a su vez, se contrasto diversas estrategias cimentadas en experiencias y habilidades de seguridad, incidiendo en la detección de patrones de ataques y accesos no autorizados, ingresados en bibliotecas de reglas difusas mediante un complejo modelo matemático, ajustándose en una estrategia de seguridad de información por juicio de especialistas con el único fin de realizar una efectiva correlación entre la evolución del comportamiento en detección y el tiempo de respuesta de predicción para enfrentar amenazas, conjuntamente este desempeño proporciona una clara visión del estado de la organización en patrones de diseño y la representación de la eficiencia en planes de contingencia frente a coacciones; indubitablemente se refleja un proceso de conocimiento en alineación a la optimización de requerimientos, probabilidad de errores y necesidades implícitas fuera del diseño de calidad de seguridad.

PALABRAS CLAVE: Dominio de seguridad, Seguridad de aplicaciones, diseño de software.

Model Knowledge Based System for the design of software in the application security domain

ABSTRACT

Software design based on application security domain covers a number of methodologies instituted in good software development practices, architectures, experiences and skills established in the knowledge of computer security; at the same time to clarify research in design and domain delineations in data protection and information, it demonstrates the interaction of knowledge based applications to meet the requirements of defense against critical failures or vulnerabilities, appreciating various aspects in relation to the data of attacks, processes or criteria of analysis in the structure of prediction or monitoring. A bibliographical and documentary investigation was carried out conducting a search in repositories of magazines, articles and scientific essays as Scopus, Redalyc and ScienceDirect. Have been assimilated various evaluations and techniques based on knowledge of security of information focused on the architecture of the software, vulnerabilities and threats in the code and implementation, deploying certain aspects of innovation in the classification procedure: rules of recognition, impacts of risks in directories or registries, among others, at the same time, various strategies based on experiences and security skills were contrasted, affecting the detection of patterns of attacks and unauthorized accesses, admitted to rule libraries diffuse through a complex mathematical model, conforming at a strategy of information security by trial by specialists with the sole purpose of performing an effective correlation between the evolution of the behavior in the detection and response time of prediction to confront threats, jointly this performance provides a clear vision of the state of the organization in bosses of design and the representation of the efficiency in risk plans opposite to coercions; unquestionably reflects a process of knowledge in alignment to the optimization of requirements, likelihood of errors and implied needs outside the design of quality of security.

KEY WORDS: Domain security, application security, software design.

INTRODUCCIÓN

El diseño de software en el dominio de un Sistema Basado en Conocimiento (SBC) aplicado al análisis de seguridad de las aplicaciones tiende a dar prioridad a la aplicación de normas, estándares y prácticas existentes en la comunidad informática considerando las vulnerabilidades presentes en las aplicaciones.

Durante el desarrollo en el **Capítulo I,** se da a conocer la problemática del diseño de software en el dominio de la seguridad de las aplicaciones, la vulnerabilidad es el principal problema de seguridad en las aplicaciones, acceso no autorizado a páginas o sitios web y las fallas que se genera en el entorno informático pues existe un alto riesgo de pérdida de información que trae como consecuencia la falta de integridad, confiabilidad y disponibilidad de los datos. El objetivo principal de la investigación es demostrar las capas de infraestructura de un modelo de sistema basado en conocimiento para el diseño de software en el dominio de la seguridad de las aplicaciones, donde la información sirve para construir sistemas capaces de aprovechar y formalizar el conocimiento del dominio y sea punto de partida para continuar con el estudio e indagación del tema de investigación presente.

En el **Capítulo II,** refleja la definición del contexto del problema que se lleva a cabo, las áreas involucradas en la problemática como la ingeniería del conocimiento, la seguridad de la información, ingeniería de requerimientos el cual conforman los sistemas basados en conocimientos.

También se da a conocer los modelo de sistemas del conocimiento el cual está constituido por muchas etapas, los estado del arte del dominio de la seguridad de las aplicaciones, la seguridad de la información y las infraestructura de capas propuesta el cuales son la capa de autenticación, capa de servidor de aplicaciones, capa de programas ejecutables y capa de seguridad de datos.

En el **Capítulo III** se detalla metodología de la investigación desde el aspecto documental y descriptiva a partir de fuentes bibliográficas, hemerográficas con la finalidad de ser analizada de las base de datos como Scopus, Redalyc y ScienceDirect.

En el **Capítulo IV** consiste en el desarrollo del tema donde refleja y analizan las comparaciones de los diferentes modelos de SBC para el diseño de software en el dominio de la seguridad de las aplicaciones y exponen los resultados obtenidos a través de la investigación.

En el **Capítulo V** presenta la conclusión del trabajo realizado y soluciones a tomar en cuenta, con la finalidad que la comunidad informática ponga en práctica el aporte investigativo al ampliar el desarrollo del SBC, para dar soluciones a problemas presentes, con base a comparaciones de otros documentos que detallan sobre la problemática y obtener capas de desarrollo de los software en el dominio de un SBC aplicado al análisis de seguridad de las aplicaciones pretende ser una contribución con la seguridad de las aplicaciones.

CAPÍTULO 1

PROBLEMA DE INVESTIGACIÓN

Planteamiento del Problema

En la actualidad existen grandes cambios tecnológicos que se han venido generando conforme al desarrollo de las aplicaciones informáticas requeridas por las organizaciones; sin embargo, se hace imperioso tener aplicaciones desde la web con acceso a base de datos ejecutados en mainframes a través de capas y abarcando plataformas que requieren entornos de seguridad con estándares que se alineen a la tecnología. Debido a la problemática dada sobre el diseño de software, dominio de seguridad de las aplicaciones, vulnerabilidades entre otros, crean un agujero ya sea en el diseño, implementación o en el acceso de las aplicaciones. Estas vulnerabilidades en forma general pueden ser:

- **Inmadurez en el conocimiento de los problemas de seguridad:** Los problemas de seguridad en las aplicaciones web cubren una gran parte de responsabilidad del programador debido a la falta de seguimiento en las entradas y salidas del sistema. El uso del parámetro register_globals, comúnmente utilizado por administradores como prioridad en la configuración, cubre el origen de los datos, pues al encontrarse habilitado existe mayor riesgo de acceso desde una variable que ingresó al sistema.
- **Fallas de Inyección:** Momento que presenta una aplicación web cuando transita información de una petición HTTP a través de una solicitud externa, utiliza parámetros al momento de acceder a los sistemas operativos locales y externos. Al inyectar comandos maliciosos internamente en la secuencia de los parámetros tendrá acceso a la aplicación Web.
- **Fallas de Cross Site Scripting (XSS):** Se encarga de crear y enviar código o script malicioso donde la aplicación web manipulada como un mecanismo que afecta al navegador de los usuarios finales, desde el acceso a la sesión del usuario, atacando la máquina local o enmascarando información de una página HTML. Este tipo de vulnerabilidad es usada para burlar los controles de acceso o al crear ataques de phishing y abusos en los navegadores.

- **Fallas de Cross Site Request Forgery (CSRF)**: Los ataques CSRF o falsificación de petición en sitios cruzados se producen cuando el atacante causa que el usuario realice una acción maliciosa de manera no intencionada en una aplicación.
- **Fallas de Autenticación y Administración de Sesión:** Surge cuando la información personal de las cuentas de usuarios y los tokens de acceso en las sesiones no se encuentran protegidos y los atacantes tengan acceso a contraseñas asumiendo identidades de otros usuarios.
- **Inadecuada configuración de seguridad:** Debe implementar y conservar una configuración segura en relación a aplicaciones, servidores web, framework, servidor de aplicaciones y plataformas existentes.
- **Almacenamiento Inseguro:** Las aplicaciones web recurren a funciones de criptografías para proteger información sensible y credenciales de usuarios, sin embargo, existen funciones como algoritmos que en ocasiones no han sido codificadas apropiadamente, donde pueden cometer delitos por la mala manipulación de la información.
- **Fallas al restringir accesos a URL:** Las aplicaciones cumplen en proteger funcionalidades sensibles evitando que se expongan URLs a usuarios que no se encuentren autorizados, donde las aplicaciones deben controlar el ingreso a una página el cual cuente con permisos necesarios a los usuarios, pues pueden atacar ejecutando operaciones no autorizadas a través de páginas ocultas generando delitos informáticos.
- **Protección insuficiente en la capa de transporte**: En general las aplicaciones tienden a fallar al momento de cifrar tráfico en la red. Durante el manejo de información sensible que debe ser protegida en el transcurso de la comunicación y evitar inconvenientes utilizando algoritmos de cifrados fuertes para aumentar niveles de seguridad con utilizar certificados permitidos.
- **Re direccionamiento sin validar:** Existen aplicaciones web que redirigen a los usuarios a diferentes páginas o sitios usando datos no confiables, es frecuente especialmente en las aplicaciones que presentan publicidad, obligando a acceder a páginas no autorizadas.

Otro tipo de vulnerabilidad de seguridad informática que con frecuencia se dan en las aplicaciones web es el Phishing, son ataques que generan combinaciones de ciertos mecanismos sencillamente vulnerables de protección de acceso a la aplicación web,

implicando el usuario y contraseña adicional a la capacidad inherente de los usuarios a revelar cualquier información detallada.

Objetivos

Objetivo General

- Describir estudios documentales acerca del modelo de sistema basado en conocimiento para el diseño de software en el dominio de la seguridad de las aplicaciones.

Objetivos Específicos

- Seleccionar fuentes de información relacionada al sistema basado en conocimiento
- Identificar estudios científicos acerca de las vulnerabilidades en las aplicaciones por falta de seguridad de la misma.
- Concluir el impacto de la información documental acerca del diseño de software para el dominio de la seguridad de las aplicaciones.

Justificación del Problema

Este trabajo de investigación se da a conocer el modelo de Sistema Basado en Conocimientos (SBC) para el diseño de software en el dominio de la seguridad de las aplicaciones, el cual cumplan con la elaboración de especificaciones de requerimientos de software (ERS), con el fin de contribuir en el desarrollo de aplicaciones y ayuden de manera eficiente a disminuir las potenciales vulnerabilidades que se presentan, como también acceder a evaluar niveles de seguridad, contribuyendo en refinamiento del conocimiento, permitiendo analizar paso a paso la exploración y el mantenimiento del software, pues los programas que manipulan conocimiento son codificados con la finalidad de solucionar problemas en un dominio especializado a la experiencia humana.

Este trabajo se considera documental pero también práctico que aporta al grupo de investigación de la Universidad Estatal de Milagro, Tics y desarrollo de software, en aporte a la línea de ciclo de vida de un proyecto de software, metodologías y plataformas en el área de calidad en desarrollo de software.

CAPÍTULO 2

MARCO TEÓRICO CONCEPTUAL

Las áreas involucradas en la problemática de estudio se encuentran:

Ingeniería del conocimiento

La Ingeniería del conocimiento (INCO) es el proceso de diseñar y hacer operativos los Sistemas basados en el conocimiento, se deriva de la Inteligencia Artificial respecto a la adquisición, representación y aplicación de conocimientos; éste se integra en un sistema de computador para solucionar problemas complejos donde normalmente requiere un alto nivel de experiencia y capacidad humana(Bajarlía, Ierache, & Eterovic, 2013).

Seguridad de la información

Consiste en proteger la información y acceso a los sistemas, para prevenir utilización, destrucción o divulgación no autorizada, englobando el área de la seguridad de aplicación de gestión.

Según ISO27001, se refiere a la integridad, confidencialidad y disponibilidad de la información y datos significativos de la organización, independientemente del formato que tengan.

Ingeniería de requerimientos

Es el proceso encargado de recopilar, analizar y verificar las necesidades del usuario de un sistema de software; la ingeniería de requerimientos (IR) debe cumplir la especificación de los requerimientos de software, el cual debe de ser correcta, completa y no ambigua. En otras palabras es una disciplina para desarrollar una especificación completa y consistente, la cual será útil para acuerdos usuales abarcando todas las partes involucradas, dando a conocer en qué consisten las funciones del sistema a ser ejecutado (Bajarlía et al., 2013). Radica inicialmente en el estándar IEEE-830 de Especificación de Requisitos de Software (ERS) al desarrollar aportes en función del modelo de conocimiento y desde el trabajo con expertos del área de Seguridad de la Información.

Sistemas basados en conocimientos

Los sistemas basados en conocimientos (SBC) son programas capaces de resolver problemas usando un determinado dominio de conocimiento, esta base de conocimiento se convierte en lo más importante y lo produce un usuario especializado o experto en el dominio, los ingenieros del conocimiento pues son diferentes a los programadores de la interfaz porque analizan para entender el problema, generan solución son los expertos en todo, en cambio los programadores su práctica los lleva a escribir código limpio produciendo software de calidad(Badaró, Javier Ibañez, & Agüero, 2013).

Los SBC consisten en la implementación de un sistema que frecuente a la elaboración de especificaciones de seguridad de la aplicación basada en la ERS, el desarrollo de implementación de un prototipo de SBC para la observación, el análisis y evaluación de ERS dirigido en aspectos de seguridad de la información, desde una perspectiva de la IR. Como se observa en la Figura 1 las áreas involucradas en el SBC (Bajarlía et al., 2013).

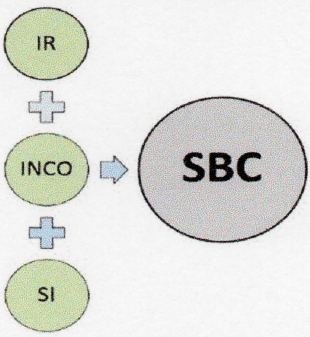

Figura N° 1: *Representación conceptual de las áreas involucradas en el SBC*
Elaborado por: *Villavicencio Edison & González Bryan.*

Los sistemas basados en conocimiento alcanzan grandes complejidades como se observa en la Figura N°2.

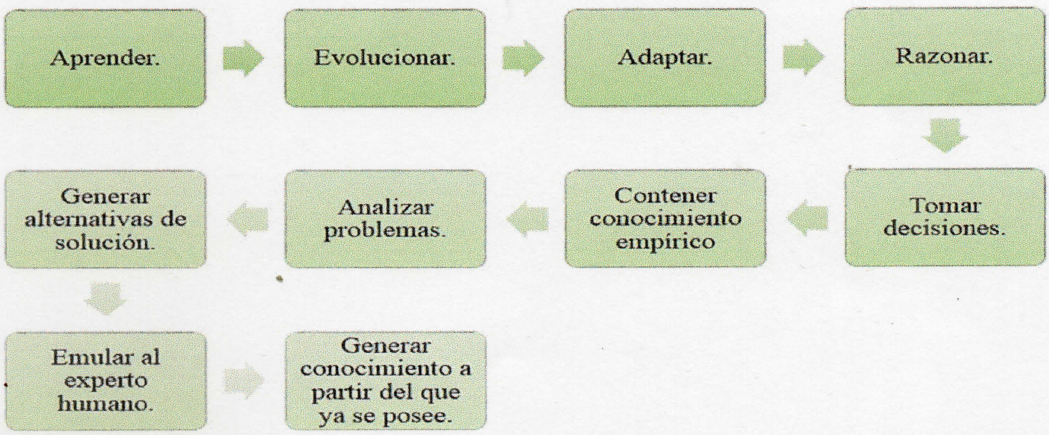

Figura N° 2: *Propósitos que destacan el SBC*
Elaborado por: *Villavicencio Edison & González Bryan.*

Modelo de sistemas del conocimiento

En la actualidad muchas organizaciones tienden a la necesidad de información y acceso a la misma donde resultan ser diferentes al momento de acceder, es difícil requerir información en cualquier momento. Sin embargo, en obtener toda la información a disposición de todos los usuarios siempre será un grave riesgo, hablando de seguridad, integridad, confiabilidad y otros aspectos que pueden generar daño al momento de ser manipulados(Chadwick Carreto, 2014).

Por lo tanto debe realizar una reestructuración en el acceso y la administración de la información donde interviene la administración del conocimiento, de forma significativa.

Un Modelo de Sistema de Conocimiento está constituido por etapas de depuración, transformando los datos a información y este a conocimiento siendo útil el perfil y la necesidad del usuario.

Las etapas son:

- Identificar, organizar y almacenar datos e información considerando los perfiles del usuario.
- Identificar obtener y determinar el conocimiento existente.
- Refinar los datos e información para mejorar la facilidad de la creación del nuevo conocimiento a generar.
- Empezar la innovación por medio de la reutilización y apoyo de la habilidad del conocimiento creado.
- Aplicar y los conocimientos generados, facilitando el proceso de enseñanza.

El modelo de etapa más importante es refinar o depurar los datos y transformarlos en conocimientos para un debido entendimiento, donde resulta de suma importancia, que permita abarcar todo este conocimiento obtenido en un proceso de enseñanza.

Para el diseño y desarrollo de un Modelo de sistema de Conocimiento que permita lo antes mencionado como se observa en la figura N°3:

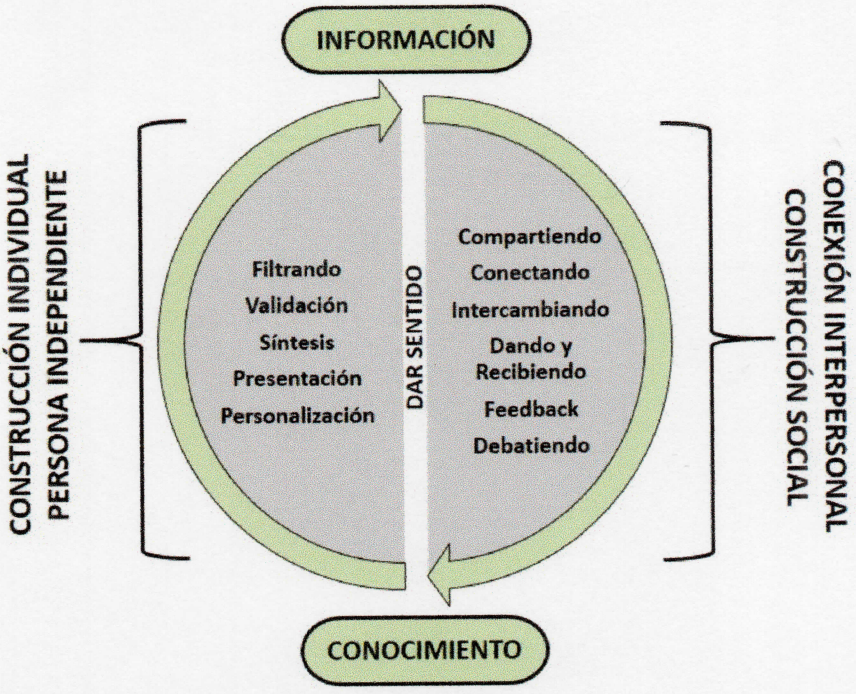

Figura N° 3: *Adaptado de Carreto Arellano, 2014.*

Diseño y desarrollo de un Modelo de sistema de Conocimiento

Metodología I.D.E.A.L

Para la construcción del modelo se escogerá una metodología apropiada de suma importancia el cual debe tomarse como referencia un manual de procedimiento a seguir que conlleve a algo imperativo al ejecutar esta metodología, consta de cinco fases las cuales optan por el nombre IDEAL que se muestran a continuación:(Chadwick Carreto, 2014)

- La Fase I: Identificación de la tarea. Es la etapa el cual se considera los objetivos del proyecto del SBC, involucrando el proceso de adquisición de conocimiento. El cual consiste en obtener los conocimientos necesarios referido al marco regulatorio con el fin de brindar seguridad informática(Chadwick Carreto, 2014).
- La Fase II: Desarrollo del prototipo. Se considera la primordial etapa de la metodología, tomando como referencia la adquisición de conocimientos, llevando a cabo la viabilidad del sistema y llegando a conceptualizar y formalizar los conocimientos e implementación del desarrollo del prototipo permitiendo validar el modelo de SBC(Chadwick Carreto, 2014).
- La Fase III: Ejecución en la construcción del sistema integrado. Este integra los sistemas experto (SE) internamente en un SBC general(Chadwick Carreto, 2014).

- La Fase IV: Actuación para obtención del mantenimiento perfectivo sobre el conocimiento. Incorpora nuevos conocimientos. Donde existe confrontación entre la participación del usuario contra la devolución por medio de las respuestas que se generan en el sistema, siendo útil para el mantenimiento actualizado del conocimiento(Chadwick Carreto, 2014).
- La Fase V: Lograr una apropiada transferencia tecnológica. Esta fase se encarga de comprender las actualizaciones que se dan en el transcurso del conocimiento dando a conocer de manera clara y especifica(Chadwick Carreto, 2014).

Estado del arte del dominio de la seguridad de las aplicaciones

Seguridad de la información

Conforme avanza la información que genera el entorno; la integridad, disponibilidad y confidencialidad de datos cada vez es menor en relación al manejo de la información actual, desde este punto de vista se plantea como interrogantes ¿Cómo actuar ante problemas de datos para obtener información de calidad? ¿Cuál será el mejor proceso para realizar una correcta experimentación de datos? ¿Qué efectos provoca el uso de herramientas para mermar las irregularidades de datos? ¿Cómo afecta la seguridad de información a la calidad de datos bajo reglas de integridad?

Una correcta conceptualización en relación a la seguridad de información es la protección de datos digitales mediante la privatización de accesos a bases de datos usando credenciales eficientes bajo ciertas condiciones de uso, adhiriéndose a ciertas regulaciones en determinados casos de recuperación o denegación de datos, además de complementar con un exhaustivo algoritmo de validación de datos basura, determinando condiciones en tiempos de respuesta, procesos y recursos de manipulación.

En relación a la seguridad de la información, desde una perspectiva de conocimiento basado en calidad, protección y de estrategia, se puede concluir:

- Confidencialidad: Protección explícita del uso de datos a personas autorizadas acorde al nivel de designación.
- Integridad: Certificar la fidelidad de información en base al acceso de datos a personas autorizadas, denegando el acceso de adición, modificación o eliminación

de información a personas no autorizadas, sea de manera intencional o convencional.

- Disponibilidad: Asegurar el acceso exhaustivo de información en respuesta de tiempo y lugar de ubicación geográfica de búsqueda.

Asimismo, se precisa de un modelo de contingencia para proteger la información almacenada en medios físicos de catástrofes naturales o amenazas del entorno, conllevando a la cohesión de procedimientos organizacionales y recursos para evadir o enfrentar dichas coacciones, teniendo en cuenta que la mejor medida de seguridad es la calidad de la información en el conjunto de procesos de captación del usuario final(Netto & Silveira, 2007).

Capa de autenticación

Un recordatorio del requisito fundamental de un sistema de información robusto es la seguridad que emplea al iniciar su ejecución, alcanzado los respectivos niveles de seguridad designados en la representación de datos, permitiendo satisfacer a los usuarios en general la funcionalidad explícita del uso especificado; empero, la abstracción de los objetos del mundo real debe contener un enfoque de calidad de contenido, generando una correcta flexibilidad en la estructura para evitar redundancias de datos o el incumplimiento de principios técnicos de diseño(Verma, Yu, & Sadler, 2015).

Por lo general, la estructura de autenticación se origina en base a las relaciones de entidades con sus respectivos atributos, conllevando a cierta complejidad un conjunto de reglas del tipo estructural con el único fin de generar eficiencia y eficacia en la información, puesto que, a medida de la delineación cognitiva y psicológica, y del proceso representacional, garantiza en cierta parte, la calidad del dato y la transformación del dato a información(Verma et al., 2015).

Capa de servidor de aplicaciones

El servidor de aplicaciones permite el desarrollo de aplicaciones concretamente escalables y de alta disponibilidad en descripción a una estructura modular, interconectando la lógica de negocio con la lógica de datos, formando parte del inicio del diseño y arquitectura de la aplicación, siendo centralizada o distribuida por el factor o alcance de recursos a disposición, además de la especificación de la tecnología a usarse en el desarrollo y por ende, el tipo de herramienta para su implementación(Patra, Naveen, & Prabhakar, 2017).

Por consiguiente, los procesos lógicos de funcionalidad ayudan de manera determinada a la ejecución de la aplicación en diferentes entornos, desde la seguridad del tráfico de datos hasta la integridad de la información proporcionada, a continuación, se nombrará los mejores servidores de la actualidad, categorizando en:

- Servidores de aplicaciones libres
    - WidFly
    - GlassFish
    - Apache Geronimo
    - Apache TomEE
- Servidores de aplicaciones privados
    - IBM WebSphere Application Server
    - Oracle Weblogic Server

Capa de programas ejecutables

Algunas arquitecturas basadas en la aplicación de distribución o en capas, mejoran en cierta perspectiva la seguridad e integridad de información, debido al uso orientado a objetos y al pensamiento analítico del desarrollo, fundamentalmente la gestión de datos puede implantar ciertos riesgos en el diseño de la lógica del negocio y en la aplicación, llevando a generar deliberadamente a un ruido de dato no transversado.

Cada vez menos posibilidades inquietantes en la seguridad del desarrollo de la aplicación de base de datos relacionales distribuidos generan un control de mantenimiento en la recuperación o modificación de datos, diferenciando al uso de archivo de aplicaciones de la independencia de datos(Bortolosso, Rossi, Pelegrini, Dalcanton, & Castella, 2017).

Capa de seguridad de datos

La porción del esfuerzo por contrarrestar las amenazas digitales representa parte del esfuerzo total de las amenazas físicas en acción, siendo su resultado el impacto final en las bases de datos, implementando desde el robo de datos hasta la suplantación o fraudes de información(Calvo, Gracia, & Bayo, 2017).

Como es natural, la inversión en una semántica de calidad y un modelado conceptual eficiente, genera una estructura robusta en relación a la seguridad de las aplicaciones(Farias, Jeréz, Armán, & Rosales, 2013).

CAPÍTULO 3

METODOLOGÍA

Este estudio presenta la metodología de investigación bibliográfica y documental, para realizar la síntesis del tema expuesto, desde un repertorio de artículos, ensayos y revistas científicas de las base de datos Scopus, Redalyc y ScienceDirect, tanto en revisión de la literatura y en el dominio del desarrollo, refinando en sí una discusión secuencial de los pensamientos de los autores en el impacto del desarrollo de la seguridad del software.

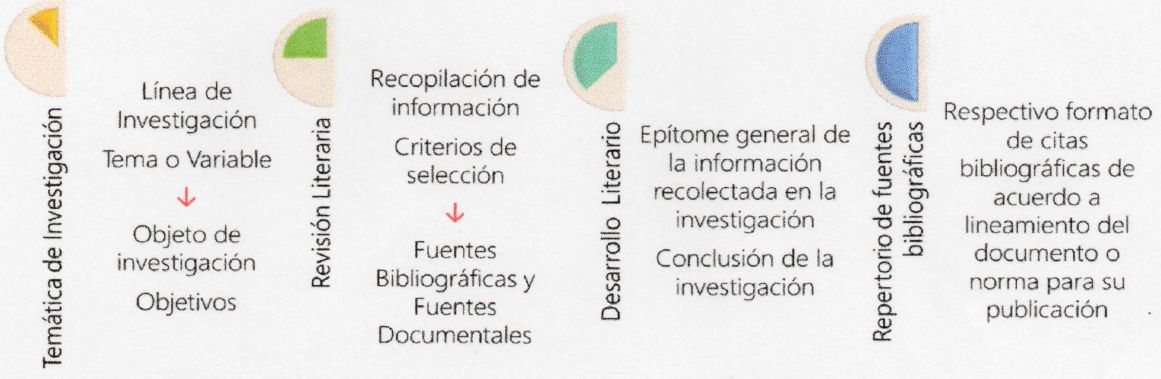

Figura N° 4: *Metodología empleada en la Investigación Propuesta.*
Elaborado por: *Villavicencio Edison & González Bryan.*

Para comprender y simplificar el procedimiento de la investigación bibliográfica y documental expuesta, se ha elaborado la siguiente representación gráfica (Figura N°4) inicia de una línea de estudio con su respectiva variable, comprende el uso de la calidad de selección literaria para continuar con la sinopsis y conclusión del tema, agregando referencias de mayor interés durante la búsqueda de información.

Tabla 1. Diferencia entre investigación documental e investigación bibliográfica.

Investigación documental	Investigación bibliográfica
Información apoyada en revistas, periódicos o editoriales sin comprobar su origen.	Información de carácter científico evidenciando su problema, objetivos e hipótesis y desenlace.

Elaborado por: *Villavicencio Edison & González Bryan*

La investigación documental (Figura N°5 – N°6) consiste en reconocer o recopilar datos formando un contexto de fuente confiable, la técnica se basa a selección de información mediante lectura, se analiza y muestra resultados coherentes.

Investigación Bibliográfica Documental

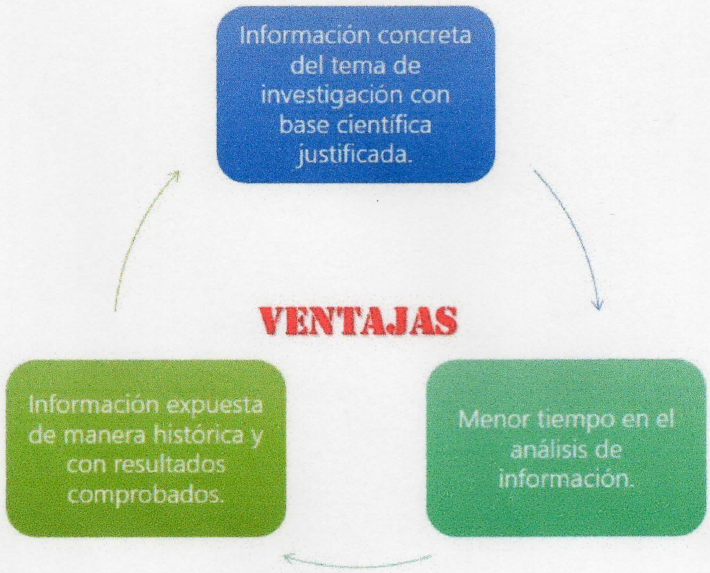

Figura N° 5: *Ventajas de la investigación bibliográfica documental.*

Elaborado por: *Villavicencio Edison & González Bryan.*

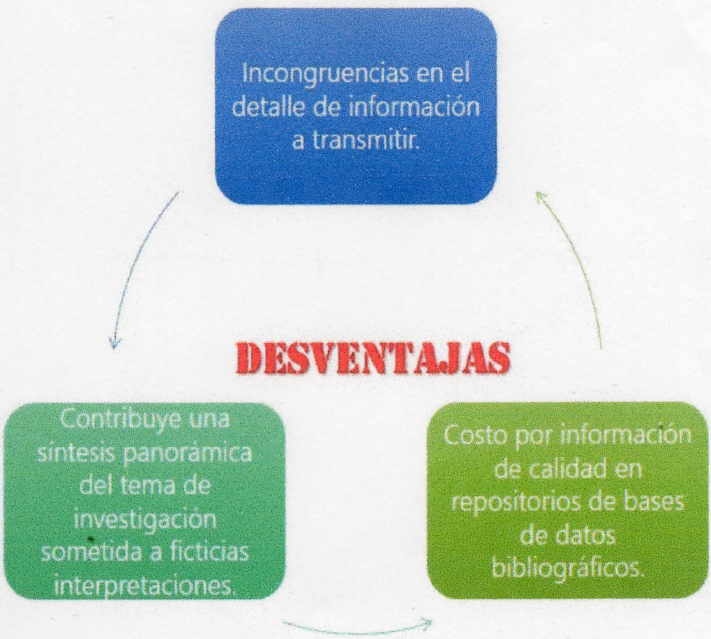

Figura N° 6: *Desventajas de la investigación bibliográfica documental.*

Elaborado por: *Villavicencio Edison & González Bryan.*

CAPÍTULO 4

DESARROLLO DEL TEMA

En el diseño de software basado en conocimiento y dominio de seguridad de aplicaciones, existen estandarizaciones en el desarrollo de la integridad y fiabilidad, debido a las buenas prácticas de organización y procesos de inteligencia fundamentados en experiencias, gestión de procesos basados en recursos e ingeniería de software, se denomina tres categorías en base al conocimiento, seguridad y metodologías, experiencias y habilidades basados en casos reales se seguridad en información, con las siguientes partes:

A. Bases de conocimiento en el desarrollo de la seguridad de aplicaciones.

Comenzando con una perspectiva de distribución, en contra a las amenazas de seguridad en el desarrollo de aplicaciones en tendencia, se han creado diversos modelos o procesos de seguridad informática para validar la calidad de información, a su vez, nuevos algoritmos de encriptación de datos y control de accesos, tecnologías de seguridad en nube, etc; asimismo, el avance imperecedero del proceso secuencial de seguridad en nuevas tecnologías con patrones de reconocimiento en base al conocimiento de vulnerabilidades se encuentra en alta demanda, integrando no solo a la ingeniería de requerimientos ni a la ingeniería de conocimiento, sino a la percepción del desarrollo de software directo a posibles fallas de seguridad por código, implementación, accesos autorizados y no autorizados, generando en sí una base de conocimiento robusta y pluscuamperfecta para relacionar desde una ingeniería inversa, ingeniería social, códigos maliciosos del tipo: troyanos, gusanos, virus polimórficos, phishing, etc., vulnerabilidades: naturales o del entorno, físicas, de interconexiones o redes, hardware y software, y por supuesto, el factor humano. En la **Tabla 2** se evidencia diversas asimilaciones en el estado del conocimiento aplicado al desarrollo de la seguridad, desde el punto de vista de diferentes autores:

Tabla 2. Desarrollo de software infalible en base al conocimiento de seguridad cibernética y su arquitectura.

Autores	Estrategia de Seguridad	Estrategia de Conocimiento
(Jovanovic & Harris, 2016)	Arquitectura de seguridad basada en la evaluación de riesgos cibernéticos y buenas prácticas de desarrollo de aplicaciones.	Modelo de seguridad aplicado al análisis de la codificación y a la evaluación de la seguridad informática. Métodos avanzados de criptografía aplicada a la seguridad de datos, redes y computación en la nube.
(El Hachem, Pang, Chiprianov, Babar, & Aniorte, 2016)	Modelo de seguridad predictivo en el descubrimiento de análisis y resolución de ataques informáticos en cascada.	Capacidad en el dominio de las especificaciones de ataques de seguridad. Refinamiento de mecanismos de análisis y especificaciones de vulnerabilidades. Comportamiento de amenazas mediante criterios de selección y predicción en cascada.
(Hazeyama et al., 2015)	Prospección de requerimientos de seguridad basada en estándares de seguridad digital y vulnerabilidades.	Experimentación de evaluaciones de vulnerabilidades y amenazas. Patrones de ataques con su pertinente categorización. Procedimientos de delineaciones del diseño de seguridad en conocimiento.

Elaborado por: *Villavicencio Edison & González Bryan*

La estrategia que utilizaron los autores (Jovanovic & Harris, 2016) en el desarrollo del software fue el Marco de trabajo de seguridad cibernética el cual corresponde a la Iniciativa nacional para la seguridad cibernética (NICE), este facilita un plan de procedimiento para categorizar, organizar y detallar el trabajo de seguridad cibernética tanto en categorías, Áreas de especialidad, conocimientos y habilidades donde provee un

lenguaje interpretativo para entender sobre roles y empleos cibernéticos y facilita a definir requisitos personales en la seguridad cibernética.

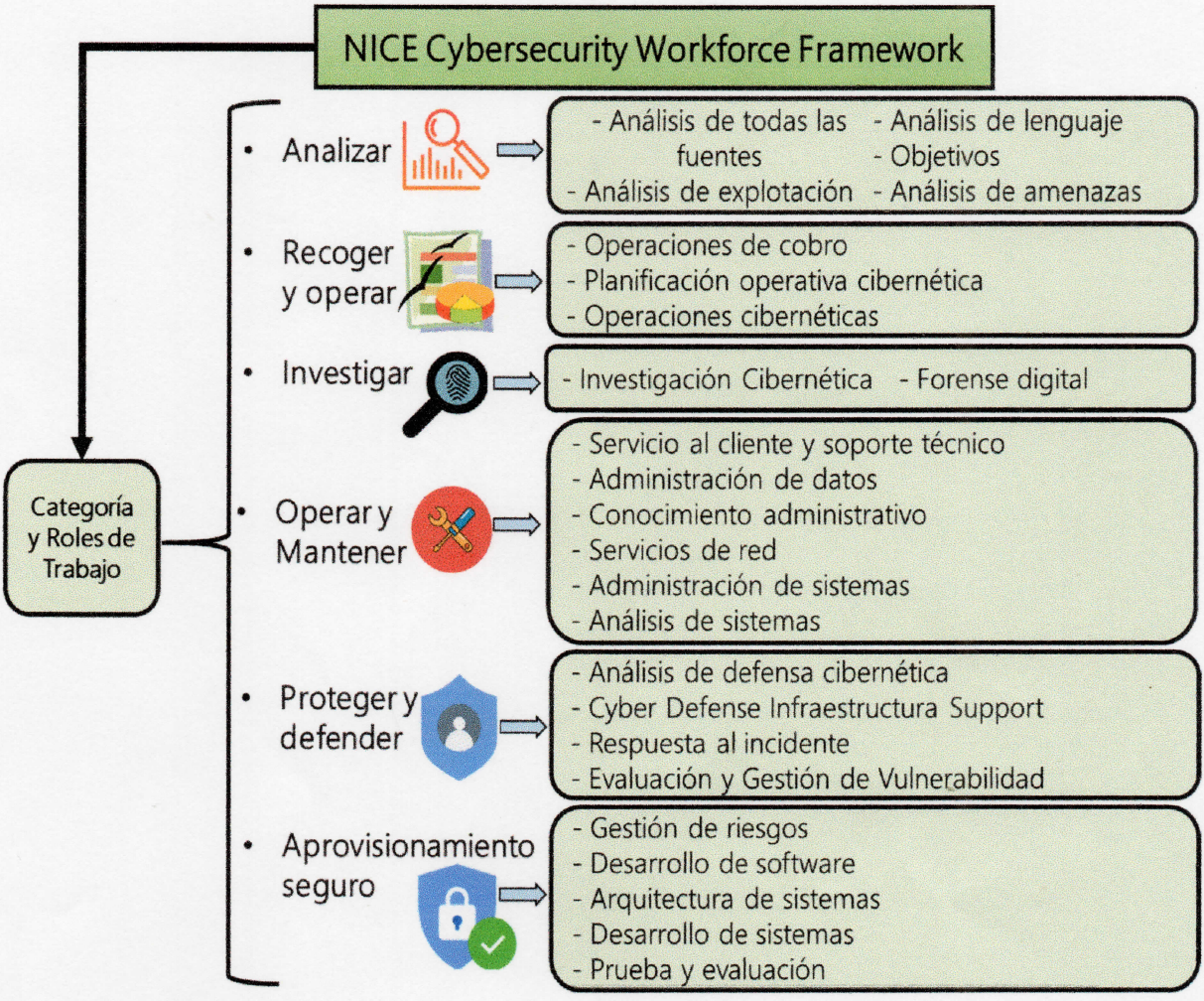

Figura N° 7: *Cybersecurity Workforce Framework en base al conocimiento de seguridad cibernética y su arquitectura.*

Elaborado por: *Villavicencio Edison & González Bryan*

En la **Tabla 3**, se observa el impacto que genera el conocimiento sobre la seguridad del software en base al asesoramiento de información, recordatorios de buenas prácticas de navegabilidad y servicios en tiempo real, conllevando a una visión perpetua de la relación del conocimiento con la seguridad de software para el usuario final. Teniendo en cuenta el estudio de la plataforma de conocimiento en seguridad energética ONWATCH manipulada por los autores (Freitas, Matrawy, & Biddle, 2016) se especifica la capacidad del análisis

predictivo establecido en la gestión de las arquitecturas u infraestructuras de software escalable.

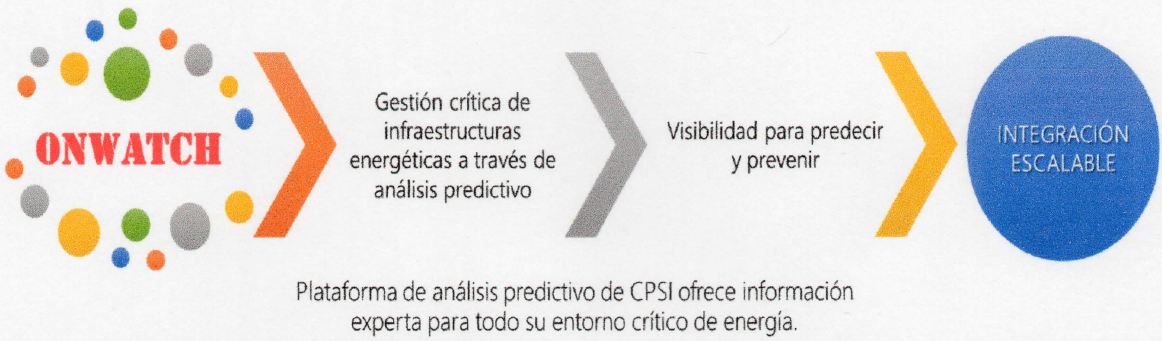

Figura N° 8: *Plataforma de análisis predictivo de CPSI – ONWATCH para administración de información energética en infraestructuras.*
Elaborado por: *Villavicencio Edison & González Bryan*

Tabla 3. Comparación entre medidas de recomendación de seguridad y la relación del conocimiento en la seguridad del software.

Autores	Modelo de comparación de la seguridad del software en base al conocimiento
(Hazeyama, 2012)	Pruebas de seguridad en análisis de requerimientos, funcionalidad y métricas en contramedidas de amenazas.
	Metodología basada en patrones de seguridad y vulnerabilidades, clasificando amenazas estáticas y dinámicas.
	Técnicas de orientación (sugerencias, consejos, etc.) en la toma de decisión para optimizar la seguridad del software ante el usuario final.
(Freitas et al., 2016)	Confianza en la toma de decisión basada en la experiencia colectiva de la seguridad de información.
	Cierta aproximación al Crowdsourcing en el conocimiento de amenazas y vulnerabilidades para la fiabilidad y eficiencia del software para el usuario final.

Elaborado por: *Villavicencio Edison & González Bryan*

B. Prospección, métodos y neutralización de vulnerabilidades basadas en el conocimiento de la seguridad de aplicaciones.

Desde el punto de vista de la seguridad de información, considerando exhaustivas pruebas de la calidad del software en base a vulnerabilidades o explotación de vulnerabilidades, la incorporación del conocimiento despliega patrones para reconocer o identificar amenazas en el sistema, sea este por exploits, proxys, accesos no autorizados, etc., con el fin de neutralizar mediante una serie de complejos algoritmos el modelo de ataque perpetuado para almacenar en una base de datos de conocimiento y dar solución eficiente analizando sus parámetros en el ciclo de desarrollo de la seguridad, como se observa en la **Tabla 4**.

Tabla 4. Análisis, métodos y neutralización de vulnerabilidades basados en el conocimiento de la seguridad de aplicaciones.

Autores	Modelos basados en el conocimiento de seguridad del software
(Wijesiriwardana & Wimalaratne, 2017)	Uso de herramientas de análisis estático de código fuente en detección de la seguridad del software.
	Enfoque de capacidad de análisis en riesgos o vulnerabilidades en el desarrollo de software en tiempo real.
	Integración de prototipos en análisis de la seguridad del software mediante múltiples ataques de vulnerabilidades para comprobar el análisis predictivo del ataque en tiempo real.
(Huang, Dangelo, Miyani, & Lie, 2016)	Código de manejo de errores de vulnerabilidades usando métodos estáticos en el desarrollo y prueba del software.
	Iteración del ciclo de vida de software en la pruebas de seguridad y vulnerabilidades en tiempo real.
(Geng, Ye, & Luo, 2016)	Predicción de vulnerabilidades en el desarrollo y desempeño del software.
	Métodos de aprendizaje autónomo en predicción y solución de diversas vulnerabilidades y amenazas de la seguridad del software.
	Refinamiento de las métricas de seguridad en el desarrollo de software en relación de tiempo – prueba.

Elaborado por: *Villavicencio Edison & González Bryan*

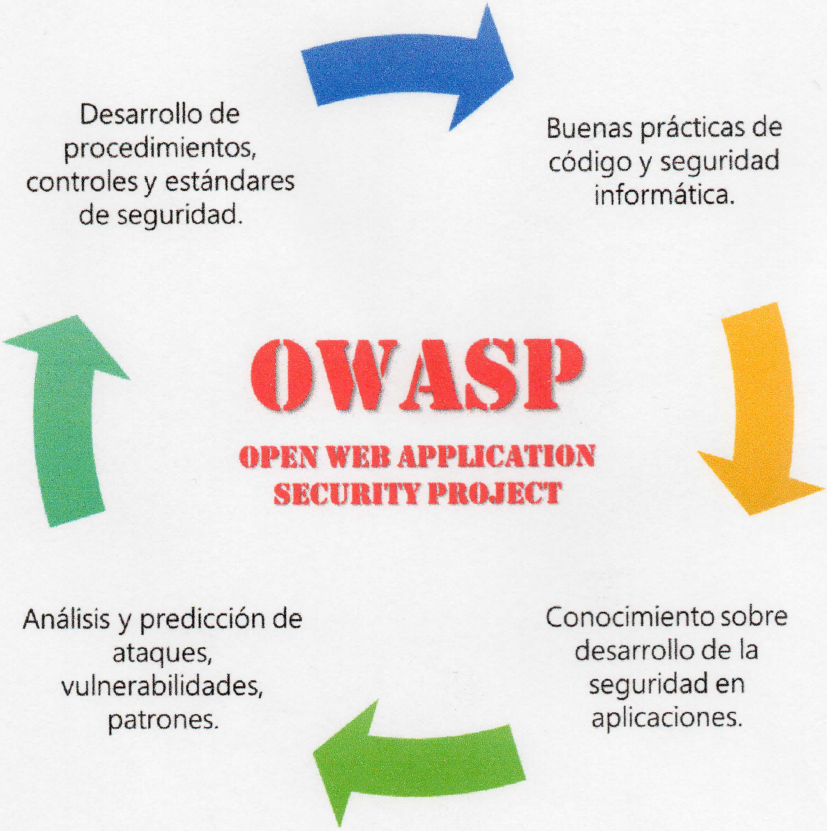

Figura N° 9: *Esquema gráfico de las fases fundamentadas en el conocimiento de la seguridad de aplicaciones frente a ataques u vulnerabilidades del proyecto de aplicación web de código abierto OWASP.*
Elaborado por: *Villavicencio Edison & González Bryan.*

En las arquitecturas de software generalmente se construye bajo una serie de decisiones de diseño, sin embargo, las tácticas de detección satisfacen las preocupaciones de calidad tales como confiabilidad, rendimiento y seguridad, el detector táctico implica tres fases; preparación, entrenamiento y detección superando a otros clasificadores de sistema de archivos. En cuanto a la evaluación de la calidad del conocimiento en la seguridad del diseño de aplicaciones, los métodos de evaluación en el proceso de desarrollo son recolectados mediantes registros de pruebas de calidad, toma de decisiones de seguridad en el diseño y eficiencia y eficacia en el rendimiento de soporte de amenazas, por el contrario, las actividades de disponibilidad e integridad de información son previsibles y robustas frente a las vulnerabilidades, considerando como calidad de seguridad de software basado en conocimiento, en la **Tabla 5** se demuestra diferentes tipos de evaluaciones utilizadas por diversos autores en la arquitectura, diseño y desarrollo de software.

Figura N°10: *Detalle de las funciones principales de la herramienta de modelado libre Archi para la arquitectura de software establecido en conocimiento y peritaje en la toma de decisiones.*

Elaborado por: *Villavicencio Edison & González Bryan.*

Tabla 5. Método de evaluación y estrategias de arquitecturas en el desarrollo del diseño de aplicaciones basadas en el conocimiento de seguridad.

Autores	Método de evaluación y estrategias de arquitecturas basadas en el conocimiento
(Duan, Lou, & Fu, 2016)	Método de evaluación basada en matrices de riesgos y vulnerabilidades para elevar la seguridad del software en pruebas de desarrollo. Modelo matemático probabilístico cuantificado en el valor del riesgo de vulnerabilidades Modelo de bibliotecas de reglas y procedimientos de seguridad en el desarrollo de la arquitectura y diseño de software. Métricas de encriptación de datos bajo el modelo de bibliotecas de reglas de seguridad de software.
(Mirakhorli & Cleland-Huang, 2016)	Comunicación asincrónica basada en tiempo de respuesta en el rendimiento de la seguridad de la aplicación en desarrollo. Arquitectura basada en la toma de decisiones en procesos de conocimiento estipulado en la seguridad y trazabilidad del diseño de la aplicación.

Táctica para el reconocimiento de diseño de análisis con sus respectivos patrones en términos de funcionalidad e interacciones.

Elaborado por: *Villavicencio Edison & González Bryan*

C. Experiencia, mantenimiento y relación de habilidades en la incorporación del conocimiento de la seguridad de aplicaciones.

Es importante destacar que el objetivo del diseño de seguridad de aplicaciones basadas en conocimiento es mermar todo tipo de vulnerabilidad o amenaza que comprometa a la inestabilidad del software en sí, considerando el remanente desasosiego en el diseño y enfoque de seguridad en el ciclo de vida del software, dicho de otra manera, una correcta incorporación de seguridad basada en el conocimiento de la toma de decisiones ante vulnerabilidades para dar una solución a ello.

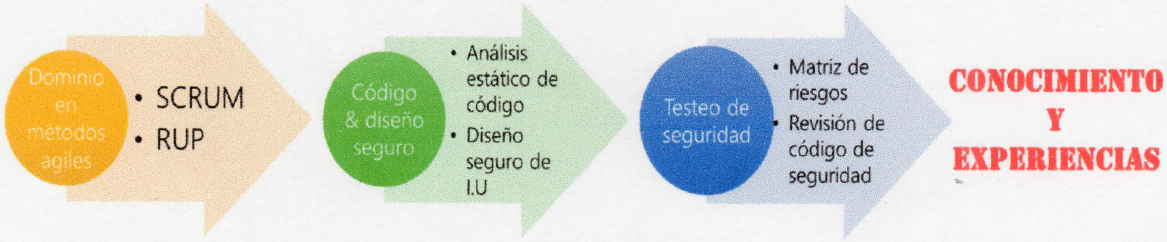

Figura N° 11: *Transformación de habilidades de un equipo de desarrollo de software en conocimiento y experiencia.*
Elaborado por: *Villavicencio Edison & González Bryan.*

Ahora bien, se ha destacado diversos enfoques para aplicar el conocimiento de seguridad en el diseño de aplicaciones, empero, con la impredecible actualización de métodos analíticos de diseño y el uso exhausto de mapeo de objeto-relacional, el uso de frameworks de desarrollo, entre otros; conllevan a un análisis de alto nivel los requerimientos de la arquitectura para considerar errores en el transcurso de la iteración de software, siendo este último, el punto clave para concatenar los diferentes errores de requerimientos, de diseño, lógicos, etc., explorando la capacidad integra de una solución latente con fase de aprendizaje autónomo. En la **Tabla 6** se realiza una síntesis de varios autores en experiencias, requisitos e incorporación de conocimientos y la relación de las habilidades de seguridad desde el punto de vista documental y de desarrollo de software.

Tabla 6. Experiencias, requisitos e incorporación de conocimientos en seguridad y la relación de las habilidades de seguridad con el diseño y desarrollo de software.

Autores	Experiencias, habilidades, requisitos e incorporación de conocimientos en seguridad
(Al-Banna, Benatallah, & Barukh, 2017)	Uso de análisis de datos cualitativos en vulnerabilidades presentes en aplicaciones actuales. Aplicaciones de descubrimiento de vulnerabilidades en tiempo real basados en conocimiento de seguridad informática. Utilización de criterios de selección de requerimientos para contrarrestar amenazas basado en experiencias de selección de expertos informáticos. Evaluación de habilidades en tiempo real mediante técnicas de expertos en toma de decisiones de seguridad informática. Identificación de problemas de seguridad en los requisitos del diseño de aplicaciones. Evaluación del tiempo de recuperación de la aplicación en base a la inestabilidad o vulnerabilidades.
(Gärtner, Ruhroth, Bürger, Schneider, & Jürjens, 2014)	Evolución de la seguridad del diseño de las aplicaciones mediante el conocimiento de incidentes de seguridad. Mecanismo de defensa basado en la heurística del conocimiento de procedimientos de seguridad en ataques informáticos, vulnerabilidades o amenazas. Constante capacitación y buenas prácticas de desarrollo de la organización frente a ataques informáticos o vulnerabilidades.
(Oyetoyan, Cruzes, & Jaatun, 2016)	Estrategias de métodos de desarrollo agiles en la seguridad de aplicaciones basado en la seguridad de datos. Utilización de herramientas para evaluar la integridad y seguridad del diseño de la aplicación basadas en métricas de conocimiento de seguridad.

Elaborado por: *Villavicencio Edison & González Bryan*

CAPÍTULO 5

CONCLUSIONES

El trabajo expone una investigación acerca de las aplicaciones de sistemas basados en conocimientos en el diseño de la seguridad de aplicaciones diferenciando niveles esenciales en el desarrollo de software. Simultáneamente, la perspectiva actual en el diseño de la seguridad de aplicaciones conlleva a restricciones en la fase del desarrollo, puesto expone en gran medida réplicas de métodos de conocimiento de seguridad generados por habilidades de la ingeniería de conocimiento y la ingeniería de requerimientos, generando incertidumbre al momento de exponer las respectivas pautas de aplicaciones de seguridad basadas en conocimientos.

Así pues, al analizar los artículos y documentos recolectado en la investigación, se encontró un enfoque peculiar a los modelos, estrategias y metodologías de integración de seguridad en las aplicaciones, alguna de ellas basadas en el conocimiento perpetuo de las amenazas, otros en las mitigaciones de las buenas prácticas y vulnerabilidades de código, empero, la esencial cúspide que comparten es la constante organización, evaluación y modificación de su arquitectura basada en el tiempo de contrarrestar la inestabilidad del software en tiempo real y su capacidad de aprender a proteger la integridad de los datos.

Los resultados obtenidos en la recopilación de la información de documentos en relación a la problemática del estudio presente, se hace comparaciones de diferentes autores sobre las tres categorías en base al conocimiento seguridad de aplicaciones, metodologías y experiencias; sobre el desarrollo de software infalible en base al conocimiento de seguridad cibernética y su arquitectura a correlación a las aplicaciones web clasificado como estrategias de seguridad y de conocimientos dando a conocer como seguridad cibernética las estrategias de protección de dicha información para prevenir, identificar, y responder a los ataques, proporcionando como solución la interconexión de toda su arquitectura de seguridad a una protección personalizada, ajustada a los entornos particulares y a sus atacantes específicos, permitiendo detectar y analizar los ataques como también combatirlos. El propósito de la seguridad cibernética y su arquitectura en todos sus ámbitos de aplicación es reducir riesgos, vulnerabilidades y amenazas hasta un nivel aceptable.

La comparación entre medidas de recomendación de seguridad de software en base al conocimiento, resulta de suma importancia en el transcurso del desarrollo de software,

dando a mostrar una serie de sugerencias y opiniones respectivamente con la seguridad planteando estándares y metodologías, como proceso estándar recomendada está la ISO 9126 estándar internacional para la evaluación de la calidad de productos de software, la ISO 15504 permite la evaluación y mejora de los procesos de desarrollo y la IEEE 1044-93 estándar para la clasificación de anomalías de software, propuesto como metodologías el CLASP (Exhaustivo Proceso de seguridad de aplicaciones livianas) y la Seguridad Ingeniería de requisitos de calidad (SQUARE) con la finalidad de mejorar el desarrollo de software seguro.

En el análisis, métodos y neutralización de vulnerabilidades basados en el conocimiento de la seguridad de aplicaciones, realiza un análisis avanzado para satisfacer las necesidades de los desarrolladores de software, utiliza herramientas de análisis estático para detectar vulnerabilidades en tiempo real con estándares de calidad ISO/IEC. Con respecto a la seguridad soluciones provisionales para respuesta rápida (SWRR), neutraliza las vulnerabilidades de manera oportuna, segura y discreta para proteger el software por atacantes.

En el método de evaluación y estrategias de arquitecturas en el desarrollo del diseño de aplicaciones, la evaluación medible para la seguridad del diseñó software es basado en la matriz de riesgo tipo cualitativa, utilizando la estructura jerárquica desarrollado por muchas métricas enfocadas en el análisis del software si cumple las funciones de seguridad propuestas, utilizando métodos matemáticos y niveles de riesgo de software ajustando la seguridad matriz de riesgo, creando biblioteca de reglas difusas, juicio de expertos y derivación difusa.

En base a las experiencias, requisitos e incorporación de conocimientos en seguridad, consiste en un indicador de experiencia de profesionales de seguridad, basándose al desarrollo de conceptos y técnicas para modelar y capturar expertos informáticos con intenciones de amenazas mediante patrones de comportamiento.

La evaluación de seguridad de los requisitos radica en la recolección de información, el problema y referencia a la mitigación efectiva, como estrategia se utiliza la heurística un método analítico para evaluar los requisitos con respecto a la seguridad, la identificación y perfección es de importancia para la evolución del software para el correcto funcionamiento.

REFERENCIAS BIBLIOGRÁFICAS

Al-Banna, M., Benatallah, B., & Barukh, M. C. (2017). Software security professionals: Expertise indicators. *Proceedings - 2016 IEEE 2nd International Conference on Collaboration and Internet Computing, IEEE CIC 2016*, 139–148. https://doi.org/10.1109/CIC.2016.28

Badaró, S., Javier Ibañez, L., & Agüero, M. J. (2013). Sistemas Expertos: Fundamentos, Metodologías y Aplicaciones. *Revista de Ciencia Y Tecnología*, *13*, 349–363. https://doi.org/http://dx.doi.org/10.18682/cyt.v1i13.122

Bajarlía, M. V., Ierache, J., & Eterovic, J. (2013). Modelo de Sistema Basado en Conocimiento en el Dominio de la Seguridad de Aplicaciones. *Revista Latinoamericana de Ingeniería de Software*, *1*(6), 241–252.

Bortolosso, H., Rossi, S. L., Pelegrini, G., Dalcanton, F., & Castella, M. F. (2017). Métodos de auditoria de sistemas de gestão de segurança e saúde no trabalho : uma revisão sistemática da literatura Auditing methods of occupational health and safety management systems : a systematic review of the literature.

Calvo, J., Gracia, J., & Bayo, E. (2017). Robust design to optimize client–server bi-directional communication for structural analysis web applications or services. *Advances in Engineering Software*, *112*, 136–146. https://doi.org/10.1016/j.advengsoft.2017.04.010

Chadwick Carreto, E. F. R. & S. N. S. (2014). MODELO DE ADMINISTRACIÓN DEL CONOCIMIENTO EN SISTEMAS MÓVILES APLICADOS A LA CAPACITACIÓN, 18.

Duan, Y., Lou, F., & Fu, Y. (2016). Research of evaluation methods for software security. *2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI)*, 467–470. https://doi.org/10.1109/CCI.2016.7778966

El Hachem, J., Pang, Z. Y., Chiprianov, V., Babar, A., & Aniorte, P. (2016). Model Driven Software Security Architecture of Systems-of-Systems. *23rd Asia-Pacific Software Engineering Conference (APSEC)*, (June), 89–96. https://doi.org/10.1109/APSEC.2016.023

Farias, G. L., Jeréz, Y. S. P., Armán, K. R., & Rosales, D. S. (2013). Componente genérico para la planificación y ejecución de acciones en aplicaciones de software Generic component for planning and execution of actions in software applications Introducción, *7*(2), 1–9.

Freitas, B., Matrawy, A., & Biddle, R. (2016). Online Neighborhood Watch : The Impact of Social Network Advice on Software Security Decisions Surveillance de voisinage en ligne : l ' impact de conseil de réseau social sur les décisions de sécurité de logiciel, *39*(4), 322–332.

Gärtner, S., Ruhroth, T., Bürger, J., Schneider, K., & Jürjens, J. (2014). Maintaining requirements for long-living software systems by incorporating security knowledge. *2014 IEEE 22nd International Requirements Engineering Conference, RE 2014 - Proceedings*, 103–112. https://doi.org/10.1109/RE.2014.6912252

Geng, J., Ye, D., & Luo, P. (2016). Forecasting severity of software vulnerability using grey model GM(1,1). *Proceedings of 2015 IEEE Advanced Information Technology, Electronic and Automation Control Conference, IAEAC 2015*, 344–348. https://doi.org/10.1109/IAEAC.2015.7428572

Hazeyama, A. (2012). Survey on Body of Knowledge Regarding Software Security. *2012 13th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing*, 536–541. https://doi.org/10.1109/SNPD.2012.64

Hazeyama, A., Saito, M., Yoshioka, N., Kumagai, A., Kobashi, T., Washizaki, H., ... Okubo, T.

(2015). Case Base for Secure Software Development Using Software Security Knowledge Base. *2015 IEEE 39th Annual Computer Software and Applications Conference*, 97–103. https://doi.org/10.1109/COMPSAC.2015.86

Huang, Z., Dangelo, M., Miyani, D., & Lie, D. (2016). Talos: Neutralizing Vulnerabilities with Security Workarounds for Rapid Response. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 618–635. https://doi.org/10.1109/SP.2016.43

Jovanovic, V., & Harris, J. K. (2016). Systems and software assurance - A model Cyber Security course. *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2016 - Proceedings*, 923–927. https://doi.org/10.1109/MIPRO.2016.7522272

Mirakhorli, M., & Cleland-Huang, J. (2016). Detecting, Tracing, and Monitoring Architectural Tactics in Code. *IEEE Transactions on Software Engineering*, *42*(3), 206–221. https://doi.org/10.1109/TSE.2015.2479217

Netto, A. da S., & Silveira, M. A. P. da. (2007). Gestão da segurança da informação: fatores que influenciam sua adoção em pequenas e médias empresas. *JISTEM: Journal of Information Systems and Technology Management*, *4*(3), 375–397. Retrieved from http://www.redalyc.org/articulo.oa?id=203219581007

Oyetoyan, T. D., Cruzes, D. S., & Jaatun, M. G. (2016). An empirical study on the relationship between software security skills, usage and training needs in agile settings. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 548–555. https://doi.org/10.1109/ARES.2016.103

Patra, S., Naveen, N. C., & Prabhakar, O. (2017). An automatedapproach for mitigating server security issues. *2016 IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2016 - Proceedings*, 1075–1079. https://doi.org/10.1109/RTEICT.2016.7807996

Verma, G., Yu, P., & Sadler, B. M. (2015). Physical layer authentication via fingerprint embedding using software-defined radios. *IEEE Access*, *3*, 81–88. https://doi.org/10.1109/ACCESS.2015.2398734

Wijesiriwardana, C., & Wimalaratne, P. (2017). On the detection and analysis of software security vulnerabilities. *2017 International Conference on IoT and Application (ICIOT)*, 1–4. https://doi.org/10.1109/ICIOTA.2017.8073635