IX Congreso iberoamericano
de seguridad informática
Universidad de Buenos Aires
Ciudad Autónoma de Buenos Aires, Argentina
1 al 3 de noviembre de 2017

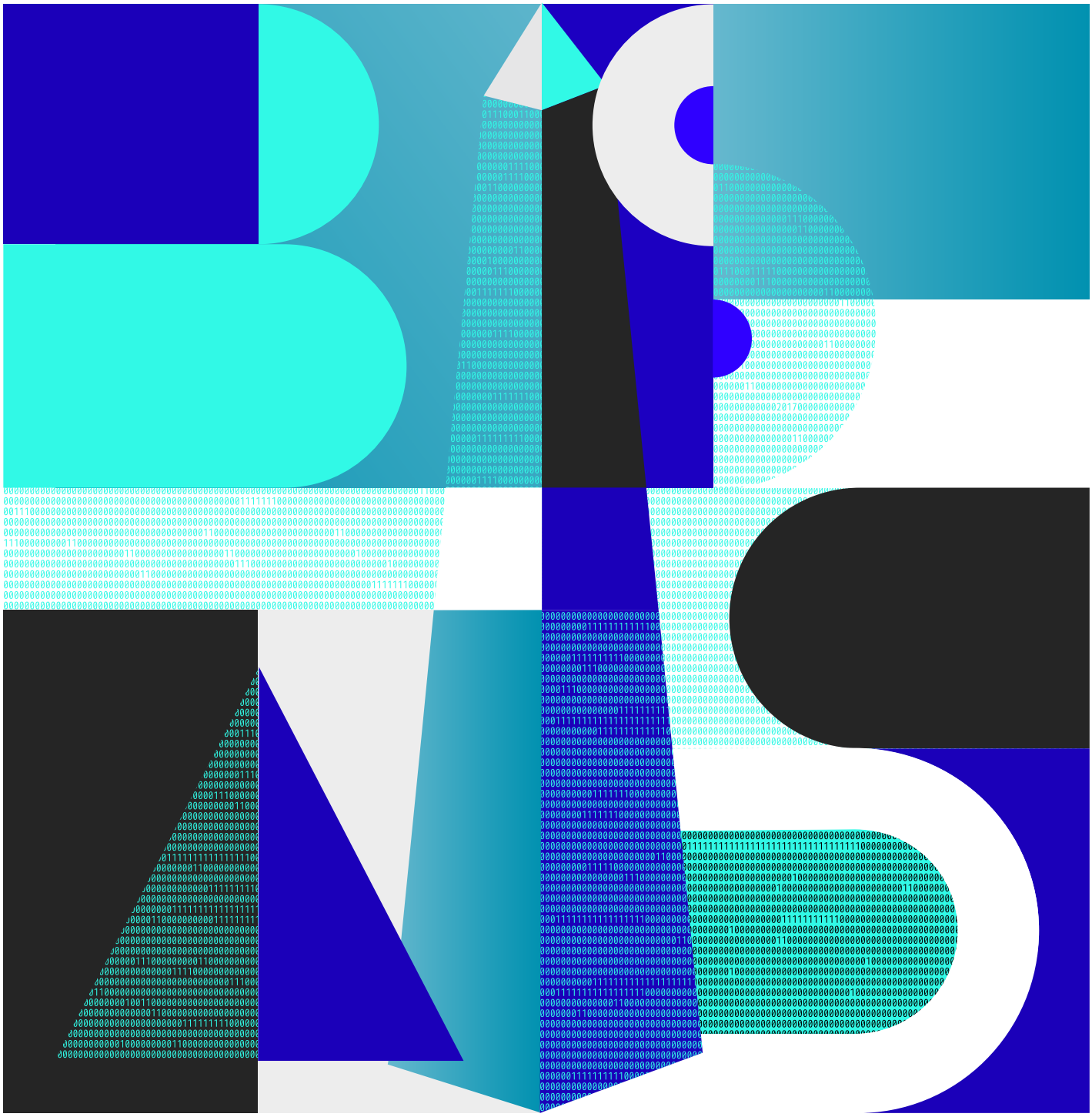
CIBSI

EU DE BA

PSI
POSGRADO EN SEGURIDAD INFORMATICA

CRIPTORED

Libro de Actas



Actas del IX Congreso Iberoamericano de Seguridad Informática
CIBSI2017, Buenos Aires, Argentina, 1 al 3 de Noviembre de 2017

Editores
Alberto E. Dams
Hugo A. Pagola
Luis E. Sánchez Crespo
Jorge Ramió Aguirre

Diseño de Tapas
Federico Dams

ISBN: en trámite

Prefacio

Del 1 al 3 de Noviembre se celebrará en la Universidad de Buenos Aires el IX Congreso Iberoamericano de Seguridad Informática - CIBSI 2017. El congreso está organizado por la Maestría en Seguridad Informática de la UBA en colaboración con la Red Temática Iberoamericana de Criptografía y Seguridad de la Información Criptored.

Este espacio permitirá a las empresas, entidades públicas, entornos militares, de defensa, centros académicos y de investigación exponer sus avances y servicios vinculados con la seguridad, facilitando el intercambio de conocimientos y la formación de redes de colaboración en este ámbito.

El congreso contará con la presencia de especialistas de Latinoamérica y de Europa entre otros de Argentina, Brasil, Colombia, Ecuador, México, Perú, Uruguay, España y Francia. Estamos muy satisfechos por el nivel de los artículos que se presentarán y el de los invitados especiales que tendremos. En esta novena edición del CIBSI, se destacan las presencias de referentes internacionales en la materia como Hugo Scolnik director de la Maestría en seguridad Informática de la UBA y Hugo Krawczyk Distinguished Research Staff Member with the Cryptography Group at the IBM T.J. Watson Research Center.

Organización de la Conferencia

Comité Organizador

Hugo Pagola, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Alberto Dams, Facultad de Ingeniería Universidad de Buenos Aires, Argentina
Jorge Ramió Aguirre, Universidad Politécnica de Madrid, España
Luis E. Sánchez Crespo, Universidad de Castilla La Mancha, España

Comité Local

Facundo Caram, FIUBA, Argentina
Luis Catanzariti, UTNfrba, Argentina
Marcia Maggiore, MUBA, Argentina
Patricia Prandini, MUBA, Argentina

Comisión de Posgrado Maestría en Seguridad Informática UBA

Mg Ing Alberto Dams, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Pedro Hecht, Maestria en Seguridad Informatica UBA, Argentina
Ing Hugo Pagola, Maestria en Seguridad Informatica UBA, FIUBA, Argentina
Dr Ricardo Rivas, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Raul Saroka, Maestria en Seguridad Informatica UBA, FCE-UBA Argentina
Dr Hugo Scolnik, Maestria en Seguridad Informatica UBA, FCEN-UBA Argentina

Comité del Programa

Marco Aurélio Amaral Henriques	State University of Campinas - Unicamp, Brasil
Javier Areitio	Universidad de Deusto, España
Rodolfo Baader	Universidad de Buenos Aires, Argentina
Gustavo Betarte	Facultad de Ingeniería, Universidad de la República, Uruguay
Carlos Blanco Bueno	Universidad de Cantabria, España
Joan Borrell	Universitat Autònoma de Barcelona, España
Pino Caballero-Gil	DEIOC, Universidad de La Laguna, España
Jeimy Cano	Universidad de los Andes, Colombia
Eduardo Carozo	Universidad de Montevideo, Uruguay
Joan-Josep Climent	Universitat d'Alacant, España
Roger Clotet	Universidad Simón Bolívar, Venezuela
Alberto Dams	Universidad de Buenos Aires, Argentina
José María De Fuentes	Universidad Carlos III de Madrid, España
Josep Domingo-Ferrer	Universitat Rovira i Virgili, España
Jose-Luis Ferrer-Gomila	University of the Balearic Islands, España
Angelica Florez Abril	Universidad Pontificia Bolivariana, Colombia
Walter Fuertes	Universidad de las Fuerzas Armadas ESPE, Ecuador
Amparo Fuster-Sabater	Institute of Applied Physics, Madrid, España
Giovana Garrido	Universidad Tecnologica de Panama
Lorena González Manzano	Universidad Carlos III de Madrid, España
Juan Pedro Hecht	Universidad de Buenos Aires, Argentina

Luis Hernandez Encinas	Institute of Physical and Information Tecnologies, España
Emilio Hernández	Universidad Simón Bolívar, Venezuela
Leobardo Hernández	Universidad Nacional Autónoma de México
Jordi Herrera	Universitat Autònoma de Barcelona, España
Monica Karel Huerta	Universidad Politécnica Salesiana, Ecuador
Angel Martin Del Rey	Universidad de Salamanca, España
Maria Vanina Martinez	Universidad Nacional del Sur in Bahia Blanca, Argentina
Vincenzo Mendillo	Universidad Central de Venezuela
Gaspar Modelo-Howard	Universidad Tecnológica de Panamá
Raul Monge	Universidad Técnica Federico Santa María, Chile
Karel Huerta Monica	Universidad Politécnica Salesiana, Ecuador
Guillermo Morales-Luna	Centro de Investigación y Estudios Avanzados, Mexico
Alfonso Muñoz	Criptored, España
Hugo Pagola	UBA - Facultad de Ingenieria, Argentina
Graciela Pataro	Universidad de Buenos Aires, Argentina
Alberto Peinado	Universidad de Malaga, España
Jose Pirrone	Universidad Catolica Andres Bello, Venezuela
Gustavo Presman	Universidad de Buenos Aires, Argentina
Jorge Ramio	Universidad Politécnica de Madrid, España
Ricardo Rivas	Universidad de Buenos Aires, Argentina
David Rosado	University of Castilla-La Mancha, España
Luis Enrique Sanchez Crespo	Universidad de Castilla La Mancha, España
Antonio Santos-Olmo Parra	Sicaman Nuevas Tecnologías
Raul Saroka	Universidad de Buenos Aires, Argentina
Hugo Scolnik	Universidad de Buenos Aires, Argentina
Pablo Silberfich	Universidad de Buenos Aires, Argentina
Jenny Torres	Escuela Politécnica Nacional, Ecuador
Urko Zurutuza	Mondragon University, España

Best security practices in software engineering with Essence

Francisco Arellano Méndez
Ma. Guadalupe. E. Ibargüengoitia González
National Autonomous University of Mexico
franciscoarellanomendez@gmail.com
gig@ciencias.unam.mx

Mario Piattini
David G. Rosado
University of Castilla-La Mancha
{mario.piattini, David.GRosado}
@uclm.es

Abstract- At present, it is recurrent to see news about failures of security of computer systems. As a result, frameworks and standards have been developed that help to incorporate security into development processes, but most of them are complex to implement. The main contribution of this work is "Essence Sec", a proposal that allows the inclusion of security in the development making use of Essence processes and the main security frameworks and standards for system development. It provides a vision with the principles of security to consider when carrying out a software project without radically altering its way of working.

Index Terms— Information Systems Security, Information systems security methods, Development of Secure Systems.

I. INTRODUCCIÓN

Actualmente, dada la diversidad de proyectos y la penetración que tienen las tecnologías de la información en toda la sociedad, es común observar que los fallos de seguridad por parte de los Sistemas de Información (SI), toman relevancia y tienen un papel crítico en la economía mundial. Lo que se traduce en que los sectores públicos y privados brinden un abanico de propuestas que pueden ser tomadas como referencia en procesos para la evaluación y mejora de la seguridad de los sistemas. Sin embargo, a pesar de que actualmente se cuenta con esa variedad de marcos y estándares para la incorporación de la seguridad a la Ingeniería de Software [7] – [15], éstos no son adoptados por parte de las organizaciones e independientes que desarrollan software por múltiples factores ya sean humanos, ideológicos o monetarios.

Sin embargo, cabe mencionar que no por el hecho de implementar alguna de estas propuestas se resolverán todos los problemas, ya que ninguno es la "panacea" o provee una solución completa a la seguridad para todos los procesos dentro del ciclo de vida del desarrollo del SI ya que su misión es el brindar una salvaguarda hasta los niveles mínimos aceptables que se plantee la organización [1].

Para lograr el objetivo de tener software seguro, las organizaciones deberían incluir en sus procesos de desarrollo medidas proactivas de seguridad que permitan brindar a sus clientes, y a sí mismos, la certeza de la correcta preservación de su información. Si ello se realiza de una forma no invasiva a sus procesos, se podrían incluir paulatinamente aspectos de seguridad, sin que se afecte la productividad, y a la larga permitir su inclusión y aceptación por parte de los interesados en el desarrollo del sistema, logrando satisfacer las demandas actuales bajo el precepto de entregar más calidad en menos tiempo. Todo ello se puede conseguir al hacer la planeación inicial del proyecto incluyendo medidas para mejorar la seguridad, ya que ésta no es un aspecto añadido al proyecto, sino es la sumatoria de personas, procesos y tecnología. Por tal motivo los involucrados deberían incluir en sus procesos de desarrollo temas de seguridad con la finalidad de solucionar esta problemática [2], [3].

En la actualidad se cuenta con una variedad de marcos y estándares [7] – [15] que permiten la incorporación de la seguridad en alguna medida dentro de los procesos de Ingeniería de software con la finalidad de reducir estados viciados en la creación de un sistema. Todos ellos tienen diferentes perspectivas para su implementación debido a que a sus funciones y practicas se adicionan ciertas áreas del ciclo de vida sin que se tenga que modificar todo el proceso.

El desarrollo de software por parte de organizaciones se realizan sin tener en consideración la preservación de la seguridad informática dentro de sus procesos en el ciclo de vida, lo que ocasiona que al menos el 80% de las aplicaciones creadas sufran vulnerabilidades graves, lo que provoca tener la información a expensas de cualquier atacante [2].

Por tal motivo, se tiene interés en proporcionar una propuesta que permita a cualquier organización incluir temas de seguridad dentro del proceso de desarrollo de software. Al realizar una revisión sistemática de las diferentes propuestas sobre enfoques de desarrollo en donde se podría realizar la inclusión de la seguridad se optó por la Esencia [4],[5], debido en primer lugar a que es un estándar del Object Management Group (OMG) aprobado en 2014 que brinda los conceptos principales que tienen en común todos los desarrollos de software a través de un lenguaje común, permitiendo aplicarse a cualquier tipo de desarrollo de software, así mismo permite representar mediante sus elementos en el núcleo otras metodologías que se crean necesarias de incorporar de acuerdo a las necesidades del proyecto, brindando una propuesta sostenible y escalable [6].

En la presente investigación se propone la adición de aspectos de seguridad a la Esencia [4], que permitirá crear sistemas robustos y con mejor tolerancia a fallos de seguridad. En primer lugar, se creó un marco común de los aspectos de seguridad que son indispensables considerar en cualquier desarrollo, tomando en consideración las diferentes propuestas

de marcos y estándares que se encuentran disponibles. Posteriormente estos conceptos de seguridad se incorporarán a la Esencia siguiendo su filosofía, completando las listas de control de algunos estados de las alfas, agregando espacios de actividades para complementar la visión de seguridad y en aquellos casos que se requiera la adicion de sub-alfas.

Este artículo se organiza de la siguiente forma: en la sección II se presentan los trabajos que tienen relación con la presente investigación tanto desde la perspectiva de seguridad, como de Ingeniería de software. A continuación, en la sección III se muestra la descripción general de la Esencia para tener un panorama de su forma de trabajar, y una vez teniendo las bases de la investigación, se presenta en la sección IV la propuesta, la cual incluye una descripción de la armonización de modelos y estándares de seguridad realizada con la integración en la Esencia de estos conceptos de seguridad. Finalmente, se expresan las conclusiones en la sección V y las fuentes consultadas para la realización de la presente investigación.

II. TRABAJOS RELACIONADOS

Para la presente investigación se realizó una revisión del estado del arte de las principales propuestas que actualmente se utilizan por parte de las organizaciones para la inclusión de la seguridad en el desarrollo de SI, con base en diferentes aspectos como lo es la institución que lo promueve, años de creación y actualización, aceptación y utilización por parte de industria, etc. Este trabajo concluye que se cuentan con diversas propuestas a implementar a diferentes niveles y áreas del desarrollo; dando como resultado la selección de las siguientes propuestas:

- ISO 27001
- SAMM
- BSIMM
- Métrica 3
- Microsoft SDL
- CISQ / ISO 25010
- Common Criteria
- NIST SDLC

A continuación se presentan estos modelos y estandares:

A. *ISO/IEC 27001* [7]

La ISO/IEC 27001 es una norma de seguridad de la información que especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información documentado (SGSI) así como los requisitos para la gestión de la implementación de los controles de seguridad.

B. *El ciclo de vida de desarrollo de seguridad de Microsoft (Microsoft SDL)* [8]

Es un proceso de desarrollo de software utilizado y propuesto por Microsoft desde el 2002, para reducir los problemas de seguridad y resolver las vulnerabilidades de seguridad de manera oportuna permitiendo reducir los costes de mantenimiento del software y aumentar la fiabilidad del software en relación con errores relacionados con la seguridad del software. Implementar Microsoft SDL implica la modificación de los procesos de la organización de desarrollo de software mediante la integración de medidas a lo largo de todo el proceso de desarrollo que conducen a la mejora de la seguridad del software, las cuales se agrupan en siete fases: capacitación, requisitos, diseño, implementación, verificación, liberación y respuesta. La figura 1 muestra las actividades clave en Microsoft SDL.

Figura 1 "Ciclo de vida de Microsoft SDL"

C. *The Building Security In Maturity Model (BSIMM)* [9]

El modelo empezó como resultado de un estudio de análisis realizado por varias empresas líderes en el desarrollo de software que estaban interesadas en implementar iniciativas de seguridad a sus procesos de desarrollo. Tiene como objetivo desarrollar un modelo de madurez. Adoptarlo suele ser lento debido al proceso de cambio que debe de realizarse, por lo que BSIMM proporciona una manera de evaluar el estado de las organizaciones, definir qué cambios deben ser priorizados y demostrar el progreso obtenido. Como se ve en la figura 2, contiene 12 prácticas que están divididas en 4 dominios: Gobierno, Inteligencia, SSDL Touchpoints y desarrollo. En conjunto suman un total de 113 actividades que miden el nivel de seguridad dentro del proceso de desarrollo.

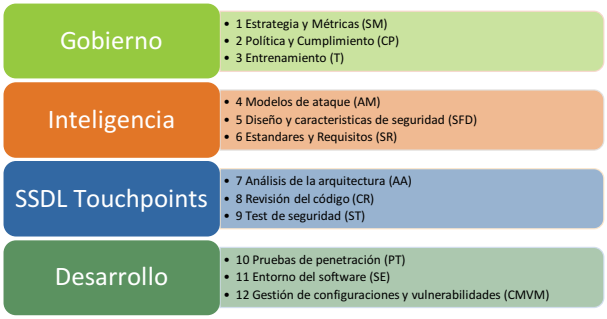


Figura 2 "Estructura general de BSIMM"

D. *The Software Assurance Maturity Model (SAMM)* [10]

El Open Web Application Security Project (OWASP) es una comunidad en línea que crea libremente artículos disponibles, metodologías, documentación, herramientas y tecnologías en el campo de la seguridad de aplicaciones web. Creó el “Software Assurance Maturity Model” (SAMM), el cual es un marco utilizable para ayudar a las organizaciones a formular e implementar una estrategia de seguridad en aplicaciones para los riesgos existentes. La base de este modelo está construida alrededor de cuatro funciones de negocio relacionadas al desarrollo de software, que a su vez incluyen una serie de

prácticas de seguridad relacionadas a cada función. Se pueden observar en la Figura 3.

Para estas prácticas se definen tres niveles de madurez como objetivos con la finalidad de implementarse de menos a más con la visión de ir optimizando el proceso paulatinamente lo que conlleva a la reducción de estados viciados en la creación del nuevo sistema.

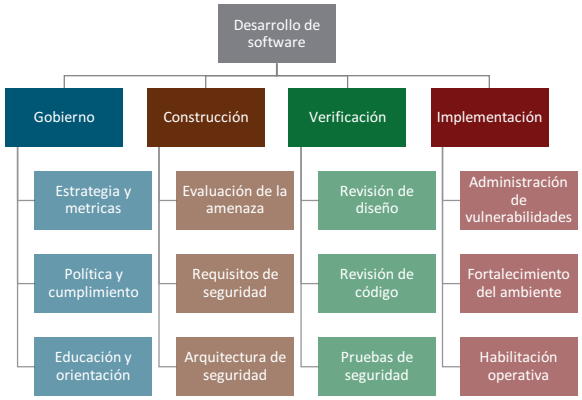


Figura 3 "Estructura general de SAMM"

E. Common Criteria (CC) [11]

Common Criteria (CC) es una norma internacional (ISO / IEC 15408) para la seguridad informática. Su objetivo es permitir a los usuarios especificar sus requisitos de seguridad, permitir a los desarrolladores especificar los atributos de seguridad de sus productos y permitir a los evaluadores determinar si los productos realmente cumplen con ambos.

Además, presenta requisitos para la seguridad de TI de un producto o sistema bajo distintas categorías de requerimientos funcionales y requisitos de aseguramiento. Los requisitos funcionales de CC definen el comportamiento de seguridad deseado. Los requisitos de garantía son la base para ganar confianza en el hecho de que las medidas de seguridad solicitadas son efectivas e implementadas correctamente**.**

F. CISQ [12]

El "Consortium for IT Software Quality" es un grupo comprometido a definir un estándar de métricas automatizables para medir la calidad y el tamaño del SW, con el objetivo de disminuir riesgos y costes, el cual en creo CISQ, una especificación para automatizar la medición de cuatro características de calidad de software: Fiabilidad, Eficiencia de Rendimiento, Seguridad y Mantenimiento. De ellas este artículo tomará como referencia la característica de Seguridad.

La cual se encarga de brindar una solución para la protección de 6 aspectos esenciales en la seguridad como lo es: La confidencialidad, integridad, no repudio, autenticidad, responsabilidad y conformidad. Esto se logra gracias a la revisión de 19 características que se deben de cubrir a través de 20 reglas establecidas.

G. Métrica 3 [13], [14]

Ofrece un instrumento para la sistematización de actividades que dan soporte al ciclo de vida del software con la finalidad de cumplir los objetivos identificados en términos de calidad, coste y plazos. Adicionalmente contiene cuatro interfaces complementarias al proceso base: Aseguramiento de la calidad, seguridad, gestión de configuración y gestión de proyectos. De ellas se hace uso de la Interfaz de seguridad cuyo objetivo es el incorporar en los sistemas de información mecanismos de seguridad adicionales a los que se proponen en la propia metodología, asegurando el desarrollo de cualquier tipo de sistema a lo largo de los procesos que se realicen para su obtención.

H. NIST Information Security [15]

"Security Considerations in the System Development Life Cycle"

El *National Institute of Standards and Technology* (NIST) Publicación Especial (SP) 800-64, fue desarrollado con la finalidad de ayudar a las agencias del gobierno federal de Estados Unidos a integrar procesos de seguridad al ciclo de vida del desarrollo de sistemas. Esta directriz se aplica a todos los sistemas de información federales. Pretende ser un recurso de referencia en lugar de un tutorial y debe implementarse junto con otras publicaciones del NIST según requiera el proyecto. La directriz describe los roles y responsabilidades clave de seguridad que se necesitan en el desarrollo de la mayoría de los sistemas de información y, en segundo lugar, proporciona información para permitir que una persona entienda la relación entre la seguridad de la información y el ciclo de vida del software.

III. La Esencia

LaEsencia [4],[5] es un estándar de la OMG que define los conceptos principales que tienen en común todos los desarrollos de software que en conjunto forman un método, ciclo de vida, proceso e incluso filosofía por lo que puede aplicarse a cualquier tipo de desarrollo de software. Permite incorporar prácticas profesionales de desarrollo ágil y tener gobernabilidad en la organización sobre todos sus procesos.

El núcleo de la Esencia proporciona los elementos comunes para, entre otros aspectos, comparar métodos y ayudar en la toma de decisiones sobre prácticas a usar. Se organiza en tres áreas de interés, cada una enfocada a un aspecto especifico de la Ingeniería de software: cliente, solución y esfuerzo (Figura 4).

- Cliente
  En esta área se revisa todo lo relativo a quien solicita el software, al uso actual y la explotación del sistema de software a producir.
- Solución
  En esta área se revisa lo relativo a la especificación y el desarrollo del sistema de software
- Esfuerzo
  En esta área se revisa lo todo lo relativo al equipo y la manera como ellos se enfocan en su trabajo

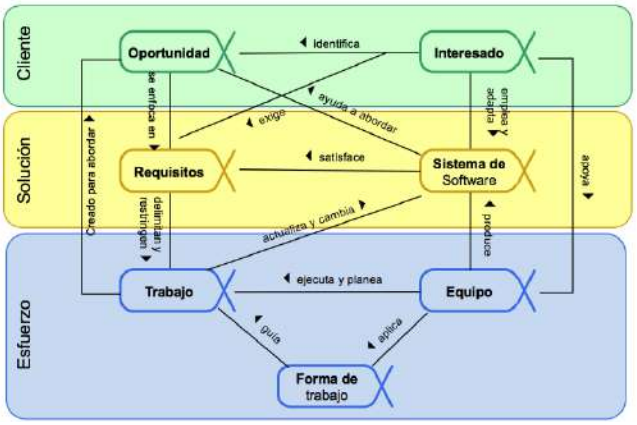


Figura 4 "Estructura General de los Alfas"

Cada área tiene *Alfas, Espacios de Actividades* y *Competencias* específicas. A continuación se presentan estos conceptos.

Alfa

Se puede definir como la representación de las cosas esenciales para trabajar al desarrollar software; provee una descripción de la clase de cosas que un equipo debe gestionar, usar y producir en cualquier esfuerzo de desarrollo de software.

Un alfa representa un indicador crítico de lo que es importante para monitorear y seguir una línea de progreso.

Cada Alfa contiene una serie de *Estados* independientes que deben ser cubiertos para cumplir con ella. A su vez los Estados contienen una *lista de control* donde se especifica a detalle lo que las actividades deben cumplir para que se alcance con éxito el estado (Figura 5). Cabe mencionar que la Esencia cuenta con 7 alfas principales que son: *Interesados, Oportunidad, Requisitos, Sistema de Software, Trabajo, Forma de trabajo y Equipo*, donde cada una tiene sus respectivos estados y lista de control .

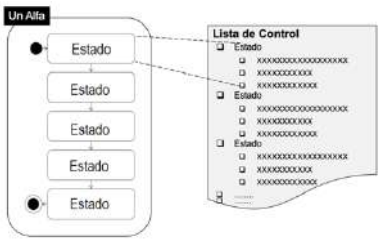


Figura 5 "Composición del Alfa"

Asi mismo, la Esencia cuenta con dos elementos que forman parte de su Estructura Genetal que son: Espacios de Actividades y Competencias, mismas que pueden ser observadas en la figura 6. A continuación se describe sus caracteristicas:

Espacios de actividad

Complementan a las Alfas, estas proporcionan un conjunto de actividades esenciales que normalmente se hacen en Ingeniería de software.

Competencias

Son las habilidades, capacidades, realizaciones, conocimiento y destrezas necesarias para hacer una cierta clase de trabajo. Estas competencias contienen una secuencia de niveles que varían desde un nivel mínimo a uno máximo. Típicamente, los niveles varían desde 0 (asistir) hasta 5 (innovar).

Figura 6 "Estructura General de Essence"

Tambien cabe resaltar que la Esencia cuenta con una serie de Anexos que le permiten adicionar aspectos que no se consideraron como esenciales en los desarrollos de software. En la presente investigacion se hace uso del Anexo A "Extensiones opcionales al Kernel", este permite incluir prácticas que el Kernel no consideró o se presentan desde una perspectiva abstracta. Una de las formas para hacer uso de la Extensión del Kernel es el uso de Sub-Alfas, las cuales permitan expresar el accionar de un Alfa a bajo nivel.

La Esencia incorpora algunos aspectos de seguridad dentro de sus actividades como lo es en el Alfa de Sistema de Software en el Estado de "Con arquitectura seleccionada" al establecer la búsqueda de una arquitectura que permita combatir los riesgos técnicos clave, así como la definición de criterios para la selección de la misma. Pero no se establece de manera regular dentro de los demás Estados de las Alfas.

Por lo que se requiere extender la Esencia con aspectos de seguridad, con la finalidad de que las organizaciones y la academia puedan incorporarla desde el inicio de sus procesos permitiendo tener software con mayor calidad.

IV. PROPUESTA

Para la realización de la propuesta de investigación se presenta en primer lugar, la armonización de los diversos marcos y estándares de seguridad, realizada con la finalidad de conocer las similitudes y diferencias que tienen, así como obtener un marco común para su posterior implementación en la Esencia, el cuál es el siguiente punto de la investigación, la integración de la Esencia con esos marcos y estándares de seguridad, donde primero se revisó una implementación ya realizada "Métrica 3" para conocer en qué áreas de la ingeniería de software se había colocado los aspectos de seguridad para posteriormente presentar la incorporación de una guía con la Esencia.

Finalmente se realizó la integración de los aspectos de seguridad de los marcos y normativas de seguridad identificadas anteriormente con la Esencia, formando Essence-Sec.

A. Armonización

La heterogeneidad de los marcos anteriores, sumada a las peculiaridades de cada organización, hace que la definición de un marco único o universal sea difícil de estructurar. Con el objetivo de desarrollar y satisfacer las necesidades de un proyecto es necesario proveer un mecanismo, que de manera sistemática facilite la gestión e implementación de las técnicas y/o métodos para la armonización de marcos. El propósito de esta investigación es proponer una armonización de las diferentes propuestas de inclusión de la seguridad en el desarrollo de software, que permita identificar y definir estrategias esenciales necesarias que conduzcan a su implementación dentro del ciclo de vida del desarrollo de software.

El objetivo general de la armonización para esta investigación es:

- Definir las áreas y funciones de seguridad que se consideran para incorporar la seguridad en el núcleo de la Esencia basándose en la armonización de las diferentes propuestas relacionadas.

Los objetivos específicos fueron:

- Conocer las diversas propuestas que implementan la seguridad en las diversas actividades realizadas durante el ciclo de vida del desarrollo de software.
- Encontrar las diferencias y similitudes que se tienen entre ellas.
- Definir las áreas y funciones de seguridad que se implementarán

Una vez que se identificaron los objetivos y lineamientos que se deben de seguir, así como los marcos y estándares a armonizar, se procedió a efectuar un análisis de la estructura con la que se describen y la filosofía que siguen. Se llegó a la conclusión que para poder realizar un mapeo de manera uniforme se debía de considerar un marco común para homogenizarlo, de ahí que se eligió la estructura de la Esencia debido a que esta maneja una estructura simple que va de lo general a lo especifico debido a que en primer lugar define las características básicas en las Alfas, posteriormente define los Estados que integran a esas alfas y finalmente las actividades que se especifican para comprobar el estatus que tienen los estados.

Con el propósito de poder llevar una mejor trazabilidad a través de todas las propuestas y en la investigación, se estableció la necesidad de colocar identificadores únicos para cada una, permitiendo rastrear sus funciones y prácticas, un ejemplo es SAMM [10], donde se definen 4 funciones de negocio esenciales para su funcionamiento, las cuales son:

SAMM	S
Gobierno	S G
Construcción	S C
Verificación	S V
Implementación	S I

Donde se definen para cada una la Inicial de SAMM seguida de la inicial de cada función. Seguidamente las funciones cuentan con sus respectivas prácticas, por ejemplo, Gobierno tiene tres que son:

Gobierno	S G
Estrategia y métricas	S G-EM
Política y cumplimiento	S G-PC
Educación y orientación	S G-EO

Y ellas a su vez contienen ciertos niveles o características a cumplir para lograr satisfacer las prácticas y éstas se señalan con un número consecutivo posterior al Id de la función a la que corresponde, por ejemplo "Estrategia y métricas" contiene 2 que son:

Estrategia y métricas	S G-EM
Establecimiento de un plan estratégico unificado para la seguridad del SW	S G-EM-1
Medir el valor relativo de los datos y bienes y luego elegir la tolerancia al riesgo	S G-EM-2

Se tiene como resultado final la definición de las funciones establecidas en cada propuesta. A continuación, se expresan como sería el resultado de la Función de Gobierno de SAMM

- SAMM
  - Gobierno (S G)
    - Estrategia y métricas (S G-EM)
      - Establecimiento de un plan estratégico unificado para la seguridad del SW (S G-EM-1)
      - Medir el valor relativo de los datos y bienes y luego elegir la tolerancia al riesgo (S G-EM-2)
    - Política y cumplimiento (S G-PC)
      - Cumplimiento de regulaciones implicadas al SW (S G-PC-1)
      - Establecer base de seguridad y cumplimiento, y entender los riesgos del proyecto (S G-PC-2)
    - Educación y orientación (S G-EO)
      - Ofrecer acceso a temas de programación segura e implementación (S G-EO-1)
      - Educar a todo el personal en el ciclo de vida del SW con lineamientos específicos en desarrollo seguro (S G-EO-2)
      - Hacer obligatorio el entrenamiento integral (S G-EO-3)

Una vez que se efectuó el mapeo de cada una de las propuestas anteriormente descritas, se llevó a cabo el análisis para poder conocer la correlación que tenían entre ellas, donde se tomaron en consideración las similitudes y diferencias entre ellas, los aspectos de la seguridad que se ven involucradas en el accionar de la propuesta, los roles y actividades que se deben de implementar para lograr con éxito su implementación.

Durante el análisis se pudo observar que existían diversas similitudes entre los aspectos de seguridad que se implementaban, así como diversas actividades que se expresaban de forma muy similar por lo que se vio la necesidad de estudiar a fondo las propuestas para revisar sus actividades y el nivel de abstracción que contenían, teniendo como finalidad el comprender si su objetivo era el mismo o contenían alguna particularidad en su accionar con el fin de determinar todos los posibles aspectos de seguridad que se deben considerar, así como las prácticas que son necesarias para poder lograr ese aspecto.

Tabla 1 "Relación de los aspectos de seguridad con prácticas de los marcos y estándares"

Amenazas		**Requerimientos de Seguridad**		**Pruebas Generales**		**Entrenamiento**		**Control de Procesos**	
SAMM	S C-EA-1	M-SDL	R 1	SAMM	S V-PS-1	M-SDL	T 1	BSIMM	B G-CP-2.3
	S I-AV-1	M-SDL	D 1		S V-PS-2	SAMM	S G-EO-1		B G-SM-1.1
M-SDL	D 3	SAMM	S C-RS-1		S V-PS-3		S G-EO-2	SAMM	S I-HO-1
Riesgos			S C-RS-2	BSIMM	B ST-ST-?.?		S G-EO-3	M 3	PSI-SEG 3.1
M-SDL	R 3		S C-RS-3		B ST-ST-1.3	BSIMM	B SM-1.3	NIST	Ni 1
BSIMM	B I-MA-1.3	BSIMM	B G-CP-1.2		B ST-ST-3.5		B G-T-1.1	NIST	Ni 2
	B I-MA-2.7	M 3	DSI-SEG 2.1	M-SDL	V 1		B G-T-1.7	NIST	Ni 3
	B ST-AA-1.4		DSI-SEG 3.1	M 3	ASI-SEG 3.1		B G-T-3.4	NIST	Ni 4
	B G-CP-2.2		IAS-SEG 2.1		DSI-SEG 4.1	M 3	CSI-SEG 3.1	NIST	Ni 5
	B ST-CR-1.5	**Diseño**			CSI-SEG 2.1	**Métricas y Apoyos**		NIST	Ni 6
SAMM	S C-EA-2	SAMM	S C-AS-1		IAS-SEG 3.1	SAMM	S I-HO-2	**Estandarización de Procesos**	
	S V-RC-3		S C-AS-2	NIST	Ni 13		S C-EA-3	SAMM	S I-HO-3
M-SDL	R 2		S C-AS-3		Ni 14	BSIMM	B G-T-1.6	BSIMM	B ST-AA-2.2
M 3	EVS-SEG 3.1		S V-RD-1	**Pen Testing**			B I-MA-1.2		B ST-CR-3.5
	EVS-SEG 4.1	**Arquitectura**		BSIMM	B D-PT-1.1		B I-SFD-2.1		B I-SR-2.6
	ASI-SEG 2.1	BSIMM	B ST-AA-2.1		B D-PT-1.3		B I-SFD-1.2	NIST	Ni 10
	DSI-SEG 2.1	M 3	PSI-SEG 2.1		B D-PT-2.3		B G-SM-2.5		Ni 11
NIST	Ni 7		PSI-SEG 2.2	**Pruebas Caja Negra**			B G-CP-1.3	**Marcos y Regulaciones**	
	Ni 8	NIST	Ni 12	M-SDL	V 2		B ST-CR-1.6	BSIMM	B G-CP-2.5
	Ni 9	**Automatización de código**		BSIMM	B ST-ST-2.1		B I-SR-1.1		B G-CP-1.1
Superficie de Ataque		BSIMM	B ST-CR-1.4	**Herramientas**			B I-SR-1.2	M 3	EVS-SEG 3.1
M-SDL	D 2	SAMM	S V-RC-2	M-SDL	I 1		B I-SR-2.2		
	V 3	M-SDL	I 3	SAMM	S I-FA-1		B ST-ST-2.4		
							B D-PT-1.2		

En la Tabla 1 se puede ver el resultado obtenido del análisis, donde se pueden observar los aspectos de seguridad con las respectivas prácticas que fueron identificadas. Tomando como ejemplo el aspecto de Riesgos, se pueden identificar 6 propuestas que lo implementan a diferentes niveles y eso se puede verificar revisando las actividades que están relacionadas. Por ejemplo, en Microsoft SDL se observa solo en las actividades R2 y R3, en NIST se trabajan en las actividades Ni 7, Ni 8 y Ni 9 así subsecuentemente con las demás propuestas.

Es así que, al concluir el análisis se encontraron 14 aspectos de seguridad que se implementan en alguna medida en las propuestas referidas:

1. Amenazas
2. Riesgos
3. Superficie de Ataque
4. Requisitos de Seguridad
5. Diseño de seguridad
6. Arquitectura de seguridad
7. Pruebas de seguridad
8. Entrenamiento
9. Herramientas
10. Marcos y Regulaciones
11. Estandarización de Procesos
12. Automatizaciones
13. Control de Procesos
14. Métricas

Estos aspectos están fundamentados en diversas prácticas que se encontraron dentro de las propuestas analizadas donde se obtuvo que perseguían objetivos en común por lo que se podían unificar, logrando una homogenización tanto para los aspectos como las actividades, logrando que en su conjunto representen salvaguardas que ayuden a preservar la Confidencialidad, Integridad y Disponibilidad (CIA) de un sistema, siendo estas cualidades el centro de la seguridad de la información, de modo que al hacer un uso adecuado de todas ayudará a que el sistema que se esté creando pueda mantener esas tres cualidades, pero siempre teniendo en mente que ningún sistema es infalible y que se busca minimizar los riesgos que pudiera tener el SI.

Este tema cobra relevancia en un entorno donde tener una buena correlación entre el costo beneficio de implementar o no ciertas medidas puede ser el principal factor para decidir si se aplica o no tal salvaguarda. De modo que parte de los objetivos

de la investigación es proporcionar una guía para la implementación de la seguridad desde etapas iniciales en el ciclo de vida del sistema ya que entre más pronto se realicen las detecciones y acciones de protección resultará más económica su implementación, a diferencia de realizarla en etapas finales del desarrollo debido principalmente al re-trabajo que se tiene que realizar.

B. Métrica 3 como base para implementación

En este punto se vio la necesidad de contar adicionalmente con una visión ya establecida de las características de seguridad que se deben de implementar en un ciclo de vida de desarrollo, por lo que se hizo uso de Métrica 3 [13], [14] propuesta del gobierno de España, que en su 3ª versión implementa una interfaz adicional de seguridad, por lo que sirve de precedente para la presente investigación. Por ello se realizó el análisis de correlación de ésta con la Esencia para tener claro en donde se pueden implementar las actividades de seguridad identificadas por Métrica 3.

Tabla 2 "Relación Esencia y Métrica 3"

<table>
<tr><td>Interesados</td><td>Oportunidad</td><td>Requisitos</td><td>Sistema de Software</td><td>Trabajo</td><td>Forma de trabajo</td><td>Equipo</td><td>Esencia</td></tr>
<tr><td rowspan="3"></td><td rowspan="2">Viabilidad del Sistema</td><td>Análisis del Sistema</td><td>Diseño del Sistema</td><td>Construcción del Sistema</td><td rowspan="3"></td><td rowspan="3"></td><td rowspan="3">Métrica 3</td></tr>
<tr><td colspan="2">Planificación</td><td>Implementación</td></tr>
<tr><td colspan="3"></td><td>Mantenimiento</td></tr>
</table>

Tabla 3 "La Esencia y los aspectos de seguridad a considerar"

<table>
<tr><td>Interesados</td><td>Oportunidad</td><td>Requisitos</td><td>Sistema de Software</td><td>Trabajo</td><td>Forma de trabajo</td><td>Equipo</td><td>Esencia</td></tr>
<tr><td rowspan="5"></td><td rowspan="5"></td><td>Amenazas</td><td>Diseño</td><td rowspan="2"></td><td colspan="2">Entrenamiento</td><td rowspan="5">Aspectos de Seguridad</td></tr>
<tr><td rowspan="2">Riegos</td><td rowspan="2">Arquitectura</td><td rowspan="2">Control de Procesos</td><td rowspan="2">Herramientas</td><td rowspan="2">Control de Procesos</td></tr>
<tr><td rowspan="3">Superficie de Ataque</td><td rowspan="3">Pruebas</td></tr>
<tr><td colspan="2">Normas y Regulaciones</td><td rowspan="3"></td></tr>
<tr><td rowspan="2">Requisitos de Seguridad</td><td colspan="2">Estandarizaciones</td></tr>
<tr><td colspan="2"></td><td>Automatizaciones</td></tr>
</table>

Puesto que Métrica 3 cuenta con 7 funciones principales que se deben de implementar a lo largo del ciclo de vida para desarrollar un sistema de manera segura las cuales son: planificación del sistema, la viabilidad del sistema, análisis del sistema, diseño del sistema, construcción del sistema, implementación y mantenimiento. Al realizar el estudio de estas 7 funciones se determinó en qué Alfas podrían estar involucrados sus actividades.

En la Tabla 2, se presenta en qué Alfas de la Esencia se podrían implementar las actividades de seguridad identificadas en Métrica 3.

C. Definición de Alfas con los 14 aspectos de seguridad

Asimismo, se procedió a realizar el análisis de la correlación de los 14 aspectos de seguridad que se obtuvieron en la armonización de los marcos y estándares con las Alfas de la Esencia. Además, ya se cuenta con la visión de Métrica 3 con respecto a en qué Alfas se pueden incorporar estos aspectos lo que origina la propuesta de este trabajo llamada "*Essence Sec*".

El análisis se puede observar en la Tabla 3, donde se presentan las relaciones.

D. Essence Sec

Al contar con el panorama general de la armonización de los marcos y estándares referidas en la sección IV-A y la visión de integración de la seguridad dentro de una metodología de desarrollo de software expuesta en la sección III, se procedió a realizar la siguiente etapa de la investigación, encargada de la integración de la armonización de los marcos y estándares de seguridad con la Ingeniería de Software a través de la Esencia debido a que es un modelo de reciente creación ello en primer lugar al ser un estándar de la OMG y seguido de la facilidad para implementarse por las organizaciones y la adaptabilidad con otras propuestas.

Para poder llevar a cabo este proceso se tomaron en consideración los siguientes puntos:

- Se tomó la determinación de solo trabajar con 4 de las 7 Alfas, las cuales son:
  - Requisitos
  - Sistema de software
  - Forma de trabajo
  - Equipo

Debido a que en estas alfas es donde se presentan los aspectos más críticos que se deben de considerar para la correcta inclusión de la seguridad dentro de los procesos de la Esencia.

- Estas Alfas se mantuvieron lo más general posible.
  - Por lo que únicamente se agregaron las Sub-Alfas que se creyeron necesarias de destacar sobre las prácticas.

- Se refinaron las listas de control, agregando un anexo a las listas con características de seguridad que se deben tomar en cuenta para que ese Estado se cumpla satisfactoriamente.
- Se agregaron actividades en los Espacios de Actividades con la finalidad de tener un mayor detalle de aquellas que necesiten tener más claridad para su implementación.

Estos puntos se consideraron con la finalidad de que los usuarios que actualmente hacen uso de la Esencia en su forma simple puedan hacer uso de la *Essence Sec* sin que requieran modificar sus procesos y su forma de trabajo, puesto que únicamente se adicionan las medidas de seguridad a lo que ya comúnmente trabajan en su día a día.

A nuevos usuarios de la Esencia, les permitirá incluir medias de seguridad en sus desarrollos de una forma más transparente.

También se tomó en consideración el nivel de los usuarios respecto a la comprensión de temas de seguridad por lo que, para los más expertos, únicamente con la especificación general podrán revisar para recordar las consideraciones de seguridad a incorporar. Para los que apenas se están familiarizando con los temas de seguridad, se especifican más detalladamente las listas de control y actividades correspondientes.

Para ejemplificar la implementación realizada en la investigación, se presenta 1 de las 4 Alfas con las que se trabajó, el Alfa de Sistema de Software debido a que cada alfa contiene sus respectivos Estados y listas de control tradicional y de seguridad respectivamente:

Alfa: Sistema de Software

Para la inclusión de medidas de seguridad en el *Alfa de Sistema de Software* se propone la inclusión de ítems extras en las listas de control de los estados, permitiendo crear el software con una arquitectura con medidas de seguridad incluidas y adicionalmente contar con la verificación en las fases de liberación, operación y el retiro del software.

Los aspectos de seguridad que se proponen para la inclusión de medidas de seguridad en el Alfa de Sistema de Software de la Esencia son:

- Diseño de seguridad
- Arquitectura de seguridad
- Pruebas de seguridad

Ya que en esta Alfa se realiza desde la selección de la arquitectura hasta la retirada.

Se proporciona en la Tabla 4, la lista de control con aspectos de seguridad que deben ser cubiertos para cada estado del, así como los aspectos de seguridad que se ven inmiscuidos en su realización:

Tabla 4 "Lista de verificación del Alfa Sistema de Software"

Estados Sistema de Software	Control de Seguridad
Con arquitectura seleccionada	• Se tienen claras las particularidades del proyecto que impactan al diseño y arquitectura del sistema • Los servicios compartidos a los que hará uso el nuevo proyecto son claros y bien definidos. • Los sistemas dependientes que están implicados con el nuevo proyecto han sido identificados. • Se han identificado claramente los posibles escenarios a los que se enfrentará el sistema • La definición de la arquitectura está alineada con la visión de seguridad. • Los procesos de diseño son dirigidos hacia servicios y diseños seguros conocidos. • Se cuenta con un esquema de integración de la seguridad claro y preciso
Demostrable	• Las descripciones de la arquitectura están estandarizadas • La integración con otros sistemas cumple las normas de seguridad establecidas • Después de realizar una revisión integral, el sistema cumple con las normas de seguridad establecidas • El sistema aprobó los posibles escenarios de vulnerabilidades o limitaciones conocidas • Los servicios compartidos y el riesgo compartido resultante han sido revisados • Se revisaron las funciones, despreciando las inseguras
Usable	• Se han verificado los controles de seguridad pactados en los requisitos. • Se han efectuado las pruebas previstas para comprobar la seguridad en el sistema y se encuentran dentro de los parámetros aceptados. • La documentación de la aceptación de la seguridad del sistema está completa
Listo	• La instalación del sistema se ha realizado de acuerdo a los lineamientos de seguridad pactados • Los interesados aceptan que los objetivos de seguridad están reflejados en el funcionamiento del sistema

Estados Sistema de Software	Control de Seguridad
Operacional	• La documentación de seguridad está actualizada y verificada • Las actualizaciones y monitoreo de la configuración se realizan periódicamente • La ejecución del plan de respuesta a incidentes se ha realizado satisfactoriamente de acuerdo a los lineamientos
Retirado	• Se ha realizado la retirada del sistema conforme al protocolo • La documentación del cierre del sistema es clara y consistente • La retirada del sistema se ha realizado conforme a las políticas vigentes • La preservación de seguridad se ha realizado de acuerdo a las políticas de seguridad

Es así que, por ejemplo, para el Estado de "Listo" es necesario cumplir con dos actividades que son:

1. La instalación del sistema se ha realizado de acuerdo a los lineamientos de seguridad pactados
2. Los interesados aceptan que los objetivos de seguridad están reflejados en funcionamiento del sistema

Adicionalmente, para el *Alfa de Sistema de Software* se realizaron tres prácticas complementarias, con la finalidad de facilitar la validación de los estados en cuestión. Estas fueron:

1. Selección de la Arquitectura de Seguridad
2. Implementación del sistema
3. Retirada Segura del Sistema

Alfas Adicionales

Como se mencionó en la sección IV.B, se realizó un análisis para realizar de forma satisfactoria la implementación de aspectos de seguridad en los procesos de la Esencia, dando como resultado la selección de cuatro Alfas específicas: *Requisitos*, *Sistema de software*, *Forma de trabajo* y *Trabajo*. Donde el Alfa de *Sistema de Software* se tomó de ejemplo para este trabajo de investigación.

En el Alfa de *Requisitos* se busca identificar todos aquellos requisitos de seguridad que ayuden a mitigar todos aquellos riesgos identificados hasta los niveles aceptables. Adicionalmente dentro de esta Alfa se considera el uso de una Sub-Alfa que permita realizar de forma adecuada la identificación de los requisitos a través de la realización de la *Evaluación de Riesgos de Seguridad* para el proyecto en cuestión. Las preguntas que se incluyen en la Lista de verificación de esta alfa son:

Requisitos 1. ¿Se identificaron todas las posibles complicaciones por la plataforma del proyecto?

Requisitos 2. ¿Las normativas y regulaciones que están asociadas al proyecto fueron procesadas y delimitadas?

Requisitos 3. ¿Se tenían claros los objetivos primarios de seguridad relacionados con el proyecto?

Requisitos 4. ¿Se llevó acabo alguna evaluación de riesgos de seguridad del proyecto?

a. ¿Cuál fue su procedimiento?

b. Sirvieron como base para la obtención de requisitos de seguridad

Requisitos 5. ¿Se identificaron aquellas medidas de seguridad a considerar en el entorno de desarrollo?

Requisitos 6. ¿Se definieron los umbrales de seguridad maximos y minimos?

Requisitos 7. Se definieron todas las pruebas de seguridad que permitan verificar que se cumplieron los requisitos

En el Alfa de *Trabajo* se hace una revisión sobre las capacitaciones que debe de tener el equipo de proyecto, las herramientas y bibliotecas a utilizar para el desarrollo. Las preguntas que se incluyen en la Lista de verificación de esta alfa son:

Trabajo -1: ¿Se establecieron principios de seguridad en la definición del trabajo a realizar?

Trabajo -2: Se realizó alguna capacitación para la realización del proyecto.

Trabajo -3: Se identificaron algunos repositorios de consulta para solución de problemas y aseguramiento de la seguridad.

Trabajo -4: ¿Cómo se seleccionaron las herramientas a utilizarse?

Trabajo -5: Se analizaron los detalles de seguridad de la aplicación

Trabajo -6: ¿Cómo fue la selección de middleware y bibliotecas? (versiones, autores)

Finalizando con en el Alfa de *Forma de Trabajo* se verifican todos los principios que se deben de considerar a la hora de trabajar, pueden ser de forma regulatoria, estándares o normas.

F Trabajo -1: ¿Se tomaron consideraciones relacionadas con la seguridad en la forma de trabajo del equipo? (Normas regulatorias, Principios de estándares/normas)

F Trabajo -2: ¿Cómo se realizó la organización del trabajo?

F Trabajo -3: ¿Comó se determinaron los roles y responsabilidades del equipo?

F Trabajo -4: ¿Se realizó alguna clasificación de los datos que se utilizaran en el sistema? (La forma en que se categorizaron los datos para determinar su relevancia

y poder tener medidas de seguridad para su protección)

F Trabajo -5: ¿Se llevó a cabo algún seguimiento durante el desarrollo del sistema para saber si se llevaba a cabo las medidas de seguridad pactadas?

F Trabajo -6: ¿Se lleva alguna retroalimentación con el avance del trabajo?

Gracias a las listas de verificación de cada Alfa así como de las Actividades que se encuentran asociadas a ellas, le permitirá a los administradores del proyecto identificar en qué fase del proyecto se encuentran, verificando las cosas que hicieron u les hicieron falta de realizar, ello les brindará una visión de cómo se encuentra implementada la seguridad dentro de sus procesos de desarrollo.

Las listas de verificación con toda su información, pueden ser consultadas en [17] para su mayor referencia.

V. Conclusiones

Al finalizar la presente investigación se identificó que, existen diversas propuestas que tienen como finalidad el incluir la seguridad en el desarrollo de software en diversos niveles, pues las organizaciones no pueden identificar adecuadamente cuál propuesta es la más idónea para su uso. Es así que se definió Essence Sec para permitir a las organizaciones que cuentan o no con áreas de seguridad, el poder implementar aspectos de seguridad a sus procesos de software ya que hace uso de las características de la Esencia, e incorpora los criterios de seguridad que son necesarios contemplar a la hora de estar realizando un sistema, permitiendo a las organizaciones producir desarrollos de forma repetible y organizada con aspectos de seguridad incluidos.

Como trabajo futuro es necesario realizar la validación del trabajo a través de diversos casos de estudios que permitan comprobar de forma práctica su uso y perfeccionarlo.

VI. Agradecimientos

Este trabajo ha sido financiado el Programa de Apoyo a los Estudios de Posgrado (UNAM) y el programa de becas del CONACyT.

Este trabajo ha sido desarrollado dentro del Proyecto SEQUOIA (TIN2015-63502-C3-1-R), cofinanciado por el Fondo Europeo de Desarrollo Regional (FEDER), Ministerio de Economía y Competitividad (MINECO/FEDER), y por el proyecto GLOBALIA (PEII11-0291-5274) de la Consejería de Educación, Ciencia y Cultura (Junta de Comunidades de Castilla La Mancha) y Fondo Europeo de Desarrollo Regional FEDER.

Referencias

[1] M. Piattini Velthuis and F. Hervada Vidal, *Gobierno de las Tecnologías y los Sistemas de Información*. Ra~Ma, 2007.

[2] Trustwave, “Trustwave Global Security Report,” 2016.

[3] M. Piattini Velthuis, F. García Rubio, I. García Rodríguez de Guzmán, and F. J. Pino, *Calidad de Sistemas de Información*. 2015.

[4] I. Jacobson, P. Ng, P. McMahon, I. Spence, and S. Lidman, “Kernel and Language for Software Engineering Methods (Essence),” *OMG*. OMG, USA, 2014.

[5] I. Jacobson, P.-W. Ng, P. E. McMahon, I. Spence, and S. Lidman, *The Essence of Software Engineering*. USA: Addison - Wesley, 2013.

[6] I. Jacobson, P. W. Ng, P. E. McMahon, I. Spence, and S. Lidman, “La esencia de la ingeniería de software: El núcleo de Semat,” *Rev. Latinoam. Ing. Softw.*, vol. 1, no. 3, pp. 71–78, 2013.

[7] ISO/IEC JTC! /SC27, “ISO/IEC 27001:2005 Information technology -- Security techniques -- Specification for an Information Security Management System.,” Geneva, Switzerland, 2005.

[8] Microsoft, “Security Development Lifecycle for Agile Development.” Microsoft, 2009.

[9] A. B. Arkin *et al.*, “Building Security In Maturity Model - Version 7.0.” 2016.

[10] The Open Web Application Security Project, “Software Assurance Maturity Model - Version 1.5.” OWASP, 2016.

[11] ISO/IEC_JTC1/SC27, “Information technology — Security techniques — Evaluation criteria for IT security, ISO/IEC 15408:2005 (Common Criteria v3.1),” 2012.

[12] Object Management Group, “Specifications for Automated Quality Characteristic Measures CISQ.” OMG, USA, 2012.

[13] M. de H. y A. Públicas, “Metrica 3 Introducción,” *Ministerio de Hacienda y Administraciones Públicas*. [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Metricav3/METRICA_V3_Introduccion.pdf. [Accessed: 25-Apr-2017].

[14] Ministerio de Hacienda y Administraciones Públicas, “Metrica 3 Interfaz de Seguridad.” [Online]. Available: http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Metricav3/METRICA_V3_Seguridad.pdf. [Accessed: 25-Apr-2017].

[15] R. Kissel, K. Stine, M. Scholl, H. Rossman, J. Fahlsing, and J. Gulick, “NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle.” NIST, 2008.

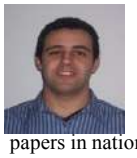
[16] C. Pardo, F. García, F. J. Pino, M. Piattini, and M. T. Baldassarre, “Método de integración para soportar la armonización de múltiples modelos y estándares,” in *XVI Jornadas de Ingeniería del Software y Bases de Datos (JISBD 2011)*, 2011.

[17] F. Arellano, “Modelo de Procesos para la Mitigación de Amenazas y Vulnerabilidades de la Seguridad Informática en el Desarrollo de Software,” National Autonomous University of Mexico, 2017.

Francisco Arellano Mendez is an BEng from the Morelia Institute of Technology with specialization in Security and Information Management and is currently a MSc student in Computer Science at the National Autonomous University of Mexico (UNAM). His research interests are software engineering, processes engineering and Information security.

Ma. Guadalupe E. Ibargüengoitia González *is a* full Professor at the National Autonomous University of Mexico (UNAM) in the Faculty of Sciences in the career of Computer Science and in the Postgraduate in Science and Engineering of Computing. He has taught courses in Software Engineering since 1982 at the undergraduate level and in 1993 at the postgraduate level. He has taught Software Engineering courses at the undergraduate and master's level at national and international universities. He has advised companies and organizations on software development. Her research interest are software engineering and processes engineering.

Mario Piattini is MSc and PhD in Computer Science from the Politechnical University of Madrid. He is certified information system auditor by ISACA (Information System Audit and Control Association). He is Associate Professor at the Escuela Superior de Informática of the Castilla- La Mancha University (Spain). He is author of several books and papers on databases, security, software engineering and infor- mation systems. He leads the ALARCOS research group of the Department of Computer Science at the University of Castilla- La Mancha, in Ciudad Real (Spain). His research interests are: advanced database design, database quality, software metrics, object-oriented metrics and software maintenance.



David G. Rosado has an MSc and PhD. in Computer Science from the University of Málaga (Spain) and from the University of Castilla-La Mancha (Spain), respectively. His research activities are focused on security for Information Systems and Cloud Computing. He has published several papers in national and international conferences on these subjects, and he is co-editor of a book and chapter books.
Author of several manuscripts in national and international journals (Information Software Technology, System Architecture, Network and Computer Applications, etc.). He is member of Program Committee of several conferences and workshops nationals and internationals such as ICEIS, ICCGI, CISIS, SBP, IAS, SDM, SECRYPT, COSE and international journals such as Internet Research, JNCA, KNOSYS, JKSU, and so on. He is a member of the GSyA research group of the Information Systems and Technologies Department at the University of Castilla-La Mancha, in Ciudad Real, Spain.