Abstraction & Application **17** (2017) 50 – 60

UADY

Incorporación de aspectos de seguridad en los procesos de desarrollo de software con Essence Sec

Francisco Arellano Méndez[1], Ma. Guadalupe E. Ibargüengoitia González[2], Hanna Oktaba[3]

Mario Piattini[4]

[1,2,3] Universidad Nacional Autónoma de México

[1,2,3] Ciudad de México, México

[1] franciscoarellanomendez@gmail.com, {[2] gig, [3] hanna.oktaba}@ciencias.unam.mx

[4] Grupo de Investigación ALARCOS, Universidad de Castilla - La Mancha

[4] Ciudad Real, España

[4] Mario.Piattini@uclm.es

Abstract

Information security has become relevant to the technological environment and society, which is more dependent on software systems. Hence the importance of developing systems that have security measures intrinsically, allowing the daily activities of society to develop smoothly. Therefore, the objective of this research is to develop and present a software development process model called Essence Sec, which allows the construction of systems by reducing states with anomalies that affect the properties of confidentiality, integrity and availability (CIA) through the use of Essence [1].

Resumen

La seguridad de la información en los últimos tiempos ha cobrado relevancia para el entorno tecnológico y de la sociedad, la cual tiene mayor dependencia de los sistemas de software. De ahí la importancia de desarrollar sistemas que cuenten con medidas de seguridad de manera intrínseca, permitiendo que se desarrollen las actividades diarias de la sociedad sin contratiempos. Por lo que el objetivo de la presente investigación es desarrollar y presentar un modelo de proceso de desarrollo de software llamado Essence Sec, que permita la construcción de sistemas reduciendo los estados con anomalías que afecten las propiedades de confidencialidad, integridad y disponibilidad (CIA), a través del uso de La Esencia[1].

Fecha de recepción: Junio 09, 2017 / Fecha de aceptación: Julio 14, 2017

Keywords and phrases: Desarrollo de Sistemas Seguros, Seguridad de Sistemas de Información, Métodos de seguridad para sistemas de información, Ingeniería de Software, Seguridad Informática.

2010 Mathematics Subject Classification: 67N30

1. Introducción

La Informática en la actualidad forma parte fundamental de la vida diaria de las personas, las computadoras, los dispositivos móviles y toda su interconexión se han convertido en algo consustancial al nuevo paradigma de la sociedad. Esto se observa en las actividades industriales, comerciales, militares, de investigación y de servicios tales como transporte, salud y la educación que dejarían de funcionar sin el apoyo que reciben de los sistemas de información, ya que la mayor parte de la información se encuentra computarizada, lo que permite mejorar su explotación, pero al mismo tiempo se hace dependiente del buen funcionamiento de los sistemas.

Es así, que la seguridad dentro de los procesos de la Ingeniería de Software ha tomado relevancia por parte de los directivos no solo de las organizaciones que los producen, sino también de aquellas que hacen uso de ellos, debido a los impactos monetarios, pérdida de reputación y otros aspectos como lo reporta Trustwave en su último informe [2]. Se observa en la prensa a nivel mundial, especializada y no en el contexto tecnológico, donde se informa de diferentes organizaciones que han sufrido vulnerabilidades en sus sistemas, afectando tanto a las organizaciones como a todos los usuarios que hacen uso de los sistemas directa o indirectamente.

Estos “fallos”, ahora lamentablemente noticia cotidiana, se producen principalmente por no aplicar medidas de seguridad en el desarrollo de sistemas de software. Y aunque existen diversas propuestas para la incorporación de la seguridad en la Ingeniería de Software, no han sido adoptadas por las organizaciones que los desarrollan por diferentes aspectos como son: el aumento de roles dentro de los procesos, cambios radicales en la forma de trabajar o por el desconocimiento o negligencia de los directivos que están a cargo del proyecto.

Por tal motivo, el objetivo de la presente investigación es el adicionar aspectos de seguridad al estándar del Object Management Group (OMG) “la Esencia” [1], a la que llamaremos Essence Sec, la cual permitirá crear sistemas robustos y con mejor tolerancia a fallos de seguridad. Para lograrlo, primeramente se creó un marco común de los aspectos de seguridad indispensables a considerar en cualquier desarrollo. Posteriormente estos aspectos de seguridad se incorporaron a la Esencia basados en su filosofía, adicionándolos a las listas de verificación de algunos Estados de las Alfas, agregando espacios de actividades para complementar la visión de seguridad y en aquellos casos que se requiera la adición de Sub-Alfas.

Este artículo se organiza de la siguiente forma: en la sección II se presenta la descripción general de la Esencia para tener un panorama de su forma de trabajar. A continuación, en la sección III se muestran las bases para la extensión de la Esencia. En la sección IV se presentan las bases de seguridad necesarias para llevar a cabo la investigación, donde se realizará la armonización de los

Marcos y Estándares que incorporan la seguridad a la Ingeniería de Software. En seguida se presenta la sección V donde está la propuesta, la cual describe la armonización de la sección IV con la Esencia. En la sección VI, se expresan las conclusiones obtenidas al finalizar la investigación, en la sección VII se presentan los agradecimientos y finalmente las fuentes consultadas en la sección VIII.

2. La Esencia

La Esencia [1] es un estándar del OMG aprobado en 2014 que define los conceptos principales que tienen en común todos los desarrollos de software a través de métodos, prácticas, un núcleo y lenguaje común [3].

El núcleo de la Esencia es un marco de trabajo que permite identificar de forma temprana la salud y progreso del proyecto; esto se logra gracias a tres áreas de interés que son: *Cliente*, *Solución* y *Esfuerzo*. Cada una de ellas contiene una serie de conceptos clave llamadas Alfas que son los aspectos que hay que tener presentes en todo momento durante un proyecto de desarrollo de software, permitiendo tener una base común para la definición de métodos y prácticas de la Ingeniería de Software [4].

La Esencia identifica siete Alfas las cuales se ubican en las tres áreas de interés:

> ***Cliente*.** Contiene las Alfas de *Oportunidad* (Opportunity) e *Interesados* (Stakeholders)
>
> ***Solución*.** Contiene las Alfas de *Requerimientos* (Requirements) y *Sistema de software* (Software System).
>
> ***Esfuerzo/Proyecto*.** Esta área considera los elementos para realizar el proyecto tales como *Equipo* (Team), *Forma de trabajar* (Way of Working) y *Trabajo* (Work).

Cada una de estas Alfas contiene una serie de Estados secuenciales que permiten observar la evolución de los temas de las Alfas desde el inicio hasta el final de un proyecto. Cada Estado tiene asociadas unas listas de verificación ya definidas que permiten analizar el cumplimiento de criterios para asegurar que se está en cierto Estado del Alfa.

Por otro lado, la Esencia presenta unos *Espacios de actividades* que definen las cosas esenciales a realizar y las *Competencias* que expresan las capacidades que deben de tener las personas que trabajarán en el proyecto.

Así mismo, la Esencia cuenta con Anexos que permiten incluir conceptos a los desarrollos de software. En este trabajo se hace uso del Anexo A que trata de “Extensiones opcionales al Kernel”, que permite aumentar prácticas que el Kernel no consideró o se presentan desde una perspectiva abstracta. Una forma de usar la Extensión del Kernel es el uso de Sub-Alfas que permitan expresar el accionar de un Alfa a bajo nivel.

El Anexo B [2] adiciona 4 Alfas a las expresadas en el Kernel que permiten trabajar con las Alfas: *Forma de Trabajo* y *Trabajo.* Así mismo se implementan “La Autorización de Prácticas” que permiten expresar la forma de trabajar de una práctica utilizando una plantilla base; en esta plantilla se solicita información y datos de la práctica. La plantilla ayuda en la síntesis de métodos y prácticas de las organizaciones.

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.

3. Extensión de la Esencia

Para realizar adecuadamente la extensión de seguridad en la Esencia se hizo uso de su filosofía, incorporando prácticas profesionales que incluyen las mejores prácticas de seguridad disponibles en la industria. Es así que se procedió a realizar esta extensión.

Se obtuvieron los siguientes principios que coadyuvaran a realizar adecuadamente la extensión:

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

Debido a que en estas Alfas son en las que se presentan los aspectos técnicos que se deben considerar para la correcta inclusión de la seguridad dentro de la Esencia.

- Estas Alfas se mantuvieron lo más general posible.
- Se incluyó una Sub-Alfa únicamente donde era necesario para hacer una distinción sobre las prácticas y la modificación a las listas de verificación realizado en base al Anexo A de la Esencia [1]. La Sub-Alfa agregada es *Evaluación de Riesgos de Seguridad* en virtud que los aspectos de seguridad a implementar son complejos de analizar si se realizan de manera dispersa.
- Se refinaron las listas de verificación de los Estados de las Alfas, agregando un anexo con las características de seguridad que se deben de tomar en cuenta para que ese Estado se cumpla satisfactoriamente.
- Se agregaron actividades en los Espacios de Actividades con la finalidad de tener mayor detalle de aquellas que necesiten tener más claridad para su realización basados en el Anexo B Kuali-Beh de la Esencia [1].

Estas acciones se consideraron con la finalidad de que los usuarios que actualmente hacen uso de la Esencia en su forma tradicional, 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. Para los nuevos usuarios que desean hacer uso de la Esencia, les permitirá incluir medidas de seguridad en sus desarrollos de una forma transparente desde el primer momento que la utilicen.

Así mismo, se consideró el nivel de comprensión en temas de seguridad por parte de los usuarios por lo que, para las personas con experiencia, al hacer uso de las listas de verificación de seguridad podrán recordar las consideraciones que llevan a cabo durante el proceso y para los usuarios que

apenas se están familiarizando con temas de seguridad, se especifican detalladamente los procedimientos en las actividades, brindándoles lo necesario a realizar para lograr las metas de las listas de verificación correspondientes a cada Estado del Alfa.

Todas estas consideraciones se realizaron con la finalidad de brindar una propuesta integral para los diversos perfiles de usuarios que hacen uso de la Esencia sin que se pierda su propósito y se proporcione un valor agregado a los productos finales.

4. Incorporando la Seguridad a la Esencia

Para lograr el objetivo de incorporar la seguridad a los procesos de desarrollo de sistemas de software, se procedió a extraer las "Mejores prácticas de Seguridad" que actualmente se implementan en la industria a través de marcos y estándares de Ingeniería de software como: ISO/IEC 27001[5], Microsoft SDL [6], The Building Security In Maturity Model (BSIMM) [7], The Software Assurance Maturity Model (SAMM) [8], Common Criteria (CC) [9], Métrica 3 [10] y NIST Information Security [11]. Se observó que cada uno de estos marcos y estándares tenían ciertas peculiaridades que hacen que su implementación por parte de las organizaciones no se lleve a cabo de forma adecuada, debido a que la mayoría propone un cambio radical en la forma de trabajar ya sea incorporando más roles al personal, hasta modificando la forma en que se da seguimiento al proyecto. Todo esto genera que las organizaciones que se van iniciando no deseen incorporar estos marcos y las organizaciones ya establecidas los implementen de manera deficiente, o los implementen debido a una obligación normativa y no por convicción.

Es así, que se buscó reunir esos marcos y estándares en un solo compendio con las mejores prácticas de cada uno. Para realizarlo primero se efectuó un análisis de la estructura con la que se describen y la filosofía que siguen, llegando a la conclusión de que, para realizar el mapeo de manera uniforme se debía considerar una estructura común para homogenizarlo.

Se llevó a cabo el análisis para poder conocer las similitudes y diferencias entre ellas, los aspectos de la seguridad que se ven involucrados, los roles y actividades que se deben de implementar.

Este análisis dio como resultado la identificación de 14 aspectos de seguridad que tienen en común los marcos y estándares analizados, los cuales son: amenazas, riesgos, superficie de ataque, requisitos de seguridad, diseño de seguridad, arquitectura de seguridad, pruebas de seguridad, entrenamiento, herramientas, marcos y regulaciones, estandarización de procesos, automatizaciones, control de procesos y finalmente métricas.

Para poder incorporar esos aspectos de seguridad identificados dentro de todo el ciclo de vida del software, se procedió a realizar un análisis a Métrica 3, la cual es una propuesta del gobierno de España, que en su 3ª versión implementa una interfaz adicional de seguridad al proceso de desarrollo normal, lo que permite identificar y comparar en qué procesos se podrían incorporar los aspectos de seguridad identificados.

5. Propuesta

Teniendo claro los principios mencionados en la sección III, que se van a tener en cuenta para la extensión de la Esencia con los marcos y estándares de seguridad, se procedió a realizar el análisis para cada una de las 4 Alfas seleccionadas. En el Alfa de *Requisitos* se identifican los Riesgos de seguridad, para posteriormente obtener los requisitos de seguridad. En el Alfa de *Sistema de Software* se diseña y desarrolla el sistema con aspectos de seguridad incluidos. En el Alfa de *Forma de Trabajo* se identifican y definen los marcos y estándares que guiarán la forma en que se trabaja. Finalmente, en el Alfa de *Trabajo* se seleccionan las herramientas de seguridad que se implementarán

en el trabajo además de los principios a considerar. En este trabajo se ejemplifica el Alfa de Requisitos y los otros podrán ser consultados en la tesis [12].

Sub-Alfa: Evaluación de Riesgos de Seguridad

Esta Sub-Alfa se incluyó como una extensión de Essence Sec y es parte del Alfa de Requisitos, para ayudar a los equipos a conocer y evaluar los riesgos de seguridad a los que el Sistema de Información (SI) está expuesto, su relación puede observarse en la Figura I. Una vez que se conocen los riesgos de seguridad es posible obtener los requisitos de seguridad que se unen a los requisitos generales en el Estado *Acotado* del Alfa de Requisitos.

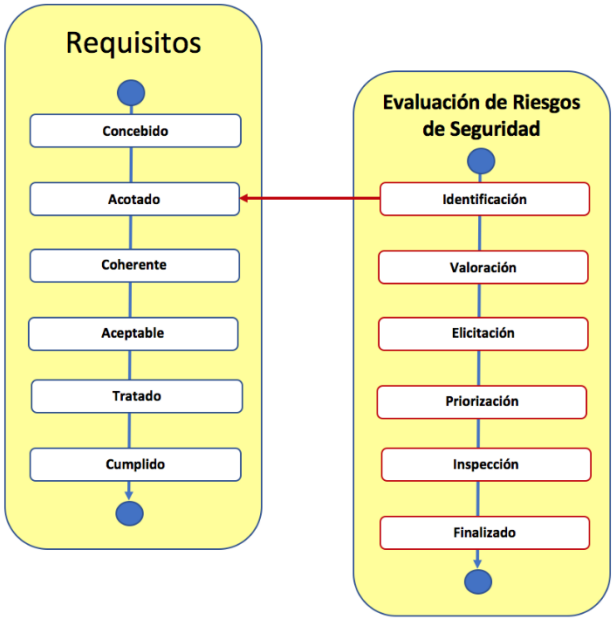

FIGURA I. Alfa de Requisitos y su relación con el Sub-Alfa Evaluación de Riesgos de Seguridad

Los Estados de la Sub-Alfa son:

Identificación	Se han identificado los activos que están involucrados en el sistema, así como las posibles amenazas que pudieran tener.
Valoración	La valoración de las amenazas provee una referencia para determinar el riesgo que pudieran tener y su relevancia de acuerdo a la visión de seguridad establecida.
Elicitación	Se realizó un estudio de la relevancia de cada objetivo de seguridad junto con las amenazas que impliquen riesgo para así obtener los requisitos de seguridad, que sirvan de salvaguarda para la reducción del riesgo hasta niveles aceptables.
Priorización	Se clasifican los requisitos de seguridad y priorizan en función de la visión de seguridad, del impacto y la probabilidad de ocurrir.
Inspección	Los requisitos de seguridad están expresados de forma adecuada sin ambigüedades ni duplicidades.
Finalizado	Se unifican los requisitos del sistema con los requisitos de seguridad obtenidos para aplicarlos en el desarrollo.

El primer estado busca identificar activos y amenazas con el fin de contar con la Evaluación de Riesgos de Seguridad del sistema de información a implementar, para establecer las fortalezas, debilidades, oportunidades y amenazas a las que se enfrentará en su entorno de operación, teniendo la posibilidad de contar con una estrategia eficaz de la gestión de riesgos, conociendo con anterioridad eventos que pudieran resultar inesperados, estando mejor preparados para responder en caso que llegaran a ocurrir.

El segundo estado realiza la valoración de todas las amenazas detectadas para cada uno de los activos o grupo de activos, así como de su entorno.

El tercer estado valora el riesgo de las amenazas y para determinar el nivel de riesgo que representan y tener la posibilidad de establecer su clasificación de acuerdo a la visión de seguridad establecida en el proyecto.

El cuarto estado es la priorización de acuerdo a las necesidades existentes. El quinto realiza la inspección para detectar ambigüedades o duplicados en los requisitos. Finalmente, el estado de Finalizado unifica los requisitos de seguridad permitiendo solventar la visión de seguridad.

Para conocer claramente el estado y progreso de la Evaluación de Riesgos, se proporciona en la Tabla I, donde se muestra la lista de verificación para cada Estado de la Sub-Alfa

TABLA I.Lista de Verificación para cada Estado del Sub-Alfa: *Evaluación De Riesgos De Seguridad*

Estado	Verificación
Identificación	• La visión de seguridad para el proyecto está definida y alineada a las metas del negocio. • Se identificaron los activos que están presentes en el sistema. • Las dependencias que tiene cada activo identificado fueron analizadas. • Los usuarios que tiene cada activo identificado fueron analizadas. • Cada activo identificado forma parte de la visión de seguridad establecida. • Se identificaron y comprendieron las amenazas. • Se modelaron las amenazas identificadas.
Valoración	• Se estimó el riesgo de las amenazas identificadas. • Se realizó un ranking para definir los riesgos prioritarios para el proyecto. • Los interesados están de acuerdo con el ranking establecido. • Los interesados tienen claro la forma en que se mitigarán los riesgos de seguridad identificados. • Se establecieron las métricas que se deberán cumplir para verificar que se mitigaron los riesgos.
Elicitación	• El equipo valoró y evaluó las alternativas de solución para los riesgos identificados. • Se modelaron importantes escenarios de los requisitos usando casos de seguridad y mal uso. • Se identificaron los requisitos indispensables para cumplir con la visión de seguridad establecida para el proyecto. • Se identificaron y resolvieron las dependencias y conflictos entre los requisitos de seguridad (Funcionales y no Funcionales). • Se definieron los criterios para verificar los requisitos de seguridad. • Se acordaron las pruebas que permitan definir el cumplimiento de las métricas establecidas.

Estado	Verificación
	• Están claros los umbrales de la seguridad y su nivel mínimo aceptable a obtener de las pruebas.
Priorización	• Las prioridades de los requisitos de seguridad en el sistema están claras. • Los interesados están de acuerdo con la priorización de los requisitos de seguridad realizada.
Inspección	• Los requisitos de seguridad obtenidos no contienen redundancias. • Los requisitos de seguridad obtenidos no contienen ambigüedades.
Finalizado	• Los requisitos de seguridad describen una solución aceptable para resolver los objetivos definidos.

Alfa: Requisitos

Otro elemento que incluye la Essence Sec es la inclusión de medidas de seguridad en el Alfa de Requisitos que propone la agregación de elementos extras en las listas de verificación de los estados ya establecidos por la Esencia. Estos elementos extras, permiten hacer revisiones periódicas para la comprobación de actividades de seguridad dentro de sus desarrollos favoreciendo la reducción de los fallos de seguridad. A continuación, en la Tabla II, se proporciona la lista de verificación con aspectos de seguridad que se agregan a la lista existente y que deben ser cubiertos para cada Estado del *Alfa de Requisitos*, así como los aspectos secundarios de seguridad que se ven incluidos.

TABLA II. Lista de Verificación para cada Estado del Alfa: *Requisitos*

Estados Requisitos	Verificación de Seguridad
Concebido	La plataforma informática a la que pertenece el proyecto está clara. Los esquemas de las normativas y regulaciones que impactan al proyecto están identificados. Se tienen identificados los usuarios que están directa e indirectamente involucrados con el sistema.
Acotado	Se ha realizado satisfactoriamente la evaluación de todos los estados del sub-alfa "Evaluación de Riesgos" generando los requisitos de seguridad. Se han acotado los requisitos de seguridad.
Coherente	Se identificaron las medidas de seguridad en el entorno de desarrollo.
Aceptable	El sistema satisface completamente las pruebas de seguridad establecidas en los requisitos de seguridad. Las métricas obtenidas de las pruebas cumplen con los umbrales preestablecidos.
Tratado	Se han monitoreado las medidas de seguridad en el entorno de operación.
Cumplido	Los interesados reconocen el valor proporcionado por la implementación de la seguridad en el proyecto.

En resumen, cabe mencionar que se cuentan con 8 prácticas que permiten realizar la validación de los Estados en la Sub-Alfa *Evaluación de Riesgos de Seguridad*, donde cada una de ellas está creada con base en las necesidades que se muestran en las listas de verificación de cada Estado que se obtuvieron a partir de las prácticas de los marcos y estándares para la seguridad existentes como se

mencionó en la sección IV, así como de los profesionales del área de acuerdo con su experiencia y conocimiento. Estas recomendaciones expresan la forma que se debe de trabajar, describiendo las actividades y sus respectivas tareas a realizar, también los recursos de entrada que se necesitan para poder operar y los recursos de salida que se obtienen como resultado de su realización. Se pueden consultar en la tesis [12] para más detalles.

Alfas Adicionales

Como se mencionó al inicio del apartado III, se realizó un análisis para poder realizar la implementación de la seguridad en los procesos de la Esencia y se trabajaron en cuatro Alfas específicas: *Requisitos*, *Sistema de software*, *Forma de trabajo* y *Trabajo*. Donde el Alfa de *Requisitos* fue la que se tomó de ejemplo para este trabajo.

En el Alfa de *Sistema de Software* se busca crear el software con una arquitectura que incluya medidas de seguridad. Adicionalmente se debe contar con la verificación de la seguridad en las fases de liberación, operación y concluyendo con el retirado del software. Las preguntas que se incluyen en la Lista de verificación de esta alfa son:

Sis Soft -1: ¿Se identificaron las particularidades de seguridad del proyecto que pueden impactar directa o indirectamente al diseño y arquitectura del sistema?

Sis Soft -2: ¿Se seleccionó una arquitectura que permita incluir los aspectos de seguridad identificados?

Sis Soft -3: ¿Se identificaron los servicios compartidos que pudieran tener el sistema y qué riesgos pueden representar?

Sis Soft -4: Los escenarios de seguridad a los que se enfrentara el sistema fueron claramente definidos.

Sis Soft -5: Los procesos de diseño fueron dirigidos hacia servicios y diseños seguros conocidos desde el inicio.

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)

Y finalmente 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?

Las listas de verificación de cada Alfa, así como las Actividades que se encuentran asociadas a ellas, le permitirán a los administradores del proyecto identificar en qué fase del proyecto se encuentran, y les brindará una visión de cómo se encuentra implementada la seguridad dentro de sus procesos de desarrollo.

6. Conclusiones

Al finalizar la presente investigación se obtuvo Essence Sec, una propuesta que incluye aspectos de seguridad dentro de los procesos de la Ingeniería de Software basada en diferentes marcos y estándares de seguridad. Esta propuesta permite a las organizaciones que cuentan o no con áreas de seguridad estructuradas, poder implementar aspectos de seguridad a sus procesos desde la visión de la Esencia permitiendo incluir en sus métodos de producción aspectos de seguridad.

Ello se realiza a través de las Listas de Verificación de Seguridad que se anexan a los procesos generales de la Esencia, brindando la posibilidad de hacer revisiones periódicas a lo largo del desarrollo para conocer en qué fase se encuentran, así como las mejoras que pudieran tener para su inclusión.

Así mismo se cuenta con una base de conocimientos sobre las implementaciones de seguridad en la industria a través del análisis y homogeneización realizada, lo que permite tener un panorama general de los aspectos de seguridad que se consideran a la hora de realizar el desarrollo del sistema.

Como trabajo futuro se propone la realización de un caso de estudio que permita validar la propuesta, ya que en estos momentos únicamente se tienen las revisiones de expertos en las áreas de Ingeniería de software y de Seguridad, pero sería ideal el poder contrastarlo con practicantes dentro de un proyecto en desarrollo.

Agradecimientos

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. También ha sido financiado por el Programa de Apoyo a los Estudios de Posgrado de la UNAM y el programa de becas del CONACyT.

A todos se les agradece el apoyo brindado para poder hacer posible la realización de la presente investigación.

Referencias

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

[2] Trustwave Holdings Inc., “Trustwave Global Security Report,” 2017.

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

[4] Software Guru, “Software Guru No.46.” Software Guru, México, 2014.

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

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

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

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

[9] Common Criteria, “Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model September 2012 Revision 4 Foreword,” ISO/IEC 15408 Common Criteria, Part 12012, no. September, p. 93, 2012.

[10] Ministerio de Hacienda y Administraciones Públicas, “Métrica 3 Introducción.” [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].

[11] 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.

[12] F. Arellano, “Modelo de Procesos para la Mitigación de Amenazas y Vulnerabilidades de la Seguridad Informática en el Desarrollo de Software,” Universidad Nacional Autónoma de México, 2017.