
LOS LIBERTADORES
1982
FUNDACIÓN UNIVERSITARIA

Ciclo de vida de desarrollo ágil de software seguro

Miguel Hernández Bejarano*
mhernandezb@libertadores.edu.co

Luis Eduardo Baquero Rey*
lebaqueror@libertadores.edu.co

Colección INVESTIGACIÓN

---

* Grupo de Investigación en Ingeniería Aplicada (GUIAS).

Catalogación en la Publicación Fundación Universitaria Los Libertadores

Hernández Bejarno, Miguel
Ciclo de vida de desarrollo ágil de software seguro Miguel Hernández Bejarano / Luis Eduardo Baquero Rey, – Bogotá: Fundación Universitaria Los Libertadores, 2020.
108 páginas, ilustraciones, gráficas; 26 cm (Colección Investigación)

ISBN: 978-958-5478-41-1 (impreso) | ISBN: 978-958-5478-44-2 (digital)

1. Seguridad en el software – 2. Metodologías ágiles – 3. Desarrollo de software seguro – 4. Seguridad informática. I Hernández Bejarano, Miguel, Autor II. Fundación Universitaria Los Libertadores.

SCDD 005.8 B222c –dc23 **FULL BIBLIOTECA**

Primera Edición: Bogotá, diciembre de 2020

Cra. 16 No. 63A-68/ Tel. 2544750.
www.ulibertadores.edu.co

Juan Manuel Linares Venegas
Presidente del Claustro

Ángela María Merchán Basabe
Rectora

Jefferson Miguel Hernández Cáceres
Diagramación

Diego A. Martínez Cárdenas
Coordinador Editorial

Los autores declaran que esta investigación fue financiada por la Fundación Universitaria Los Libertadores en el marco de la Convocatoria de Investigaciones internas de la institución. Los conceptos emitidos en esta publicación son responsabilidad expresa de los autores y no comprometen de ninguna forma a la institución.
 Escrito en LaTeX.

Agradecimientos

Los autores expresan especial agradecimiento a todas aquellas personas que de una u otra manera han contribuido para que esta obra haya sido posible, empezando por los estudiantes del semillero de investigación en seguridad informática donde nació la idea del proyecto, a los colegas del programa de Ingeniería de Sistemas, a los colegas del Grupo de Investigación en Ingeniería Aplicada (GUIAS), a los directivos de la Facultad de Ingeniería y Ciencias Básicas, y en general a la Fundación Universitaria Los Libertadores por brindar los espacios y el apoyo financiero necesario.

A Dios, a mi esposa Flor Ángela e hijos (Jefferson, Julieth y Oscar).
Miguel

A Dios, mi familia, colegas y estudiantes
Eduardo

Prólogo

Nos encontramos inmersos en una sociedad donde el consumo de datos sobre diversas plataformas conectados a través de Internet requiere de un alto nivel prestacional por parte de diversos sectores y actores tecnológicos, como proveedores de servicio, fabricantes, así como el sector de la industria del software. Soluciones basadas en aplicaciones que soportan solicitudes para el ingreso o consumo de datos en tiempo real sobre cualquier área: lúdica, consumo, ocio, trabajo, educación, entre otros. Esta variedad de soluciones demanda grandes desafíos, orientados a cada vez más altos niveles de prestaciones que puedan ofrecer, tales como la disponibilidad, robustez, interoperabilidad, integridad, etc., de cada uno de sus componentes, incluyendo aspectos trascendentales propios para lograr mitigar riesgos y vulnerabilidades de seguridad.

La realidad de la cantidad de procesos que se desprenden de soluciones informáticas es tan variada, que, para llevar a cabo su correcto desarrollo bajo especificaciones y estándares, requieren de un alto nivel de madurez en todos y cada uno de los procesos establecidos en las etapas de desarrollo de software. Es así como la presente obra, presenta una de esas realidades inmersas sobre un variado ecosistema de soluciones digitales basadas en software; enfocado puntualmente sobre estrategias y métodos para mitigar riesgos de seguridad dentro de procesos enmarcados en el ciclo de vida del desarrollo de software. Lo anterior, bajo diversas miradas que presenta el mercado informático a partir de metodologías ágiles. Indudablemente una apuesta que permite acercarnos a una de serie de consideraciones y criterios que todo equipo, empresa o casa matriz de desarrollo necesitan conocer e identificar, con el propósito de poder cubrir aspectos esenciales en el despliegue de aplicaciones y soluciones informáticas que logren ser distribuidas sobre el mercado.

Dentro de la presente obra, el lector podrá encontrar apartados orientados a destacar el panorama que presentan las metodologías de desarrollo ágil dentro del contexto de software seguro. Así mismo, la relevancia que presenta el desarrollo ágil, de la mano de estrategias y buenas prácticas para el desarrollo seguro del software. Finalmente, los autores exponen de manera detallada y validando mediante caso de estudio aplicado, una propuesta metodológica partiendo de los principios de ciclo de vida de desarrollo de software, y el uso de estrategias de seguridad a considerar en cada una de las fases planteadas.

Me place encontrar dentro de la literatura nacional, este tipo de apuestas orientadas a ofrecer espacios de análisis, reflexión y propuestas concretas asociadas a métodos de desarrollo de software ágil a partir de estrategias de seguridad, sobre todo, en el marco de una variada industria de software apalancada por emprendimientos de base tecnológica, donde el software como actor del ecosistema digital, es uno de los insumos valiosos para una sociedad que demanda cada vez más servicios en línea.

Paulo Alonso Gaona García, Ph.D

Introducción

El mercado es cada día más exigente en cuanto a desarrollo de software se refiere. Ya no es suficiente con que las casas desarrolladoras de programas informáticos cumplan a cabalidad con los requerimientos de funcionalidad que satisfacen las necesidades del cliente, sino que además se deben involucrar aspectos relevantes de los requisitos no funcionales que de alguna manera mitiguen los posibles riesgos a los que pueda estar expuesto el producto cuando este se encuentre en la etapa productiva, pues el número de vulnerabilidades es cada vez mayor, lo que pone en riesgo la información y, por ende, la continuidad del negocio de las organizaciones.

Las herramientas ágiles buscan dar soluciones informáticas oportunas con la participación activa y directa del cliente, y pueden ofrecer mayor seguridad a las aplicaciones desarrolladas al involucrarlas con un ciclo de vida de desarrollo de software seguro. Esta obra da cuenta de los resultados obtenidos durante una investigación aplicada a la integración de un ciclo de vida de desarrollo de software seguro (S-SDLC), de fundamentos teóricos y herramientas existentes para el desarrollo ágil de este tipo de proyectos y de buenas prácticas de seguridad de la información en los desarrollos de productos software. Para ello, se propuso una metodología implementada bajo las circunstancias del planteamiento de un caso de estudio hipotético, que podría ser real.

Es conveniente reseñar la concepción del proyecto desde el semillero de investigación en seguridad informática, que posteriormente se planteó en el marco de la convocatoria interna de proyectos de investigación institucional en la línea de investigación de Innovación y Emprendimiento, como parte integrante del Grupo de Investigación en Ingeniería Aplicada (GUIAS).

El objetivo fundamental en la seguridad del software es la construcción de aplicaciones informáticas de mejor calidad, más robustas y libres de fallos, que implementen el principio de resiliencia, es decir, que sigan funcionando correctamente ante ataque malicioso (McGraw, 2006).

En respuesta a la creciente tasa de daños y perjuicios causados a las empresas por explotación de las vulnerabilidades de seguridad en los productos de software, se requiere de mayor esfuerzo para desarrollar software más seguro (Keramati y Mirian-Hosseinabadi, 2008).

Para tal efecto, este documento se presenta en seis capítulos, de la siguiente manera:

En el capítulo 1 se realiza un estudio comparativo de diferentes ciclos de vida de desarrollo de software seguro y se determinan sus ventajas y desventajas, para luego establecer la conveniencia de su aplicabilidad con metodologías ágiles de desarrollo de software, partiendo de la flexibilidad y las características que ofrecen, lo que producirá un análisis de resultados y su posterior discusión. Ello servirá de insumo para la industria en este campo.

En el capítulo 2 se estudian los principales elementos y técnicas ágiles implicadas en el desarrollo de un producto software, a fin de determinar los principales elementos aportantes para el desarrollo de la investigación.

El capítulo 3 trata sobre las buenas prácticas y los estándares de seguridad de la información, como la norma ISO 27001 y los Common Criteria (CC); estudia organizaciones como Open Web Application Security Project (OWASP), que aportan esfuerzos importantes para el desarrollo de aplicaciones web seguras; compara herramientas para el desarrollo de software seguro y para el análisis de código, como UMLsec, e identifica las propiedades que debe cumplir un software seguro y las amenazas a dicha seguridad.

En el capítulo 4 se presentan las fases del ciclo de vida de desarrollo de software propuesto, la metodología adoptada, el caso de estudio planteado y su desarrollo en los términos ya enunciados, adoptando el marco de trabajo SCRUM.

Finalmente, en los capítulos 5 y 6 se hace un análisis de los resultados obtenidos y se relacionan las principales conclusiones producto del desarrollo del proyecto, respectivamente.

Con esta investigación se busca adoptar una buena práctica que dé respuesta a requisitos de seguridad que deben contemplar los equipos de desarrollo ágil de software, con el fin de construir productos más estables y robustos, fundamentales en materia de seguridad informática, en pro de garantizar la confidencialidad, disponibilidad e integridad de un producto software. Entretanto, también pretende servir de apoyo a la academia en la formación de nuevos profesionales, como un insumo a tener en cuenta en las líneas de Ingeniería de Software y Seguridad de la Información.

Índice general

Índice de figuras