Revista Cubana de Administración Pública y Empresarial
ISSN 2664-0856 RNPS 2458 / Vol. 8 Núm. 2 / Mayo-Agosto (2024) / e306
Disponible en: https://apye.esceg.cu/index.php/apye/article/view/306

Artículo original

CICLO DE VIDA DE DESARROLLO SEGURO DE SOFTWARE EN LA EMPRESA DATYS

SECURE SOFTWARE DEVELOPMENT LIFECYCLE AT DATYS COMPANY

Sacha Pelaiz Barranco [I] https://orcid.org/0000-0003-1966-7203
Mercedes Delgado Fernández [II] https://orcid.org/0000-0003-2556-1712

[I] Empresa DATYS Tecnologías y Sistemas, La Habana, Cuba
✉ sacha.pelaiz@datys.cu
[II] Escuela Superior de Cuadros del Estado y del Gobierno (ESCEG), La Habana, Cuba
✉ mercedes@esceg.cu

*Autor para dirigir correspondencia: sacha.pelaiz@datys.cu

Clasificación JEL: J24, O31, L86

DOI: https://doi.org/10.5281/zenodo.11221500

Recibido: 13/02/2024
Aceptado: 04/05/2024

Resumen

Abordar la seguridad en etapas demasiado avanzadas del SDLC, después de haber completado las tareas más importantes de análisis, diseño y desarrollo, genera problemas de eficiencia y seguridad, ya que el costo de solucionar vulnerabilidades aumenta mientras más avanzada sea la fase del ciclo, y puede requerir que se vuelva a desarrollar y probar todo el software. Asumir en la empresa DATYS un SDLC tradicional ha impactado en que su proceso productivo, si bien es eficaz, no es del todo eficiente, ya que –en general- las soluciones de software para ser certificadas y liberadas, deben pasar múltiples iteraciones incurriéndose en horas hombre extra plan, y dilatando en muchos casos su culminación. En este artículo se proyecta la transformación del SDLC de la empresa DATYS a un ciclo de vida de desarrollo seguro (SSDLC) a partir de integrar, de manera sistémica, los aspectos de seguridad en cada fase del ciclo de vida de desarrollo.

Publicado por Escuela Superior de Cuadros del Estado y del Gobierno, La Habana, Cuba

Escuela Superior de Cuadros del Estado y del Gobierno

Palabras clave: ciclo de vida, desarrollo, software, seguridad, eficiencia

Abstract

Addressing security too late in the SDLC, after the most important analysis, design, and development tasks have been completed, creates efficiency and security issues, as the cost of fixing vulnerabilities increases the later in the cycle, and may require all software to be redeveloped and tested. Assuming a traditional SDLC in the DATYS company has had an impact on the fact that its production process, although effective, is not entirely efficient, since - in general - the software solutions to be certified and released must go through multiple iterations, incurring hours man extra plan, and in many cases delaying its completion. This article projects the transformation of the DATYS company's SDLC to a secure development life cycle (SSDLC) by systematically integrating security aspects into each phase of the development life cycle.

Keywords: lifecycle, development, software, security, efficiency

Introducción

La Industria del Software es considerada una industria de conocimiento, perteneciente a un sector que ha presentado con un crecimiento acelerado en los últimos años.[1-6] Una de las características principales de las empresas de esta industria es que internalizan la investigación científica y la innovación en la cadena de valor. Para este tipo de empresa la competencia (más que en la escala y el costo) se centra en la innovación, que genera diferenciación de productos y servicios. La innovación es un proceso fundamental dentro de cualquier organización, y en particular en el sector empresarial, ya que se convierte en el motor más importante para su desarrollo. Innovar permite aumentar los beneficios de los productos y servicios; ofrece la oportunidad de lograr una mayor satisfacción por parte de los clientes; generar incrementos en la productividad, posicionamiento estratégico y aprovechar nuevas oportunidades en el mercado logrando mayor competitividad.

En Cuba. la voluntad del gobierno de impulsar la creación y el avance de organizaciones empresariales que garanticen la integración de la investigación y la innovación, el incremento rápido, eficiente y eficaz de nuevos productos y servicios, con estándares de calidad reconocidos y una efectiva gestión de comercialización interna y externa, ha quedado expresada en los Lineamientos de la Política Económica y Social del Partido y la Revolución.[7-8] DATYS es una empresa que produce bienes y servicios informáticos (mayormente de software) de alto valor agregado, sobre cuya base entrega soluciones adaptadas a necesidades específicas de sus clientes, empleando conocimientos científicos y tecnologías propias, combinados con la asimilación de conocimientos de terceros -nacionales y foráneos-. En la empresa se tiene un enfoque continuo hacia la mejora, orientados no solo en mantener los actuales niveles de desempeño, si no creando nuevas oportunidades de negocios con nuevos e innovadores productos y servicios con mayor calidad y seguridad.

La seguridad del software debe ser un aspecto fundamental y prioritario para las empresas que los desarrollan. Sistemáticamente se publican noticias de ciberataques que se aprovechan de vulnerabilidades en las soluciones de software. Un error durante el desarrollo de un software puede causar graves consecuencias a las empresas que los utilizan, tales como: pérdida o robo de información, daños a la imagen corporativa o sanciones económicas. Los riesgos de ciberseguridad aumentan y evolucionan

de una manera incontenible, en correspondencia con los ciberataques que se diversifican y aumentan año tras año,[9,10] convirtiendo en imprescindibles los ciclos de vida de desarrollo seguro de software, así como las metodologías que otorgan un papel protagonista a la seguridad del software.

El ciclo de vida de desarrollo de software (SDLC) es un marco o metodología de trabajo utilizado para desarrollar, implementar y mantener software.[11-13] El SDLC formaliza las tareas o actividades en varias fases con el objetivo de mejorar la calidad del software centrándose en el proceso. La formalización de los pasos tiene como objetivo permitir la medición y el análisis para realizar mejoras mientras se monitorea el progreso y los costos. Tradicionalmente el desarrollo de software está enfocado -principalmente- en cumplir con las funcionalidades exigidas por el cliente, es decir, garantizar la eficacia de las soluciones de software, mientras que, a otras cuestiones, como la seguridad, se les presta mucho menos atención y se le dedica menos recursos, y casi siempre, al final del ciclo de vida de desarrollo.

Abordar la seguridad en etapas demasiado avanzadas del SDLC (por lo general en la fase de pruebas y control de la calidad), después de haber completado las tareas más importantes de diseño y desarrollo, genera problemas de eficiencia, ya que, al igual que con cualquier tipo de fallo, si se encuentra una vulnerabilidad durante la fase de pruebas o tras entregar el software al cliente, el costo de solucionarla puede ser muy alto, tanto en pérdidas económicas, prestigio de la empresa que los desarrolló, como en tiempo de trabajo.[14] Además, los controles de seguridad que se ejecutan -por lo general- en la fase de pruebas o control de la calidad generalmente se limitan al análisis y las pruebas de intrusión. Por eso, es posible, que se pasen por alto problemas de seguridad más complejos que, de detectarse, podrían retrasar la llegada del software al cliente. Además, la resolución de los problemas lleva mucho tiempo y es más costosa, ya que puede requerir que se vuelva a desarrollar y probar todo el software.

Las soluciones informáticas desarrolladas por DATYS para ser liberadas y desplegadas, deben cumplir con los requerimientos de seguridad establecidos en las normas nacionales, así como con los requerimientos del Departamento de Calidad de la empresa, siendo un elemento clave su certificación por el Departamento de Ciberseguridad del Ministerio del Interior. Se define entonces el problema científico a resolver: ¿Cómo transformar el ciclo de vida de desarrollo de software en la empresa DATYS, en un ciclo de vida de desarrollo seguro de software (en lo adelante SSDLC por sus siglas en inglés), en interés de alcanzar mayor eficiencia y seguridad en el proceso productivo de la empresa hacia el 2025?

Este problema se corresponde con la proyección estratégica de la empresa de actualizar su proceso clave productivo de desarrollo de productos y servicios informáticos, en función de lograr mayor eficiencia a partir del ahorro de horas-hombre y recursos materiales, así como de proyectar la seguridad de las aplicaciones y sistemas como un proceso transversal, que debe ser tenido en cuenta en todas las fases del ciclo de vida de desarrollo de software. La solución a este problema transita -esencialmente- por integrar los elementos de seguridad en cada una de las fases del SDLC implementado en la empresa. Por consiguiente, el objetivo del artículo está dirigido a: diseñar el ciclo de vida de desarrollo seguro de software en la empresa DATYS, a partir de la integración de la seguridad en cada una de las fases del ciclo, y en interés de alcanzar mayor eficiencia y seguridad en el proceso clave de la organización.

Materiales y métodos

La transformación del SDLC en la empresa DATYS en un SSDLC requirió de la adaptación de la metodología de gestión de la innovación[15-17] al contexto de aplicación del desarrollo de software. Como parte de la metodología, el diagnóstico organizacional integral realizado en la empresa a su proceso

productivo, permitió conocer las potencialidades de la organización para la introducción de innovaciones, así como identificar las principales causas que impactan en la eficiencia y la seguridad del ciclo de vida de desarrollo de software, con la aplicación de varias técnicas soportadas en el trabajo en equipo con directivos de la organización.

La generación de la innovación con las fases y requisitos del SSDLC, la valoración de los principales indicadores organizacionales y la propuesta de nuevos indicadores o métricas relacionados con la seguridad del proceso de desarrollo de software también forman parte de la metodología de gestión de la innovación adoptada.[15] Los pasos y métodos utilizados se muestran en la **Tabla 1**.

Tabla 1. Metodología de gestión de la innovación para el SSDLC en DATYS

PASOS	MÉTODOS
1. Diagnóstico integral de DATYS sobre necesidades y oportunidades de mejora del ciclo de vida de desarrollo de software.	Vínculo con Lineamientos de la Política Económica y Social 2021-2026 y Plan Nacional de Desarrollo económico y social al 2030 (PNDES 2030), estrategias genéricas, estadísticas de iteraciones, diagrama causa-efecto, variables claves (MICMAC), escenarios (SMIC)
2. Identificación en fases del SDLC los aspectos de seguridad a gestionar y elementos transformadores	Fases del SDLC según diagrama causa efecto y aspectos de seguridad por fase
	Clasificación de la innovación y matriz de impacto, lista de control del proyecto de innovación, fases del ciclo como subprocesos, diagrama integral de seguridad de fases del SLDC y diagrama de flujo de procesos
3. Proyección y validación del SSDLC en DATYS	Indicadores de impacto de eficiencia y seguridad, diseño de experimentos del SSDLC, gestión de riesgos, diagrama de actividades por ciclo Deming (P-H-V-A), plan de actividades y Project por ciclo Deming

Fuente: elaboración propia según metodología[15]

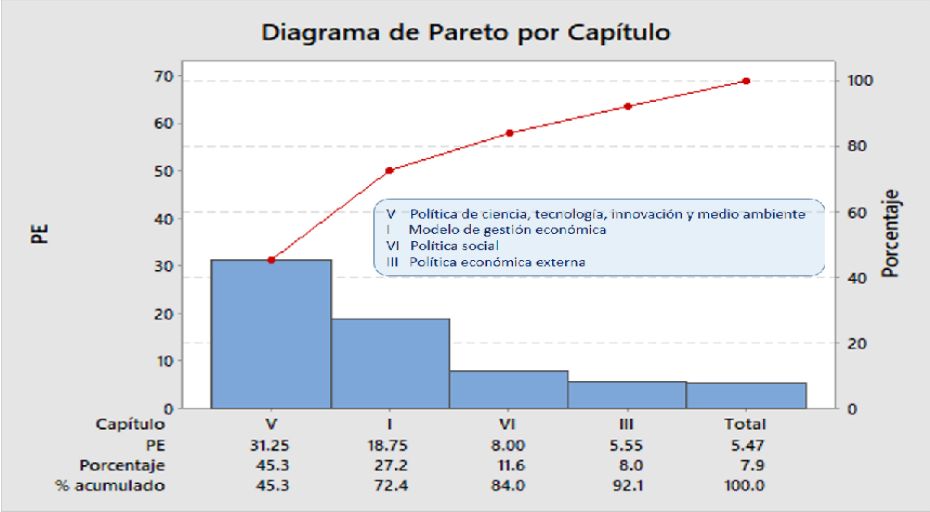
Para la realización de esta investigación se emplearon herramientas de evaluación de gestión integrada y del enfoque de procesos,[18,19] métodos de análisis de razones económico-financieras,[20] matriz DAFO, métodos MICMAC y SMIC de la prospectiva estratégica,[21,22] encuestas y test de innovación a una muestra de 10 directivos de la empresa,[15] diagrama causa-efecto, Pareto y técnicas de estadística descriptiva,[15,23,24] diseño de experimentos[25] y herramientas de software Microsoft Office Excel y Minitab.

Resultados

Diagnóstico integral de DATYS sobre necesidades y oportunidades de mejora del ciclo de vida de desarrollo de software

El ciclo de vida de desarrollo del software con la integración de requisitos de calidad, seguridad, eficacia y eficiencia es un tema que se vincula directamente con cuatro capítulos de los Lineamientos de la Política Económica y Social y en particular con más peso con los capítulos 5 y 2 (ver **Figura 1**). Con los proyectos del Plan Nacional de Desarrollo Económico y Social al 2030 se obtuvo que el mayor vínculo del tema se tiene con los ejes estratégicos del potencial humano, ciencia, tecnología e innovación, así como con la eficiencia y la transformación productiva.

Figura 1. Vínculo con los Lineamientos de la Política Económico y Social



Fuente: Elaboración propia

Las necesidades de adoptar el SSDLC en DATYS se evidencia en la **Tabla 1** con el número de iteraciones que fueron requeridas para la certificación y liberación de tres productos de software de la empresa en el 2022, en función de solucionar los problemas de seguridad detectados.

Tabla 1. Iteraciones para certificación y laboratorio de calidad de DATYS

Producto	Número de iteraciones		Bugs de seguridad		Nuevo desarrollo
	Certificación	Calidad	Certificación	Calidad	
Producto 1	2	3	8	5	Si
Producto 2	4	6	12	2	Si
Producto 3	5	8	16	6	Si

Fuente: Elaboración propia

Se puede apreciar además que, para dar solución a los problemas de seguridad detectados, hubo que realizar nuevos desarrollos, por lo que el número de horas-hombre (en lo adelante HH) planificadas en esos proyectos aumentó, lo que derivó en incumplimiento de planes y de los tiempos de entrega de estos productos al cliente, haciendo ineficiente el proceso de desarrollo de esos productos.

La encuesta de innovación aplicada a 10 directivos de la empresa DATYS permitió conocer que las estrategias genéricas de mayor importancia en este orden son: Liderazgo, Innovación y Calidad, cuyos valores (en un 50%) se encuentran acotados entre 2 y 6 (1 es el más importante); teniendo los dos últimos aspectos un impacto muy importante en el proceso productivo de desarrollo de software.

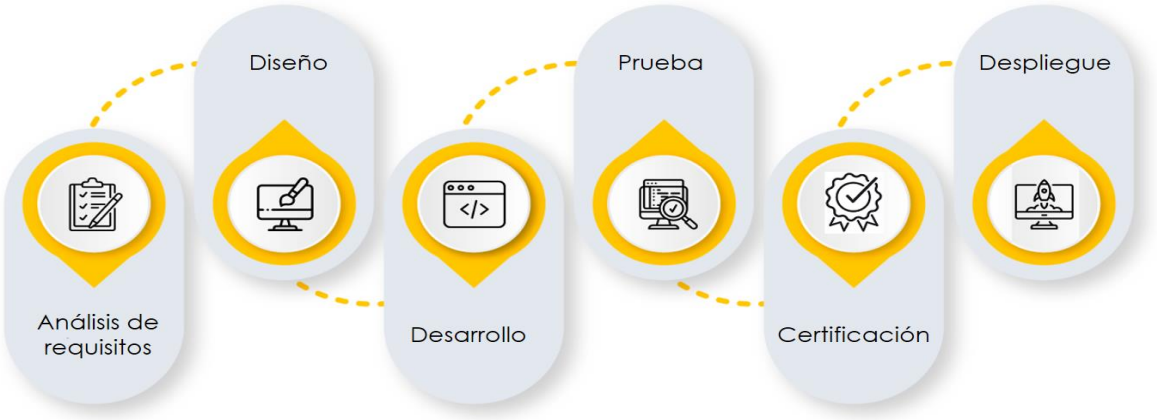
El diagrama causa-efecto o espina de pescado del **Anexo 1** muestra como efecto a analizar la transformación del ciclo de vida de desarrollo de software (SSDLC) en la empresa DATYS. a un ciclo de vida seguro. La proyección de la innovación está en función de lograr mayor eficiencia a partir del ahorro de HH y recursos materiales, así como de proyectar la seguridad de las aplicaciones y sistemas como un proceso transversal, que debe ser tenido en cuenta en todas las fases del ciclo de vida de desarrollo de software. La propuesta innovadora elevaría la calidad del proceso a partir de la implementación y uso de metodologías y estándares internacionales.

Con la aplicación del MICMAC (Matriz de Impactos Cruzados de Multiplicación Aplicada a una Clasificación)[21] se pudo determinar el plano de influencias-dependencias indirectas potenciales y con ello las variables claves del SSDLC referidas al control de calidad, evaluación de dependencias e integración de herramientas de pruebas, cuestiones que se tuvieron en cuenta en la propuesta de innovación.

Identificación en fases del SDLC los aspectos de seguridad a gestionar

El SDLC implementado en la empresa DATYS está conformado por 5 fases[26]: (1) Análisis de requisitos, (2) Diseño, (3) Desarrollo, (4) Pruebas o Control de la Calidad, y (5) Implantación o Despliegue, siendo la seguridad considerada únicamente en la fase de Prueba o Control de la Calidad. La propuesta de SSDLC para la empresa DATYS quedaría conformado por 6 fases (**Figura 2**), las que fueron convenientemente asociadas -relación 1 a 1- con las 6 causas identificadas en el diagrama causa-efecto, elaborado para dar respuesta al problema planteado.

Figura 2. Propuesta de SSDLC a implementar en DATYS.



Fuente: Elaboración propia

Los aspectos de seguridad que deberán ser integrados y gestionados en cada una de las fases del SSDLC, logrando que la seguridad sea gestionada de manera transversal en todo el ciclo de vida de desarrollo del software de la organización se presentan en la **Tabla 2**.

Tabla 2. Aspectos de seguridad a gestionar por fases del SSDLC.

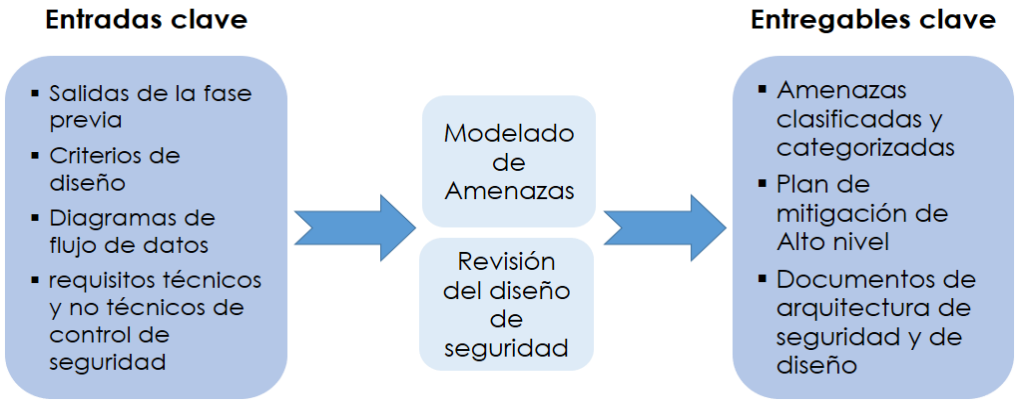
Fase del SSLDC	Aspectos de seguridad
Análisis de requisitos	▪ Identificación de riesgos ▪ Requisitos de seguridad ▪ Requisitos y políticas normativas ▪ Modelado de amenazas ▪ Privacidad y protección de datos ▪ Seguridad en las interfaces y comunicaciones
Diseño	▪ Arquitectura de seguridad ▪ Gestión de configuraciones seguras ▪ Documentación y formación

Desarrollo	▪ Pruebas de seguridad ▪ Uso de bibliotecas y *frameworks* seguros ▪ Gestión de errores y excepciones ▪ Buenas prácticas en el desarrollo de código ▪ Capacitación y concienciación
Prueba	▪ Análisis estático y dinámico de código ▪ Pruebas de transferencia segura de datos
Certificación	▪ Requisitos y políticas normativas
Despliegue	▪ Configuración adecuada ▪ Control de acceso ▪ Monitorización y auditorías ▪ Actualizaciones y parches ▪ Implementación de medidas de mitigación ▪ Registro de auditoría ▪ Detección de actividades sospechosas ▪ Análisis de logs ▪ Gestión de incidentes

Fuente: Elaboración propia

Para cada fase detallaron los subprocesos con sus entradas y salidas, lo que se muestra a modo de ejemplo para el diseño en la **Figura 3**.

Figura 3. Subproceso: Fase Diseño

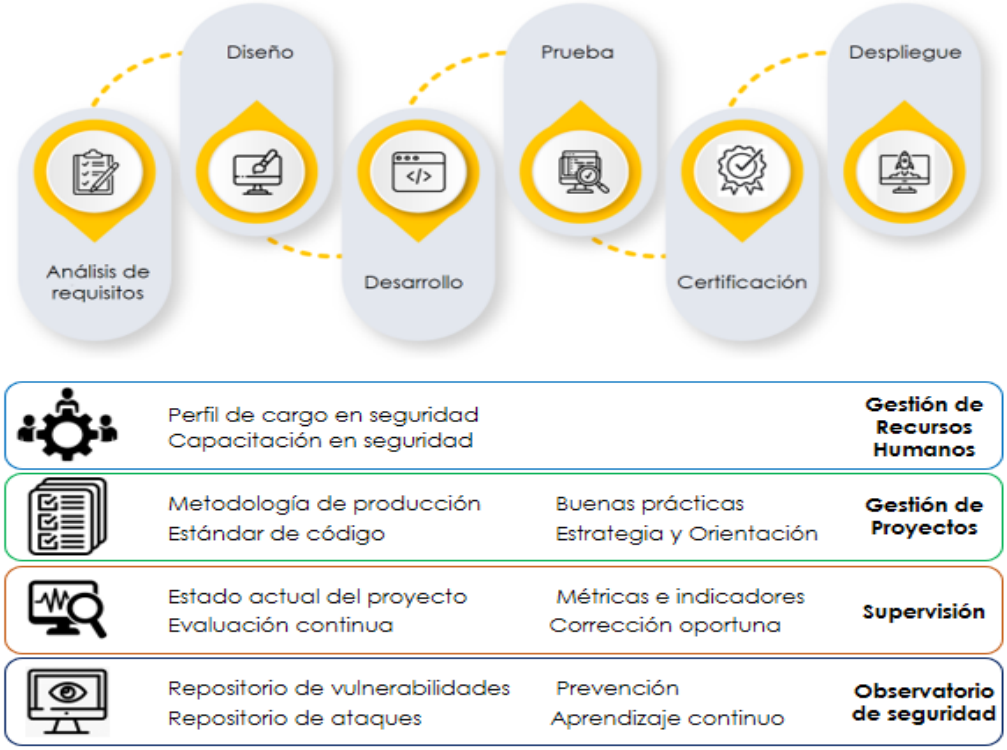


Fuente: elaboración propia

La **Figura 4** muestra una vista integral de la innovación propuesta para dar solución al problema planteado, siendo complementada con un conjunto de elementos sin los cuales no se concretaría el concepto de modelo de innovación integrado. Estos elementos están relacionados con:

- la gestión de los recursos y el talento humano,
- la actualización de los manuales de procedimiento y reglamentos del proceso productivo para lograr un proceso planificado, organizado, controlado y que mejora a partir de su propia gestión,
- la observancia continua de la evolución de la amenazas y riesgos de seguridad,
- la supervisión continua de la evolución del proyecto.

Figura 4. Vista integral de la propuesta de innovación.



Fuente: Elaboración propia

Se determinó que el índice de mérito global del proyecto[15] tiene un valor de 0.85, por lo que las propuestas de innovación son factibles de asumir y se considera que tienen elevadas probabilidades de éxito. También se tuvo en cuenta que el SSDLC ha evolucionado[26-28] para adaptarse a los cambios en las amenazas y tecnologías de seguridad.

Discusión

La preparación y capacitación de los recursos humanos es clave para adoptar de manera efectiva un SSDLC en una organización. Capacitar al personal en las mejores prácticas de seguridad durante el desarrollo de software es fundamental para: garantizar que se sigan estándares y protocolos de seguridad reconocidos; identificar y prevenir brechas de seguridad potenciales; comprender y cumplir con las regulaciones y requisitos de seguridad; ahorro de costos a largo plazo; mejora de la calidad del software y toma de medidas proactivas y preventivas. Un personal preparado en materias de seguridad facilita el desarrollo de un software más robusto y seguro, lo que a su vez mejora la satisfacción del usuario y la reputación de la organización.

Otro aspecto que debe ser analizado por la dirección de la organización y por la de recursos humanos es la pertinencia -a partir de las facultades otorgadas al sector empresarial- de crear un nuevo cargo de perfil estrictamente especializado en la seguridad del software y de su proceso de desarrollo. Algunos ejemplos de cargos profesionales especializados en seguridad del desarrollo de software son: arquitecto de seguridad de software, ingeniero de seguridad de aplicaciones, consultor de seguridad de software, analista de seguridad de código y gerente de seguridad de desarrollo.

Es importante destacar que implementar un SSDLC no es un proceso único, sino que requiere un enfoque transversal, multidisciplinario hacia la mejora continua. Contar con un observatorio de seguridad y con un repositorio actualizado de vulnerabilidades y ataques, proporciona una visión integral de los riesgos de seguridad para una organización que implementa un SSDLC, lo que le permite tomar medidas proactivas para proteger sus activos digitales y mantener la confianza de los clientes, así como un aprendizaje continuo en materias de seguridad.

Proyección y validación del SSDLC en DATYS

Una organización debe evaluar y adaptar su metodología y reglamentos a medida que evoluciona el entorno de amenazas y los requisitos de seguridad cambian. Por consiguiente, la supervisión y evaluación continuas del estado de los proyectos de desarrollo de software, así como la actualización de las métricas y los indicadores de evaluación y control juegan un rol importante en la efectividad de la implementación y evolución del SSDLC.

Para evaluar o medir la efectividad de la integración de la seguridad en cada una de las fases del SSDLC se deben emplear métricas de seguridad, claras y medibles, que evalúen el cumplimiento de los controles de seguridad, la detección y corrección de vulnerabilidades, y el impacto de las amenazas en el software.

Las innovaciones propuestas deben impactar en la mejora de los indicadores de evaluación del proceso de desarrollo de software que actualmente se utilizan en la organización: 1) HHEP por proyecto (eficiencia), referida a las (HH extra plan) y 2) Índice de bugs / Iteración (calidad). Se espera que sus valores disminuyan en función de que se deba emplear un número menor de HH fuera de plan para resolver bugs o mitigar vulnerabilidades de seguridad que se resolvieron durante las etapas iniciales del SDDLC (actualmente son identificados en la etapa de Prueba) y, evidentemente, que su número también disminuya en las iteraciones realizadas por el departamento de calidad de DATYS para la liberación del software.

Se diseñaron dos experimentos para los que fueron seleccionadas como variables respuestas: HHEP e Índice Bugs / Iteración (IBUGS). Se recopilaron los datos relevantes en un periodo de 6 meses (en la primera iteración de la fase Prueba para el caso IBUGS) según las métricas definidas, y se analizaron los resultados de la aplicación del método de Análisis de Varianza (ANVA) para determinar si los cambios propuestos a introducir en la organización tienen un impacto en los indicadores seleccionados. Para procesar los datos se empleó el software Minitab. Ambos experimentos se realizaron para un mismo proyecto de desarrollo de software y se realizaron 3 iteraciones con un total de 6 programadores para lograr mayor variabilidad en los datos.

Para el Experimento 1 se seleccionaron 3 factores: evaluación de dependencias (ED), identificación de requisitos de cumplimiento normativo (RN) y el nivel de preparación y experiencia del equipo de desarrollo (NP); y para el Experimento 2 se seleccionaron 2 factores: implementación de pruebas unitarias en fase Desarrollo del SLDC y el nivel de preparación y experiencia del equipo de desarrollo. Los factores seleccionados se corresponden con subcausas que impactan actualmente en la eficiencia del proceso de desarrollo de software de la organización.

El resultado más importante de ambos experimentos fue la coincidencia en la importancia significativa y determinante de la preparación y capacitación de los programadores en materias de seguridad para

disminuir el número de HHEP y la implementación de las pruebas unitarias en la fase Desarrollo del SLDC, requeridas para mitigar o solucionar riesgos y vulnerabilidades de seguridad no tenidas en cuenta en las fases iniciales del SDLC y en la disminución del índice de bugs de seguridad por iteraciones (Ver **Tabla 3**).

Tabla 3. Resumen de los dos diseños de experimentos 1 y 2

Factor	Nivel (-1)	Nivel (+1)	Decisión
Diseño de experimento 1			
ED	No se realiza evaluación	Si se realiza evaluación	Factores significativos (valor $P<0,05$): RN, NP, RN*NP y ED*RN*NP. La decisión se toma por la interacción ED*RN*NP
RN	No se identifican los requisitos normativos	Si se identifican los requisitos normativos	
NP	Programadores sin conocimientos de seguridad	Programadores con conocimientos de seguridad	
Diseño de experimento 2			
TP	No se implementan pruebas unitarias	Si se implementan pruebas unitarias	Factores significativos (Valor P<0,05): TP y RN. La decisión se toma por los factores TP y RN
RN	Programadores sin conocimientos de seguridad	Programadores con conocimientos de seguridad	

Fuente: Elaboración propia

Como contribución de este trabajo, se presentan otras métricas, que podrán ser utilizadas para medir la efectividad de la seguridad en el SSDLC en la empresa:

- Número de vulnerabilidades identificadas.
- % de vulnerabilidades corregidas en desarrollo.
- Tiempo promedio de resolución de vulnerabilidades.
- Nivel de cumplimiento de estándares de seguridad.
- Impacto de las amenazas detectadas.

Estas métricas deberán ser recopiladas y analizadas a lo largo del ciclo de vida de desarrollo de software para evaluar cuantitativamente la efectividad de la seguridad y tomar acciones correctivas o mejorar las prácticas de seguridad si fuese necesario. El Instituto Nacional de Estándares y Tecnología de los Estados Unidos plantea que con el enfoque SSDLC se logra alrededor de un 30% de reducción de los costos de solucionar defectos y vulnerabilidades al ejecutarse en las fases tempranas del ciclo,[14] lo que también constituye una métrica a tener en cuenta. La efectividad de la propuesta de innovación dependerá de factores como la madurez de los procesos de desarrollo, la capacitación del personal, la implementación de mejores prácticas de seguridad, la cultura organizacional en torno a la seguridad, la infraestructura, la colaboración internacional, la adquisición de recursos materiales, entre otros.

Las etapas establecidas para generar la innovación siguen el ciclo de Deming (Planificar, Hacer, Verificar, Actuar) promueve la mejora continua en cualquier proceso y garantiza que el ciclo de vida de desarrollo seguro de software se mantenga actualizado y adaptado a los cambios en las amenazas y vulnerabilidades de seguridad. También se diseñó el plan de medidas de la gestión de riesgos. La **Figura 5** muestra el Diagrama de actividades. Con el software Project se identifican más de 100 actividades con una duración de 297 días en las que se incluyen los aspectos de seguridad que deberán ser integrados y gestionados por los equipos de proyecto en cada una de las fases del SSDLC, con el objetivo de gestionar la seguridad de manera trasversal durante todo el ciclo de vida de desarrollo del software, como aspecto clave de trasformación hacia un proceso de desarrollo seguro.

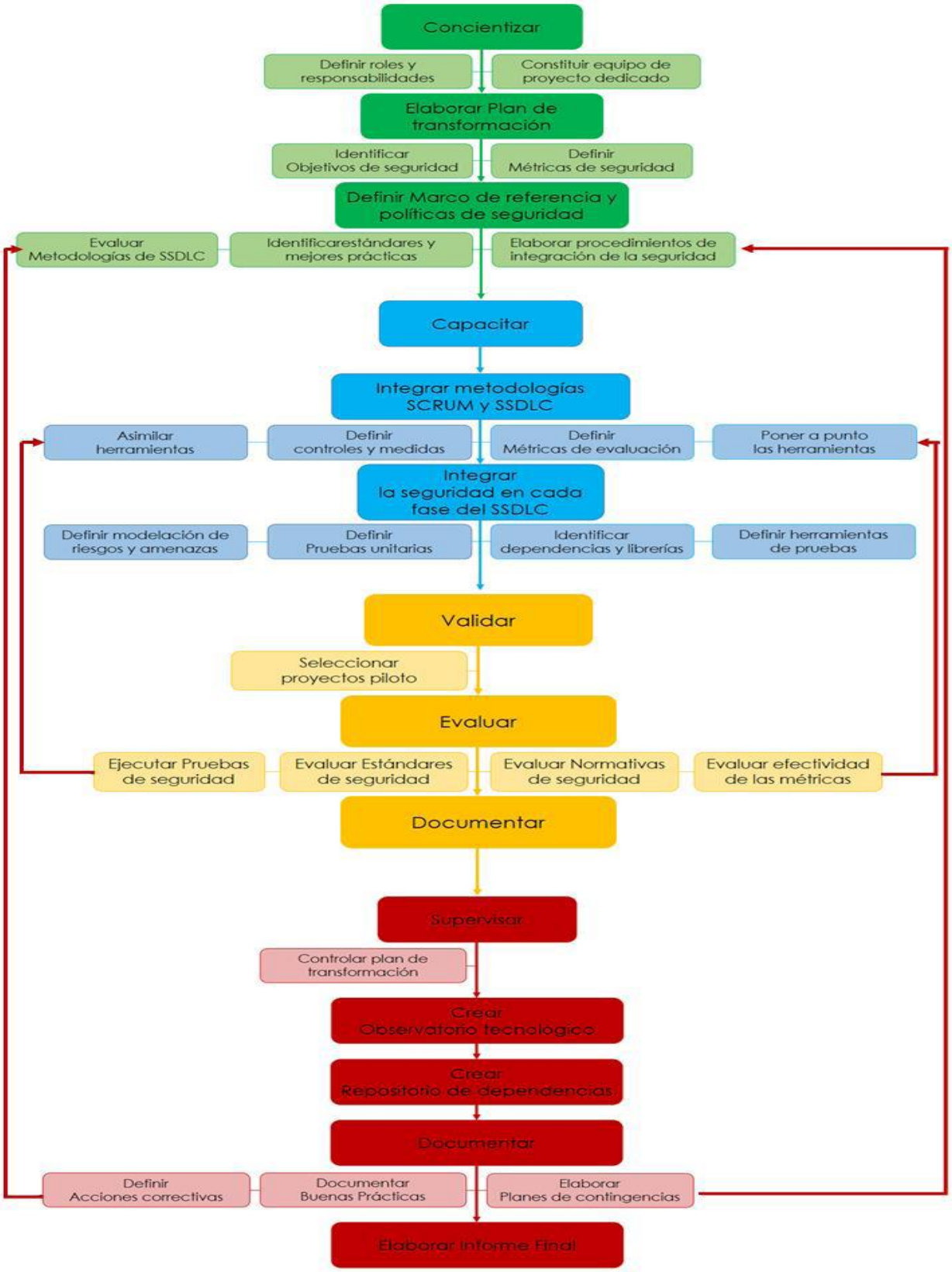


Figura 5. Diagrama de actividades
Fuente: Elaboración propia

Conclusiones

La seguridad del software, la eficiencia y seguridad del proceso productivo de desarrollo de software son elementos clave y prioritario para la empresa DATYS, y responden -fundamentalmente- a las necesidades del Ministerio del Interior como su principal cliente.

Las causas identificadas, que impactan en la seguridad y eficiencia del proceso de desarrollo de software en la organización objeto de estudio, pueden ser abordadas y solucionadas, siguiendo un enfoque sistémico e innovador, el que provee el SSDLC.

El análisis de varios documentos rectores de la política económica, social y de informatización de Cuba, permitió ilustrar que existe total concordancia y vinculación entre las estrategias nacionales y la propuesta de innovación organizacional y de proceso de DATYS, que pretende elevar la eficiencia y la seguridad del proceso de desarrollo de software, a partir de la integración de los aspectos de seguridad en cada una de las fases del SDLC, transformándolo en un SSDLC.

Las actividades de concientización de los directivos sobre la necesidad de adoptar en la empresa un SSDLC evidencian el marcado interés de la dirección de la empresa DATYS por mejorar y perfeccionar los procesos clave de la organización a partir de la aplicación práctica de la ciencia, la tecnología y muy en particular de la innovación, dedicándose recursos humanos, financieros y materiales y métricas efectivas para la evaluación de la eficiencia y calidad del desarrollo del software.

La investigación demuestra que implementar en la empresa DATYS un SSDLC implicaría no solo mayor seguridad y calidad en el proceso de desarrollo de software, sino también mayor eficiencia por la disminución de las horas extra plan y los costos de tiempo de trabajo, para lo cual el plan de actividades elaborado con el ciclo Deming cuenta con más de 100 actividades a ser ejecutadas en 297 días.

Referencias bibliográficas

1. Laato S, Mäntymäki M, Islam AKN. et al. Trends and Trajectories in the Software Industry: implications for the future of work. Inf Syst Front 2023;25:929–944. [consultado 12 diciembre 2023]. Disponible en: https://doi.org/10.1007/s10796-022-10267-4
2. Vinodh S, Antony J, Agrawal R, Douglas JA. Integration of continuous improvement strategies with Industry 4.0: a systematic review and agenda for further research, The TQM Journal, 2021; 33 (2): 441-472. [consultado 11 diciembre 2023]. Disponible en: https://doi.org/10.1108/TQM-07-2020-0157
3. Gurcan F, Ayaz A, Menekse Dalveren GG, Derawi M. Business Intelligence Strategies, Best Practices, and Latest Trends: Analysis of Scientometric Data from 2003 to 2023 Using Machine Learning. Sustainability. 2023; 15: 9854. [consultado 12 diciembre 2023]. Disponible en: https://doi.org/10.3390/su15139854
4. Orges LJ, Anh HZ, Exploring the intersection between software industry and Software Engineering education - A systematic mapping of Software Engineering Trends, Journal of Systems and Software, 2021;172:110736. [consultado 13 diciembre 2023]. Disponible en: https://doi.org/10.1016/j.jss.2020.110736.
5. Greenup ID. Bases para fortalecer las exportaciones de software y servicios informáticos del país. Revista Cubana De Administración Pública Y Empresarial, 2019;3(2): 177–198. [consultado 13 diciembre 2023]. Disponible en: https://apye.esceg.cu/index.php/apye/article/view/82

6. Misra S, Kumar V, Kumar U, Fantazy K, Akhter M. Agile software development practices: evolution, principles, and criticisms. International Journal of Quality & Reliability Management, 2012; 29 (9):972-980. [consultado 12 diciembre 2023]. Disponible en: https://doi.org/10.1108/02656711211272863
7. Partido Comunista de Cuba. Lineamientos de la Política Económica y Social del Partido y la Revolución para el período 2016-2021. La Habana, julio; 2017, 23-32. [consultado 14 diciembre 2023]. Disponible en: http://media.cubadebate.cu/wp-content/uploads/2017/07/PDF-321.pdf
8. Partido Comunista de Cuba. Conceptualización del modelo económico y social cubano de desarrollo socialista. Lineamientos de la política económica y social del Partido y la Revolución para el período 2021-2026. VIII Congreso. Partido Comunista de Cuba (PCC). La Habana, Abril; 2021. p. 86. [Consultado 15 diciembre 2023] Disponible en: https://www.pcc.cu/sites/default/files/pdf/congresos/tesis-resoluciones/2023-05/conceptualizacion-del-modelo-economico-y-social-cubano-de-desarrollo-socialista-y-lineamientos-de-la-politica-economica-y-social-del-partido-y-la-revo.pdf
9. McShane M, Nguyen T. Time-varying effects of cyberattacks on firm value. Geneva Pap Risk Insur Issues Pract 2020;45:580–615. [Consultado 18 diciembre 2023] Disponible en: https://doi.org/10.1057/s41288-020-00170-x
10. Pérez-Morón, J. Eleven years of cyberattacks on Chinese supply chains in an era of cyber warfare, a review and future research agenda, Journal of Asia Business Studies, 2022; 16 (2):371-395. [Consultado 19 diciembre 2023] Disponible en: https://doi.org/10.1108/JABS-11-2020-0444
11. Boehm BW. A Spiral Model of Software Development and Enhancement. ACM SIGSOFT Software Engineering Notes, 1988;11(4): 14-24. [Consultado 19 diciembre 2023] Disponible en: https://doi.org/10.1145/12944.12948
12. Hwang JJ, Ho JH. A comparative study on software development life cycle models in common use. International Journal of Software Engineering & Applications. 2013;4(1):25-35. [Consultado 19 diciembre 2023] Disponible en: https://www.irjet.net/archives/V5/i2/IRJET-V5I2154.pdf
13. Gurung G, Shah R, Prasad D. Software Development Life Cycle Models - A Comparative Study. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 2020;6(4):30-37. [Consultado 20 diciembre 2023] Disponible en: https://doi.org/10.32628/CSEIT206410
14. NIST: National Institute of Standards and Technology, Security considerations in the System Development Life Cycle, NIST Special Publication 800-64 Revision 2; 2019. https://csrc.nist.gov/pubs/sp/800/64/r2/final
15. Delgado M. Innovación Empresarial. En: Delgado M, Coordinador académico. Temas de Gestión Empresarial. Vol. II. La Habana: Editorial Universitaria Félix Varela; 2017, p. 117. [Citado 2 diciembre 2023]. Disponible en: http://bibliografia.eduniv.cu:8083/read/14/pdf
16. Delgado M, Lage A, Ojito E, Espinosa MM, Arias MÁ. Visión de la innovación en un centro cubano de la biotecnología aplicada a la salud. Revista Cubana de Salud Pública [Internet]. 2020;46(1). [consultado 23 diciembre 2023] Disponible en: https://revsaludpublica.sld.cu/index.php/spu/article/view/1941/1526
17. Díaz-Canel M. Sistema de gestión del gobierno basado en ciencia e innovación para el desarrollo sostenible en Cuba. Tesis doctoral en Ciencias Técnicas. Ingeniería Industrial. Universidad Central "Marta Abreu" de las Villas. La Habana, marzo, 2021.
18. Michelena ES, Isaac CL, Delgado M, González A, Díaz S. Gestión integrada calidad y medioambiente. En: Delgado M (Coordinador académico). Temas de Gestión Empresarial. Volumen I. La Habana: Editorial Universitaria Félix Varela.; 2017. p. 81. [consultado 11 noviembre 2023] Disponible en: http://bibliografia.eduniv.cu/read/16/pdf

19. Antúnez V, Fernández MV, Delgado M. Calidad, medio ambiente, seguridad y salud, y control interno en el contexto económico actual: diagnóstico de un laboratorio farmacéutico cubano. COFIN Habana. 2017; 11 (1). [consultado 11 noviembre 2023] Disponible en: https://revistas.uh.cu/cofinhab/article/view/1065
20. Campos L. Análisis económico financiero. En: Delgado M. Coordinador académico. Temas de Gestión Empresarial. La Habana: Editorial Universitaria Félix Varela; 2017. pp. 1-23. [consultado 12 noviembre 2023] Disponible en: http://bibliografia.eduniv.cu/read/18/pdf
21. Garrigó LM. Prospectiva estratégica. En: Delgado M, Coordinador académico. Temas de Gestión Empresarial. Vol. I. La Habana: Editorial Universitaria Félix Varela; 2017, pp. 157-195. [consultado 1 diciembre 2023] Disponible en: http://bibliografia.eduniv.cu:8083/read/19/pdf
22. Garrigó LM, Delgado M. Un enfoque prospectivo en torno al desarrollo de la Escuela Superior de Cuadros del Estado y del Gobierno hacia el año 2021. Revista Cubana de Administración Pública y Empresarial, 2017;1(1):17–29. [consultado 2 diciembre 2023] Disponible en: https://apye.esceg.cu/index.php/apye/article/view/3
23. Delgado M. Modelos de gestión de la innovación: conceptos, enfoques, normas y tendencias. Ingeniería Industrial, 2024;45(1): 1–10. [consultado 12 abril 2024] Disponible en: https://rii.cujae.edu.cu/index.php/revistaind/article/view/1258
24. Delgado M. Aprendizajes de la gestión de I+D+I biofarmacéutica cubana: caso de empresa de alta tecnología. Revista Universidad y Sociedad, 2022;14(5):133-141. [consultado 10 enero 2023] Disponible en: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202022000500133&lng=es&tlng=es.
25. Delgado M. Uso del diseño de experimentos para la innovación empresarial. Revista de Métodos Cuantitativos para la Economía y la Empresa. 2020;29:38–56. [consultado 12 enero 2024] Disponible en: https://doi.org/10.46661/revmetodoscuanteconempresa.2450
26. Gonchar L. Implementation of Secure Software Development Lifecycle in a Large Software Development Organization. 21st International Scientific Workshop on Computer Science and Information Technologies (CSIT 2019). Atlantis Highlights in Computer Sciences. december; 2019. [consultado 15 enero 2024] Disponible en: https://doi.org/10.2991/csit-19.2019.23
27. Gu Q, Lu Y. Software security assurance based on SSDLC and risk assessment. Proceedings of the International Conference on Software Engineering and Knowledge Engineering, 2018; pp. 307-312. [consultado 21 enero 2024] Disponible en: https://doi.org/10.18293/SEKE2018-220
28. Saidani, N, Cherif, W. A systematic literature review on the integration of security into software development life cycle. Journal of Software Engineering and Applications, 2020;13(1): 1-15. [consultado 15 enero 2023] Disponible en: https://doi.org/10.4236/jsea.2020.131001

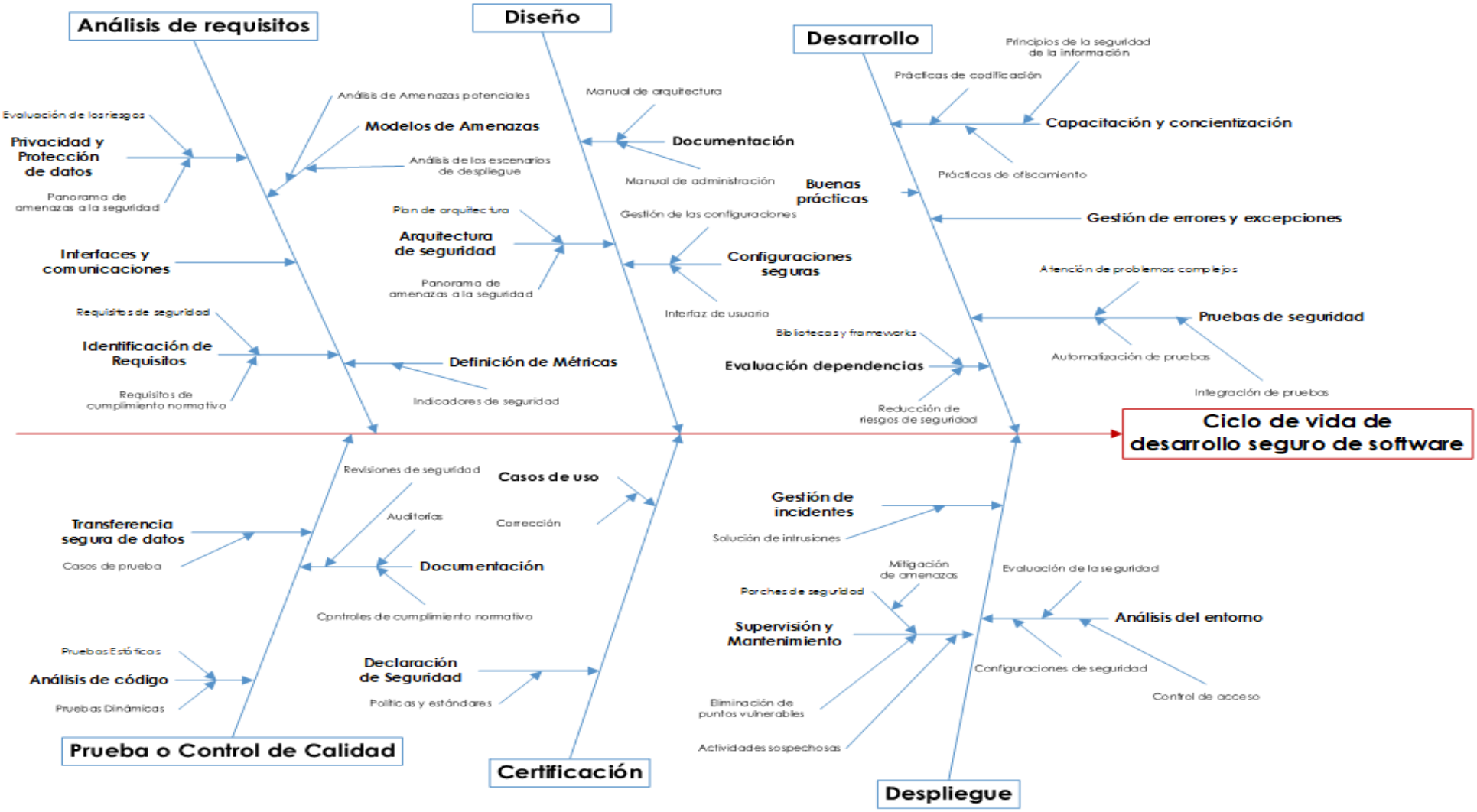
Conflictos de intereses:
Los autores refieren no presentar conflictos de intereses.

Contribución de los autores:

- Sacha Pelaiz Barranco: Conceptualización, Análisis Formal, Investigación, Metodología, Validación, Escritura, Borrador Original.
- Mercedes Delgado Fernández: Conceptualización, Metodología, Supervisión, Validación, Escritura, Redacción: revisión y edición.

Revista Cubana de Administración Pública y Empresarial
ISSN 2664-0856 RNPS 2458 / Vol. 8 Núm. 2 / Mayo-Agosto (2024) / e306
Disponible en: https://apye.esceg.cu/index.php/apye/article/view/306

Anexo 1. Diagrama causa efecto del ciclo de vida de desarrollo seguro de software



Fuente: Elaboración propia