UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
POSGRADO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

Modelo de Procesos para la Mitigación de Amenazas y Vulnerabilidades de la Seguridad Informática en el Desarrollo de Software

T E S I S

QUE PARA OPTAR POR EL GRADO DE
MAESTRO EN CIENCIA E INGENIERÍA DE LA COMPUTACIÓN

PRESENTA:
FRANCISCO ARELLANO MÉNDEZ

TUTORA:
M. EN C. MARÍA GUADALUPE ELENA IBARGÜENGOITIA GONZÁLEZ, FACULTAD DE CIENCIAS

CDMX, SEPTIEMBRE 2017

RESUMEN

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. Observándose 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 ya hoy en día reciben de los sistemas de información debido a que toda su información pasa a estar mecanizada, permitiendo mejorar su explotación, pero al mismo tiempo se hace dependiente del buen hacer de los sistemas y al estar teniendo un gran volumen de información procesándose diariamente por los diversos sistemas a lo largo del mundo, los vuelve fundamentales para el accionar de las organizaciones y a la par se vuelven universales en principio porque más personas tienen acceso a la tecnología y adicionalmente por la interconectividad entre los diversos sistemas.

Estos aspectos refuerzan la capacidad respecto a lo que los sistemas puedan hacer para un trabajo colaborativo; pero al mismo tiempo potencian lo que se puede hacer desde el punto de vista destructivo. Antiguamente los sistemas eran muy suyos y se requería una formación especializada, así como acceder físicamente al entorno de los equipos para poder acceder a la información. Hoy en día todos los sistemas son ampliamente conocidos, las comunicaciones están a la orden del día y el acceso físico es solo una forma adicional de llegar a los equipos. Lo que antes era fácil de proteger de unos cuantos ataques, ahora hay que protegerlo de infinitas vías de ataques y una ingente cantidad de posibles actores, inocentes o malintencionados. (Piattini Velthuis & Hervada Vidal, 2007)

Un aspecto clave es que la seguridad de los sistemas a lo largo de estos años ha pasado de ser un suplemento a ser una necesidad crítica que se debe de gobernar ya que de no hacerlo las actividades estratégicas que administran vía el sistema pueden llegar a convertirse en un dolor de cabeza y la causante de diversas repercusiones para la organización.

Para completar esta visión hay que reconocer que hacemos cosas extremadamente complejas y que actualmente es imposible que alguien logre controlar todos y cada uno de los mecanismos que entran en la más íntima transacción: las aplicaciones, sistema operativo, código máquina, comunicaciones, emanaciones electromagnéticas, instalaciones físicas y el eslabón más débil de la cadena que es el componente humano. Los sistemas simplemente, no se pueden gestionar a base del detalle: es necesario gestionar su globalidad.(Piattini Velthuis & Hervada Vidal, 2007)

Es así, que la seguridad dentro de los procesos de la Ingeniería de Software, han tomado relevancia por parte de los directivos no solo de las organizaciones que los producen sino también de aquellas que hacen uso de ellos. Esto debido a los impactos monetarios, pérdida de reputación y otros aspectos que se ven inmiscuidos tal como lo reporta Trustwave en su último informe (Trustwave Holdings Inc., 2017). La prensa a nivel mundial, especializada o no en el contexto tecnológico nos ha acostumbrado últimamente a las noticias de fallos de seguridad de los sistemas de información con los que solemos trabajar u de ocio.

Estos “fallos”, ahora noticia cotidiana, se producen por aplicar un enfoque distinto al de la seguridad en el desarrollo de estos sistemas. Normalmente durante las etapas de requerimientos y diseño únicamente se tienen en consideraciones aspectos como el menor consumo de memoria, el tiempo de respuesta a peticiones y de puesta en marcha, pero prácticamente a no ser que esté regulado nunca se considera un enfoque de seguridad.

Así mismo, proliferan las publicaciones donde se habla de las “vulnerabilidades” de protocolos concretos, servicios o aplicaciones, sin darnos cuenta de que quizás ese protocolo date de los años 60 o bien la aplicación en cuestión no sea sino una nueva interfaz de usuario sobre una antigua implementación inclusive dándose el caso que se reutilicen componentes de esos sistemas antiguos, los cuales contienen esos defectos. Como ejemplo está el protocolo SMTP (Simple Mail Transfer Protocol) que data de finales de los años 80 y se utiliza en los modernos clientes de correo electrónico o las mismas distribuciones del sistema operativo de Microsoft.

Durante el diseño de servicios y aplicaciones (Garfinkel, Spafford, Daltabuit Godas, Gonzalez Velazquez, & Mallen Fullerton, 1999) es muy común que, el equipo de desarrollo sea sometido a las presiones de los plazos de entrega y a los ajustes al presupuesto establecido, la seguridad no sea tenida en cuenta “al tratarse de un elemento adicional”, de forma que normalmente sus esfuerzos se concentran en factores como la correcta funcionalidad, máxima velocidad de ejecución, menor consumo de memoria entre muchas otras. En este nivel es donde se podrían centrar los servicios de seguridad que permitan asegurar la confidencialidad e integridad de la información que se transmite a través de las aplicaciones y en la identidad de los usuarios que acceden, entre otros.

Por tal motivo, el objetivo de la presente investigación es adicionar aspectos de seguridad a los procesos de la Ingeniería de Software, que 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 un estándar aprobado por las organizaciones encargadas de desarrollar Sistemas de Información (SI).

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

TABLA DE ACRÓNIMOS

Siglas	Significado
CC	Common Criteria
CIA	Confidentiality, integrity y availability
CISQ	Consortium for IT Software Quality
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
OMG	Object Management Group
PDCA	Plan-Do-Check-Act
SDL	Security Development Lifecycle
SGSI	Sistema de Gestión de la Seguridad de la Información
SAMM	Software Assurance Maturity Model
SDLC	Systems Development Life Cycle
TI	Tecnología de la información
BSIMM	The Building Security in Maturity Model
OWASP	The Open Web Application Security Project
SI	Sistema de Información

INTRODUCCIÓN

PLANTEAMIENTO DEL PROBLEMA

El desarrollo de software de cualquier índole por parte de organizaciones se realiza 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 (Trustwave Holdings Inc., 2017) ocasionando que la información contenida en las aplicaciones quede a expensas de cualquier atacante.

HIPÓTESIS

La hipótesis de esta tesis es la siguiente:

Implementar un modelo de procesos que incluya a la seguridad informática desde las primeras fases del ciclo de vida del desarrollo del software, permitirá la reducción de fallos informáticos logrando un software con mejores niveles de seguridad.

OBJETIVOS

El objetivo de este trabajo es desarrollar y presentar un modelo del proceso de desarrollo de software que permita la reducción de estados con anomalías que afecten las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas a realizar; proporcionando una guía sobre cómo planificar, gestionar y ejecutar los procesos de desarrollo; proporcionando valor agregado a los productos desarrollados a través de medidas proactivas en las fases iniciales del ciclo de vida del desarrollo.

En este trabajo de investigación se persiguen los siguientes objetivos específicos:

- Desarrollar una base de conocimientos para la inclusión de procesos de seguridad en el desarrollo de software, permitiendo tener un software más estable y, por tanto, reduciendo el número de vulnerabilidades del software.
- Proporcionar un valor agregado al software creado a través de la implementación proactiva de calidad a los procesos.
- Proporcionar una guía y dirección sobre la implementación de la seguridad en los procesos de desarrollo de software.

Contribuir a reducir la vulnerabilidad del software que producen las PYMEs, desarrollando una guía que direccione y estandarice la implementación de seguridad en los procesos de desarrollo del software.

Ello bajo el precepto de que no hay un software totalmente infalible, ni totalmente perfecto.

QUÉ SE QUIERE LOGRAR / ALCANCES DE LA INVESTIGACIÓN

- Brindar una guía que permita incorporar la seguridad en proyectos de desarrollo de software a través de la mitigación de los principales riesgos existentes en esa área.

- Que el software creado tenga las medidas mínimas proactivas contra ataques informáticos con la finalidad de prevenir:
    - El mal uso del sistema por parte de terceros
        - La fuga de información sensible desde las aplicaciones creadas.
            - Credenciales de acceso
            - Documentos confidenciales
        - No se manipule información por personas indebidas al proceso
    - Que el sistema se caiga y por ende no brinde el servicio
- Generar software con calidad que esté a la altura de los retos que existen en la actualidad.
    - Evitando que se genere software con baja calidad en seguridad.

Estructura del Documento

La obra se divide en dos secciones principales: Conceptos Teóricos, y Essence Sec. La primera parte (Conceptos teóricos), incluye los conceptos, definiciones y teoría sobre las diversas propuestas que actualmente se utilizan en la industria. Se compone de 4 capítulos:

- El Capítulo I. Antecedentes de Seguridad, presenta una serie de temas de seguridad para conocer los aspectos esenciales de la Seguridad de la información.
- El Capítulo II. Terminología de Seguridad, en ella se presenta una serie de términos que serán utilizados durante toda la investigación con la finalidad que el lector pueda comprender el contexto.
- El Capítulo III. Modelos y Normas de Seguridad, resume los trabajos afines a esta tesis que fueron estudiados con el propósito de obtener el estado del arte de la misma, entre los cuales están: SAMM, BSIMM, Microsoft SDL, CISQ, Common Criteria y Métrica 3; así mismo incluye el marco teórico sobre los riesgos conducentes en los sistemas de información.
- El Capítulo IV. La Esencia en el desarrollo de software seguro,
- El Capítulo V. Armonización de Estándares y Modelos, presenta la investigación de las diversas propuestas de los marcos y estándares utilizados para la integración de la seguridad en la Ingeniería de Software, así como la propuesta para la unificación de ellas.

La segunda parte (Essence Sec), incluye los pasos que se siguieron para la obtención de la inclusión de seguridad en la Esencia, comenzando con la armonización de los marcos y estándares para su posterior adición con la Esencia, una vez con Essence Sec se puede presentar sus características principales. Se compone de 4 capítulos:

- El Capítulo VI Métrica 3 como base para implementación de Essence Sec, proporciona la integración de los aspectos de seguridad identificados e unificados en el capítulo IV con la Esencia teniendo como resultado Essence Sec.

- El Capítulo VII. Essence Sec, en este capítulo se presenta la propuesta de la incorporación de la Seguridad a la Esencia.
- El Capítulo VIII. Alfa: Requisitos, se presenta la inclusión de seguridad al Alfa de Requisitos.
- El Capítulo IX. Alfa: Sistema de Software, se presenta la inclusión de seguridad al Alfa de Sistema de Software.
- El Capítulo X. Alfa: Trabajo, se presenta la inclusión de seguridad al Alfa de Trabajo.
- El Capítulo XI. Alfa: Forma de Trabajo, se presenta la inclusión de seguridad al Alfa de Forma de Trabajo.
- Capítulo XII. Caso Práctico que permitirá validar la propuesta de investigación.
- En el Capítulo XIII, incluye las conclusiones obtenidas al finalizar la investigación.

Finalmente, se presenta las referencias bibliográficas utilizadas durante la tesis y los anexos que servirán de apoyo para el uso de la Essence Sec.

PRIMERA PARTE. CONCEPTOS TEÓRICOS DE SEGURIDAD

CAPÍTULO I. ANTECEDENTES DE SEGURIDAD

La Seguridad de la Información, según ISO 27001 (ISO/IEC JTC1 /SC27, 2005), se refiere a la Confidencialidad, la Integridad y la Disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, pudiendo ser electrónicos o de papel.

Consistiendo en asegurar que los recursos del Sistema de Información se utilicen de la forma que han sido concebidos y el acceso de información se encuentra contenida, así como controlar que la modificación sólo sea posible por parte de las personas autorizadas para tal fin todo ello realizado dentro de los límites de la autorización establecidos.

I.1 LA SEGURIDAD

La seguridad de la información desde sus inicios, siempre fue concebida como un atributo deseable a implementar dentro del software y forma parte del conjunto de atributos a considerar para determinar la calidad del mismo observándose en la ISO/IEC 25000 (ISO/IEC_JTC1/SC27, 2005). Dado que en la actualidad existe un aumento en los ataques a aplicaciones web vulnerables ha traído consigo un reconocimiento gradual por parte de la comunidad de especialistas, empresas e industria del software que las protecciones a nivel de infraestructura (hardware) no son suficientes para garantizar un comportamiento seguro de las mismas. Por tal motivo, en la actualidad los expertos reconocen que las protecciones y mitigaciones de seguridad de las aplicaciones se deben especificar desde el inicio de la construcción del software, ello tanto durante su proceso de desarrollo, y su despliegue y operación (Castellaro et al., 2009).

Todo lo anterior da como resultado que la seguridad sea considerada por las organizaciones como un factor crítico a considerar a la hora de crear o hacer uso de las tecnologías de la información (TI) dentro de sus procesos internos y externos ya que las repercusiones de no hacerlo podrían llegar a ser incosteables. Lamentablemente, en la actualidad generalmente las organizaciones abordan la seguridad dentro de los proyectos de TI de forma fragmentada y sin seguir un proceso lo que ocasiona estancos en distintas áreas y momentos del proceso de desarrollo e implementación del proyecto e inclusive lamentablemente se dan el caso que se realice de manera posterior a su implementación lo que ocasiona re trabajo y altos costos (Castellaro et al., 2009).

Todo ello ocasionado por la falta de una visión integral y transversal generando situaciones que implican mayores costos (muchos de ellos innecesarios), mayor trabajo, re-trabajo, rechazos de los participantes y, en muchos casos, hasta se incorporan nuevas vulnerabilidades a las ya contenidas por el sistema.

En virtud de lo cual, es necesario plantear los objetivos de seguridad en el contexto de una estrategia de la seguridad, que esté directamente ligada a los objetivos de la organización y alineados a casos de negocio, considerándose desde el inicio de los proyectos de SI, y que además evolucionen de la manera más efectiva y eficiente posible acompañando el crecimiento de la empresa.

Adicionalmente se pueden identificar tres sub características que tiene la seguridad:

- Riesgo de daño económico (Economic damage risk): Grado de impacto previsto de dañar a la propiedad comercial, a las operaciones o la reputación en determinados contextos de uso. Esto podría incluir los costes administrativos de corregir errores de producción, de la incapacidad de proporcionar un servicio aceptable, o de la pérdida de ventas actuales o futuras.
- Salud y seguridad en uso (Health and safety): Grado de impacto previsto de dañar a las personas en determinados contextos de uso.
- Riesgo de daño al entorno (Environmental harm risk): Grado de impacto previsto de dañar la propiedad o al entorno en determinados contextos de uso.

Por lo que es importante considerar no solo por el valor de calidad que adiciona al proyecto si no por todas las cuestiones que se pueden involucrar a su entorno.

I.2 EVOLUCIÓN HISTÓRICA DE LA SEGURIDAD

Desde el principio de la informática, todos los sistemas han estado expuestos a la existencia de “vulnerabilidades”. Durante los primeros años, para atacar un sistema se necesitaba poca sofisticación técnica, prácticamente provenían del interior o bien, en caso de realizarse desde el exterior, únicamente era necesario conocer una contraseña válida. Con el paso del tiempo, se han ido desarrollando formas en demasía complicadas de descubrir y explotar las vulnerabilidades (Fernández-Medina, Moya, & Piattini, 2003).

Después aparecieron los intentos de explotar las vulnerabilidades de los protocolos, programas y redes, realizando ataques contra la lógica que contienen. Estos han dado en llamarse la segunda generación: “ataques sintácticos” (Schneier, 2004).

Actualmente con el boom de Internet, cualquier vulnerabilidad puede ser descubierta, difundida y explotada en muy poco tiempo. Una vez difundida aparece un nuevo riesgo; los “aprendices”, el aprendiz de atacante únicamente tiene que descargar una herramienta de Internet y ejecutarla, sin tener en cuenta el daño que puede llegar a realizar en su “víctima”, estos llamados *script-kiddie* (Fernández-Medina Patón et al., 2003).

Aunque exista trabajo realizado por organizaciones alrededor del mundo como OWASP, NIST, Microsoft relativo a la difusión y educación en seguridad en el desarrollo de software, el último informe de Trustwave (Trustwave, 2016) relativo a la evolución de la seguridad en el software desarrollado pone de manifiesto que las vulnerabilidades y el número de ataques sigue en aumento, teniendo cifras alarmantes para la industria como

son:

- El 80% de las vulnerabilidades afectan tecnologías Web.
- Entre el 90% y 97% de las aplicaciones son vulnerables.
    - Contienen un promedio de 14 vulnerabilidades
- Al menos el 80% de las aplicaciones sufren vulnerabilidades graves.
- El 75% de los ataques se producen a través de sitios Web.
- Crisis económica
    - Se reduce la inversión en seguridad a nivel de aplicación
    - Aunque curiosamente se sigue invirtiendo en seguridad a nivel de red.

Este hecho pone sobre la mesa que hay algo que no se está haciendo bien ya que, en vez de que cada año se reduzcan las cifras, éstas aumentan considerablemente. Esto se puede deber a que o bien no se entienden las amenazas que se tienen; o se asumen de forma consciente o inconscientemente estos riesgos, ello debido quizás al desconocimiento de la dimensión real del problema ya que existen percepciones erróneas de que la seguridad es costosa por parte de la alta dirección. Lo que ocasiona que las empresas que cumplen o hacen uso de medidas de seguridad en el desarrollo, realizan esta actividad principalmente por cumplir las normativas que las rigen en su área, como son los servicios financieros, la salud y el gobierno. Ello ocasiona que no se realice con la convicción de que es necesario realizarlo ocasionando que no forme parte de los procesos de las empresas.

Y en la actualidad, la información y los sistemas que la soportan, constituyen recursos valiosos para la organización o incluso a manera personal. Su dependencia de la información se pone de manifiesto cuando se presenta alguna amenaza contra el flujo normal de los datos. La seguridad de la información también es imprescindible para mantener valores esenciales en el sector público, en el sector privado o bien en ambos. Se trata en suma de poder depositar una confianza razonable en la capacidad de esa información para sostener el funcionamiento adecuado de las funcionalidades y valores de cada organización (Fernández-Medina Patón et al., 2003).

Los sistemas de información están amenazados por agresores malintencionados o no, más o menos sofisticados y están en constante actualización, que interaccionan con los sistemas de información para obtener información, reducir o anular alguna de sus funcionalidades. Pero no debe haber una resignación fatalista, porque hay soluciones, cuyo coste depende ampliamente de su implementación inteligente y temprana. La seguridad siempre es barata a largo plazo.

El ahorro y la eficacia son mucho mayores si los requerimientos y especificaciones de seguridad se incorporan en fases tempranas del ciclo de vida del desarrollo de la aplicación. Cuanto más temprano se actué para dar seguridad a los sistemas, más sencilla y económica resultará a la organización.

De ahí que las estrategias de seguridad que se implementan en el Ciclo de Vida de Desarrollo Seguro de Software (SDLC) deben incluir entre otras actividades, la educación y concientización de todos los involucrados en el proceso desde el desarrollador hasta la alta

gerencia, ya que sin éstos últimos sería imposible su implementación, dado que son los responsables de la disposición de medios, guías de ayuda y seguimiento de su cumplimiento en toda la empresa.

I.3 EL PAPEL DE LA ADMINISTRACIÓN EN EL DESARROLLO DE SISTEMAS DE INFORMACIÓN

En la actualidad las administraciones de todo tipo de empresas sean públicas o privadas hacen un uso intensivo y dependiente de sistemas informáticos para automatizar un sin fin de tareas ya sean de baja o alta complejidad, pero todas ellas forman parte esencial del trabajo del día a día de la empresa y sin ellas se verían fuertemente afectadas sus actividades o incluso puede significar el paro total de sus actividades.

Esto se da a consecuencia de que la creación de nuevos sistemas de información ha sido impulsora de innovaciones o de la extensión de la capacidad de invenciones preexistentes; por ejemplo, la interoperabilidad de las aplicaciones; la utilización de la firma electrónica; la creación de modelos de procesamiento de datos, como ligados a la población o a las estadísticas, por citar algunos (Fernández-Medina Patón et al., 2003).

Todo esto en su conjunto reclama una cultura de la seguridad, en la que tienen responsabilidad todos los participantes desde el gobierno hasta el usuario final que hace uso del sistema. Es por ello que desde la administración es necesario la difusión general de las directrices, estableciendo o modificando las políticas, prácticas u procedimientos para que se encuentren alineados a las directrices de seguridad necesarias para preservar la información contenida.

I.4 CARACTERÍSTICAS DE SEGURIDAD

Citando a Fred Brooks (1986) refiriéndose a la Ingeniería de Software, “No parece existir la ‘bala de plata’ que resuelva los problemas esenciales de la seguridad de las tecnologías de la información, que logre de manera rápida y eficaz la confianza universal. Ciertamente la seguridad no puede sustraerse a las limitaciones de la creación de los sistemas informáticos”.

De acuerdo con la Real Academia Española, algo seguro, se define como “libre o exento de riesgo, que brinda seguridad, certeza y confianza” (Real Academia Española, 2017). Sin embargo, se trata de una condición ideal, ya que en la realidad no es posible tener la certeza de que se pueden evitar todos los riesgos asociados al proyecto. Por tanto, su propósito es el reducir los riesgos hasta un nivel aceptable para los interesados.

No en vano, la inteligencia aplicada a sacar provecho de las vulnerabilidades de la tecnología, a impedir su funcionamiento o a engañar a los participantes, ofrece, en la actualidad, un campo aparentemente inagotable (Fernández-Medina Patón et al., 2003).

Los usuarios buscan confiar en los sistemas que utilizan (Piattini Velthuis & Hervada Vidal, 2007). La confianza es la ausencia de sorpresas y la certeza, razonable, de que se alcanzarán los objetivos deseados. La confianza puede tener infinitos orígenes; pero no hay confianza que dure si no hay seguridad. Y la seguridad nos concreta algunas características esenciales de los sistemas de información:

I.4.1 CONFIDENCIALIDAD

Es que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

I.4.2 INTEGRIDAD

Es el mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una organización.

I.4.3 DISPONIBILIDAD

Es la disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción en el servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

Estas características de seguridad las requerimos según el valor que represente para el sistema en cuestión y coloquialmente se representan con las siglas CIA. Si el secreto de la información es muy importante solo se confiará en un sistema que nos asegure un alto nivel de confidencialidad. Si la interrupción del servicio fuera muy grave, solo se confiará en un sistema que nos asegure un alto nivel de disponibilidad, etc.(Piattini & Hervada, 2007)

I.4.4 AUTENTICIDAD (NO REPUDIO)

Es que no haya duda de quien se hace responsable de una información o prestación de un servicio, teniendo como finalidad el poder confiar en quien realiza la acción, así como de poder perseguir posteriormente los incumplimientos o errores. Contra la autenticidad se dan suplantaciones y engaños que buscan realizar un fraude. La autenticidad es la base para poder luchar contra el repudio y, como tal, fundamenta el comercio electrónico o la administración electrónica, permitiendo confiar sin papeles ni presencia física.

I.5 SITUACIÓN DE LA CALIDAD DE LOS SISTEMAS DE INFORMACIÓN

La calidad de los productos no es un proceso separado que deba esperar al final del desarrollo del proyecto para su aseguramiento o implementación, ya que se trata de un proceso que debe de realizarse de forma continua desde el inicio del proyecto teniendo como meta el diseñar, planificar e implementar el proyecto de forma efectiva y eficiente de acuerdo a los objetivos del proyecto. Por tanto, es un proceso vital que permite asegurar que los proyectos cumplan con los requisitos de calidad esperados.

CAPÍTULO II. TERMINOLOGÍA DE SEGURIDAD

En la siguiente sección de la investigación se define una serie de términos bajo el contexto de seguridad de la información, permitiendo tener una correcta interpretación de esta investigación

II.1 ACTIVOS

De acuerdo a la ISO 27001 los activos son cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

El entorno del Sistema de Seguridad de la Información basado en ISO 27001, que comprende:

1. Los activos y que se precisan para garantizar los siguientes niveles.
2. El sistema de información en sí.
3. La misma información generada por la aplicación del Sistema de Seguridad de la Información.
4. Las funcionalidades de la organización, en las que se justifican las exigencias de los Sistemas de Información anteriores y les generan la finalidad deseada.
5. Otros activos, ya que el tratamiento realizado a los activos es un método de evaluación de riesgos que tienen que permitir la inclusión de cualquier otro activo, sea cual sea su naturaleza.

Los fallos que se producen en los activos del entorno son:

- Provocar fallos en los Sistemas de Información
- Provocar fallos en la información
- Condicionantes de otros activos

II.2 AMENAZAS

Las amenazas son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas materiales en sus activos. (ISO/IEC_JTC1/SC27, 2016)

La definición anterior recoge la esencia dinámica de la amenaza: es un potencial evento una acción, una interrupción o una falta de acción fuera del control de los actores de la seguridad, distintas de las acciones de tipo decisión humana.

La definición de amenaza sobreentiende que hay diversidad de consecuencias, lo que habrá de tenerse en cuenta al examinar la entidad impacto.

La consecuencia de la amenaza, si llegara a materializarse, es un incidente que modificaría el estado de seguridad de los activos amenazados, haciéndolo pasar de un estado anterior al evento a otro posterior, potencial o realmente.

II.2.1 TIPOS DE AMENAZAS

Las diversas causas de las amenazas permiten clasificarlas según su naturaleza lo que orienta sobre las medidas a tomar para neutralizarlas. MAGERIT (Consejo Superior de Administración Electrónica, 2012) considera cuatro tipos de causas amenazadoras:

1. No Humanas (Accidentes)
2. Humanas Involuntarias (Errores)
3. Humanas Intencionales
4. Humanas Intencionales de origen remoto

Grupo 1 “No Humanas (Accidentes)”:

- Accidente físico de origen industrial: Incendio, explosión, inundación por roturas etc.
- Avería: de origen físico o lógico, debido a un defecto de origen o sobrevenida durante el funcionamiento del sistema.
- Accidente físico de origen natural: sismo, tormenta eléctrica, derrumbe, etc.
- Interrupción de servicios o de suministros esenciales: energía eléctrica, telecomunicaciones, etc.

Grupo 2 “Humanas Involuntarias (Errores)”

- Errores de utilización ocurridos durante la recogida y transmisión de datos o en su explotación por el sistema.
- Errores de diseño existentes desde los procesos de desarrollo del software como lo pueden ser de dimensionamiento, por la posible saturación etc.
- Errores de ruta, secuencia o entrega de la información en tránsito.

Grupo 3 “Humanas Intencionales”

- Acceso lógico con intercepción pasiva simple de la información. (Requiere solo lectura)
- Acceso lógico con alteración o sustracción de la información en tránsito (Requiere lectura y escritura); o sea reducción de la confidencialidad para aprovechar programas o datos.
- Acceso lógico con alteración o sustracción de la información en tránsito (requiere lectura y escritura); o sea, reducción de la integridad y/o disponibilidad del sistema sin provecho directo (sabotaje, infección vírica…).

Grupo 4 “Humanas Intencionales de origen remoto”

- Acceso lógico con intercepción pasiva (para análisis de tráfico…)
- Acceso lógico con corrupción (O destrucción) de información en tránsito o de configuración.

- Acceso lógico con modificación (inserción, repetición) de información en tránsito.
- Suplantación de origen (del emisor o reemisor) o de identidad.
- Repudio del origen o de la recepción información de tránsito.

II.2.2 MODELADO DE AMENAZAS

El Modelado de Amenazas es una técnica de ingeniería cuyo objetivo es ayudar a identificar y planificar adecuadamente la mejor forma de mitigar las amenazas de un sistema informático. Permitiendo comprender el perfil de amenazas a las que está expuesto un sistema. Con técnicas tales como la identificación de puntos de entrada, fronteras de privilegios y árboles de amenazas, se pueden identificar estrategias para mitigar las posibles amenazas del sistema.

Este también permitirá la justificación de la implementación de las características de seguridad dentro de su sistema, o las prácticas de seguridad para utilizarlo, para la protección de los activos de la organización. Su implementación en un escenario ideal debería iniciarse desde las primeras etapas del desarrollo y planificación de sistema con la finalidad de aprovechar mejor los beneficios que proporciona su uso.

En este sentido, y de forma reciente, Microsoft ha sido uno de los grandes impulsores de esta técnica, así mismo existen otras alternativas en desarrollo. A continuación se expondrán dos de las principales propuestas en este tema.

II.2.2.1 EL MODELADO DE AMENAZAS ("THREAT MODELING"' - TM)

(Castellaro, Romaniz, Ramos, Feck, & Gaspoz, 2016)

La tarea de identificar los riesgos y las amenazas en el software requiere un esquema estructurado y repetible, que mejore el entendimiento de los involucrados en el desarrollo, ayude a identificar problemas de diseño e integración de componentes, y sirva como input para el equipo de pruebas. El TM constituye un marco de trabajo específico para el proceso de análisis de riesgo estructurado, que permite identificar las amenazas de una aplicación y cuantificar los riesgos a los que la misma estará expuesta.

El proceso de TM consta de las siguientes etapas:

(1) conformar un grupo de análisis de riesgo;
(2) descomponer la aplicación e identificar componentes claves;
(3) determinar las amenazas a cada componente de la aplicación;
(4) asignar un valor a cada amenaza;
(5) decidir cómo responder a las amenazas;
(6) identificar las técnicas y tecnologías necesarias para mitigar los riesgos identificados.

Si bien este proceso constituye un esquema estructurado, se reconoce que el TM se presenta como un conjunto complejo y multidimensional de compensaciones que podrían ser hechas para encontrar un juego de objetivos implícitos o explícitos.

Desde distintas dimensiones se pueden observar diferentes enfoques o empleos para la obtención de las amenazas:

- Respecto al término 'amenaza': se utiliza tanto para referirse a los posibles "ataques" intencionales, como al "riesgo" que se corre cuando alguien se equivoca.
- Respecto a las acciones: mediante el modelado de amenazas se puede referir a una técnica para obtener requerimientos (qué amenazas se van a modelar) o a técnicas de análisis y diseño (cómo se analizan y reflejan esas amenazas en el modelo)
- Respecto al foco: el modelado puede ser 'centrado en el activo' (implica algún nivel de evaluación de riesgo, aproximación o clasificación), 'centrado en el atacante' (implica la clasificación de riesgo o intenta estimar recursos, capacidades o motivaciones, y conlleva a determinar escenarios de amenazas) o 'centrado en el software' (análisis de software, redes de organización o sistemas y conlleva al modelado de protocolos y de amenazas de red).
- Respecto a los recursos humanos: el modelado de amenaza puede ser hecho por expertos de seguridad, en colaboración de ingenieros con expertos, o por ingenieros sin expertos disponibles.

Para finalizar se puede concluir que el modelado de amenaza TM abarca una amplia variedad de actividades en la definición de requerimientos de seguridad y análisis de diseños de seguridad. Teniendo siempre en consideración que no hay un único modo 'mejor' o 'correcto' de modelado de amenaza.

II.2.2.2 MICROSOFT, "THREAT ANALYSIS AND MODELING"

(Microsoft, 2013)

Esta metodología de Microsoft dispone de 5 pasos, los cuales se presentan a continuación:

1. Identificar los objetivos de seguridad.
    a. Se determinan los objetivos que ayudan a cuantificar el esfuerzo necesario para llevar a cabo lo siguiente.
2. Crear una descripción general de la aplicación.
    a. Se identifican los actores involucrados y características importantes de la aplicación. Esta tarea facilita la identificación de amenazas.
3. Descomponer la aplicación.
    a. A partir de la arquitectura general se identifican los componentes que la forman. Se deben analizar de manera independiente y sobretodo sus interacciones.
4. Identificar amenazas.
    a. Con toda la información se identifican las amenazas más importantes, deben estar priorizadas anteriormente.
5. Identificar vulnerabilidades.
    a. Se revisan las diferentes capas de la aplicación y se identifican los puntos débiles de ésta.

A través de los flujos de datos se comprende la lógica de la aplicación y se conoce cómo puede afectar al tratamiento de los datos a la integridad de los activos. Se tiene claro que para conocer las amenazas se debe conocer los puntos de entrada a la aplicación, niveles de confianza y activos.

Por otro lado, los árboles de ataques permiten identificar amenazas y analizar cuáles son las formas de mitigación. ¿Cómo funciona? En el nodo principal o raíz del árbol se sitúa un objetivo del atacante. Los hijos representan los caminos que tiene el atacante para conseguir dicho objetivo. Los nodos hijo representan métodos y/o técnicas para conseguir los objetivos.

II.3 VULNERABILIDAD

Una vulnerabilidad es un defecto que afecta a la seguridad de un sistema informático, las vulnerabilidades también son denominadas "agujeros" de seguridad y permiten a los usuarios sin autorización acceder a un sistema informático. Actualmente con la inclusión del Internet de las cosas todas las plataformas, desde un PC, un Smartphone hasta un poderoso mainframe tienen vulnerabilidades unas ya conocidas y otras pendientes de descubrirse, de hecho, como ya se ha comentado no hay nada que sea absolutamente seguro (Piattini Velthuis & Hervada Vidal, 2007).

II.3.1 CARACTERÍSTICAS DE LA VULNERABILIDAD

La vulnerabilidad es una propiedad de la relación entre un activo y una amenaza, aunque suele vincular más al activo como una "no-calidad" de éste. La vulnerabilidad es un concepto con dos aspectos:

- Forma parte del estado (aspecto estático) de seguridad del activo en su función propiedad entre el activo y la amenaza en acción.
- En su aspecto dinámico, es el mecanismo obligado de conversión de la amenaza en una agresión materializada sobre un activo.

II.3.2 CLASIFICACIÓN DE LAS VULNERABILIDADES

Las vulnerabilidades pueden ser clasificadas de múltiples maneras , en este caso se utilizará la clasificación propuesta por Erick Knight (2000) que está referida a dos factores ¿Cuál es el objetivo específico de la vulnerabilidad en términos de la computadora o de la persona? Y la segunda es ¿Con qué rapidez funciona la vulnerabilidad?, dando respuesta a las preguntas se tiene la Tabla II.1.

TABLA II.1 CLASIFICACIÓN DE LAS VULNERABILIDADES POR ERICK KNIGHT (2000).

	Afecta a la persona	Afecta a la Computadora
Instantáneo	Ingeniería Social	Error Lógico
Requiere un periodo de tiempo	Supervisión de políticas	Debilidad

Error Lógico	Es un error de programación que altera la seguridad, el cual generalmente es considerado un bug básico. Estos tipos de problemas se producen debido a una circunstancia especial (Normalmente código mal) que permite un acceso mayor al debido.
Debilidad	Es un defecto en el diseño de la aplicación que puede conducir a una violación de seguridad. Por lo general también involucra cosas de seguridad que pueden ser o no sólidas y por ende se puede llegar el caso de ser vulneradas como lo es el cifrado de la aplicación o de los datos.
Ingeniería Social	Es un área nebulosa de ataque asociado con un ataque dirigido contra las políticas de la organización. Esta va desde un trabajador interno, sabotaje, una estafa telefónica dirigida a un empleado o indagar en información que fue desechada.
Supervisión de Políticas	Es un defecto en la planificación para evitar una situación, que sería por ejemplo el no producir copias de seguridad de manera adecuada, manejo de contraseñas seguras, manejo de escritorio limpio etc. Ella requiere principalmente del involucramiento de la alta gerencia para que pueda realizarse de forma adecuada ya que de lo contrario las contramedidas existentes para la protección son inútiles.

II.3.3 ANÁLISIS DE LAS VULNERABILIDADES

La identificación de las vulnerabilidades debe ser efectuado analizando el contexto en el que se va a desenvolver la aplicación ya que existen factores tanto externos como internos que pueden afectar seriamente el análisis como lo es el entorno en el que se desarrolla la actividad de la organización e inclusive el país y región donde se utilizara dado que pueden existir normativas específicas que puedan afectar su implementación dado que las organizaciones están sujetas a la creatividad de los políticos o reguladores.

Otros factores que hay que considerar son la cultura propia de la organización, El sector de actividad o si la organización pertenece un sector en donde se realiza un uso intensivo de la tecnología o donde la tecnología informática es un factor estratégico como en el sector financiero.

Las vulnerabilidades pueden estar asociadas al aspecto físico, organización, procedimientos, personal, gestión, administración, equipos, software o información.

El hecho que exista una vulnerabilidad no implica que está cauce un daño, pero la amenaza que puede explotarla puede causar daño a activos del sistema de TI o a otros activos de la organización.

Entre las razones de vulnerabilidades en un software pueden citarse:

- La falta de cultura de prevención.
- Falta o nula prevención desde el inicio del proyecto.

- Deficiente o nula realización del análisis de riesgos.
- Falta de capacitación al personal en temas de seguridad.
- Desarrollo inseguro por parte de los programadores
- Falta de planeación para la fase de pruebas y liberación del sistema.

Esta enumeración pone en evidencia que la utilización exclusiva de medios tecnológicos no es suficiente para la protección de los activos de la organización. Es necesaria la aplicación de principios de buena administración y de otras herramientas y recursos para protegerla de los riesgos potenciales a que está expuesta.

Además de identificar las vulnerabilidades, se debe de evaluar con qué facilidad se pueden explotar, esto es analizarlas con respecto a cada amenaza que pueda afectarla. Este proceso, denominado valoración de las vulnerabilidades, dará como resultado una calificación de baja, media o alta posibilidad.

II.4 IMPACTO

Impacto en un activo es la consecuencia sobre éste de la materialización de una amenaza.

El impacto es, de forma dinámica, la diferencia en las estimaciones del Estado de seguridad del activo antes y después de la materialización de la amenaza. O sea, el evento amenaza materializada produce en el estado anterior (a la amenaza) de seguridad del activo un cambio, hacia un nuevo estado posterior (a la amenaza), midiendo el impacto la diferencia entre ambos estados.

II.5 RIESGO

El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, que puede ser positivo o negativo.

En el cálculo del riesgo tiene gran influencia en evaluación del impacto, que es un proceso difícil. El nivel de riesgo depende de la vulnerabilidad y del impacto, pero se da un peso mayor en el proceso de decisión que subyace al cálculo del riesgo: cualquiera prefiere como riesgo menor en la combinación de un impacto –negativo– bajo, aunque la potencialidad sea muy alta (Piattini Velthuis, García Rubio, García Rodríguez de Guzmán, & Pino, 2015).

El riesgo debe ser el mínimo razonable posible y en todo caso no debería ser mayor que el posible beneficio(Piattini Velthuis & Hervada Vidal, 2007). Ante los riesgos posibles no es normal quedarse quieto. Normalmente se toman medidas, desplegando una serie de salvaguardas que cambien el escenario. Las salvaguardas reducen la vulnerabilidad del sistema, bien reduciendo las oportunidades de que la amenaza se materialice, bien limitando el impacto en caso que ocurriera. En ambos enfoques el resultado final es mejorar la posición de riesgo que pasa a un valor reducido o “riesgo residual” (Piattini Velthuis & Hervada Vidal, 2007).

Puesto que las amenazas son a menudo dinámicas, evaluar el riesgo asociado a una amenaza debe ser un proceso continuo. La mitigación eficaz de riesgos de seguridad consiste en seguir un proceso de seguimiento continuo, la evaluación y el ajuste de la mitigación basado en perfiles de riesgo actuales. Idealmente, la frecuencia de la evaluación será mayor que la tasa de cambio de las condiciones que afectan manifiestamente este perfil de riesgo (Young, 2010).

Dada la complejidad y el alcance que puede tener un programa de seguridad aunque sea modesto para el entorno actual, junto con la necesidad de poder contener los costos de producción, es necesario un proceso general de evaluación de riesgos que sea eficaz y eficiente de forma mensurable para la organización. (Young, 2010).

Esto puede lograrse realizando los siguientes pasos:

1. Identificar las amenazas que afectan al proyecto.
2. Especificar los factores que mejoran los componentes individuales del riesgo para cada amenaza.
3. Establecer las medidas de mitigación para abordar los factores de riesgo identificados.
4. Establecer métricas y medir la brecha entre la amenaza y la mitigación para conocer su correlación de costo/beneficio.

En la Figura II.1, muestra un gráfico donde se indica a las amenazas como progenitores del riesgo, los componentes individuales del riesgo y el ciclo continuo de evaluación, mitigación y medición del riesgo.

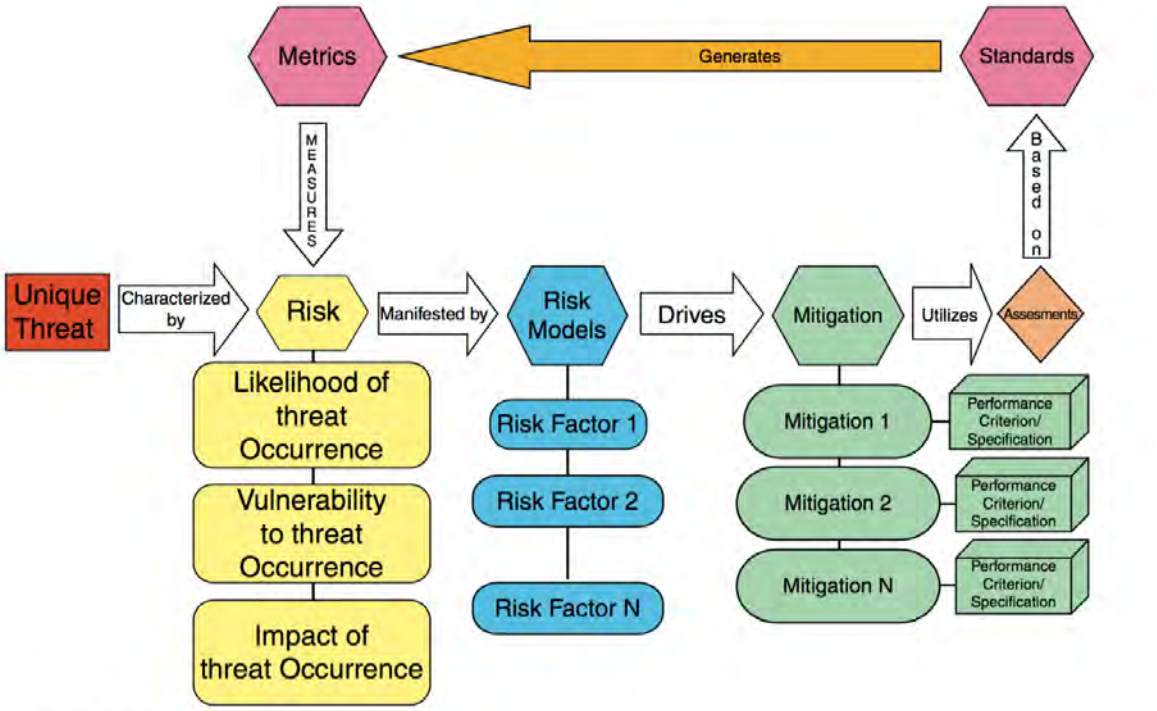


Figura II.1 "EL PROCESO DE EVALUACIÓN DEL RIESGO DE SEGURIDAD" (YOUNG, 2010)

Vale la pena repetir que todas las cuestiones de riesgo de seguridad son derivadas de las amenazas. Por ello es útil volver a los principios cuando se examina cualquier problema de seguridad con la finalidad de comprender a fondo cada amenaza dado que ello incrementa la posibilidad de que la mitigación se realice de forma correcta y eficiente (Young, 2010).

Para poder realizar una evaluación de riesgos apropiada, se requiere una revisión completa de las amenazas desde la perspectiva del "cliente" o de los actores más afectados por los riegos.

El conjunto de amenazas únicas en última instancia impulsa a crear los requisitos para la mitigación del riesgo de seguridad. Donde cada factor de riesgo está asociado a una amenaza única, dando lugar a la aplicación de una salvaguarda determinada para mitigarlo(Young, 2010).

Todos los métodos de mitigación deben en última instancia vincularse a uno o más de un requisito. Además, representan los requisitos más generales para una estrategia de mitigación del riesgo de seguridad. También hay que tener en consideración que el único propósito de la mitigación es minimizar la probabilidad o vulnerabilidad de los componentes del riesgo.

Por lo que como ya se mencionó anteriormente hay que identificar e implementar una serie de métodos de mitigación eficaces para cada amenaza única, teniendo en consideración la priorización de las amenazas de acuerdo a las políticas y necesidades de la organización en cuestión. Requiriendo de un procedimiento en el que se apliquen las medidas de mitigación de manera coherente y consistente en todos los escenarios de amenaza posibles. De ahí la importancia de identificar con precisión y categorizar el conjunto de amenazas al comienzo de cualquier desarrollo (Young, 2010).

Esto permite poner el problema en categorías generales de amenazas e identificar los factores de riesgo para cada categoría. Así, tras el análisis crítico de la amenaza y la clasificación asociada de los factores de riesgo, establecemos un conjunto de medidas de mitigación de alto nivel denominadas “Controles” que son necesarias para abordar cada factor de riesgo. Estos controles pueden incluir algunas funciones generales de seguridad como son el uso de herramientas seguras, protocolos de comunicación validados, administración de la configuración, etc. En este proceso de mitigación, se debe especificar al menos un control para cada factor de riesgo. Los controles no constituyen por sí solos una estrategia, pero representan un importante paso en la dirección correcta (Young, 2010).

Pasando de lo general a lo específico, se debe identificar y utilizar un método o una serie de métodos para implementar cada control.

En resumen, el proceso utilizado para desarrollar una estrategia específica de seguridad es:

1. Identificar el conjunto de amenazas.
2. Determinar los factores de riesgo relevantes que aumentan la probabilidad o vulnerabilidad del riesgo asociado con cada amenaza.
3. Establecer un conjunto completo de controles para abordar cada factor de riesgo.
4. Especificar los métodos necesarios para implementar cada control

5. Asegurarse de que cada método logra los criterios de desempeño requeridos a las especificaciones técnicas que cumplen con los estándares de seguridad acordados.

El proceso de mitigación del riesgo se captura en la Figura II.2

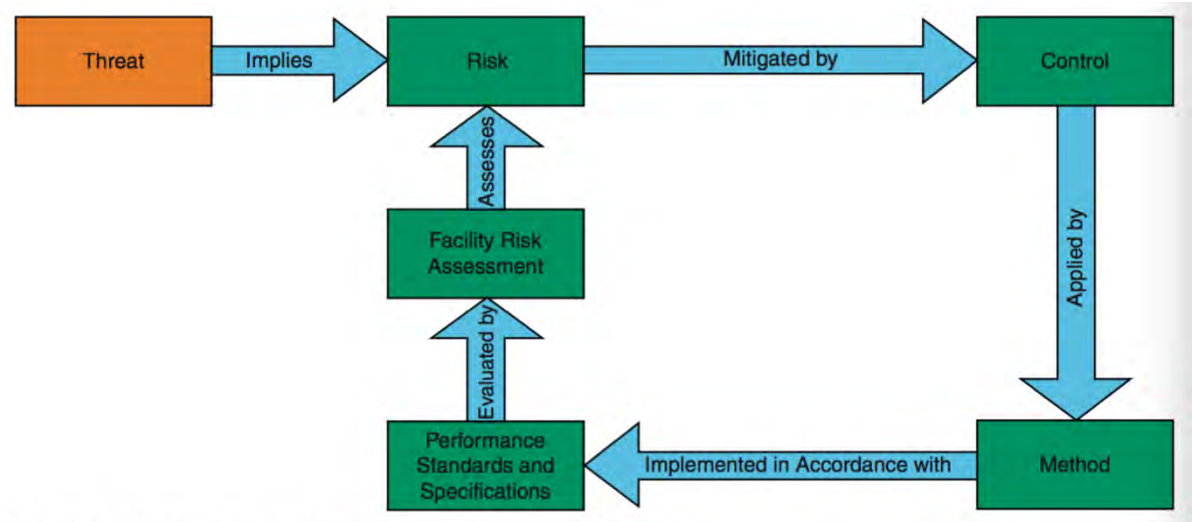


Figura II.2 "EL PROCESO DE MITIGACIÓN DEL RIESGO DE SEGURIDAD" (YOUNG, 2010)

II.5.1 NIVEL DE RIESGO

Es la magnitud de un riesgo expresado en términos de la combinación de sus consecuencias y su probabilidad de que suceda.

II.6 ATAQUE

Es el intentar destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo (ISO/IEC_JTC1/SC27, 2016).

II.7 SALVAGUARDA

Son aquellas políticas, procedimientos, prácticas u estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido (ISO/IEC JTC1 /SC27, 2005).

II.8 SUPERFICIE DE ATAQUE

Es el subconjunto de recursos del sistema que un atacante puede utilizar para atacar un sistema en cuestión. Es así que un atacante puede usar los puntos de entrada del sistema y los puntos de salida, los canales y los elementos de datos no confiables para enviar (recibir) datos al (desde) el sistema para atacar el sistema (Manadhata, 2008).

II.9 ATACANTE

Se puede considerar un atacante a toda aquella persona que atenta de manera no autorizada en contra del sistema, vulnerando alguno de los objetivos de la seguridad identificados.

Dedicándose a quebrantar sistemas para poder acceder a funciones no autorizadas, consiguiendo información restringida (Corrales Hermoso, Beltrán Pardo, & Guzmán Sacristán, 2006).

II.10 CONTROL

Es la medida que está modificando el riesgo, este incluye cualquier proceso, política, equipo, práctica o cualquier otra acción que modifique el nivel de incertidumbre (ISO/IEC_JTC1/SC27, 2016).

II.11 SDLC

El término Ciclo de Vida de Desarrollo Software, en ingles SDLC (Software Development LifeCycle), describe el desarrollo de software desde la fase inicial hasta la fase final. Su propósito no es otro que definir el conjunto de etapas por las que pasa el sistema que se está desarrollando desde que nace la idea hasta que el software es retirado o remplazado.

Las fases por las que transcurre el desarrollo del software son un conjunto de actividades relacionadas con un objetivo en el desarrollo del proyecto. Cada fase se construye agrupando tareas (actividades elementales) que pueden compartir un tramo determinado del tiempo de vida de un proyecto. La agrupación temporal de tareas impone requisitos temporales correspondientes a la asignación de recursos (humanos, financieros o materiales).

El ciclo de vida permite que los errores se detecten lo antes posible y por lo tanto, permite a los desarrolladores concentrarse en la calidad del software, en los plazos de implementación y en los costes que conllevan.

II.11.1 S SDLC (SECURE SOFTWARE DEVELOPMENT LIFE CYCLE)

Es un conjunto de principios de diseño y buenas prácticas a implementar en el desarrollo de un ciclo de vida, para detectar, prevenir y corregir los defectos de seguridad en el desarrollo y adquisición de aplicaciones, de forma que al finalizar se obtenga un software de confianza y robusto frente a ataques maliciosos. De esta manera el software realice solo las funciones para las que fue diseñado, quedando reducido de vulnerabilidades, ya sean intencionalmente diseñadas o accidentalmente insertadas durante su ciclo de vida y se asegure de preservar su integridad, disponibilidad y confidencialidad.

Las actividades que realizan estos SDLC en común son:

- La planeación del proyecto
- El desarrollo de requerimientos de seguridad
- El desarrollo de diseños de sistemas seguros
- La integración de componentes al sistema
- Las pruebas al sistema y demás componentes

Cabe destacar que incluso aun cuando las organizaciones se ajustan a un modelo de procesos en particular, no hay garantía de que el software que crean está libre al 100% de vulnerabilidades de seguridad no intencionales o de código malicioso intencional. Sin embargo, es probable que haya una mayor probabilidad de construir software seguro cuando una organización sigue sólidas prácticas de Ingeniería de Software con énfasis en un buen diseño, prácticas de calidad como inspecciones y revisiones, uso de métodos exhaustivos de prueba, gestión de riesgos, gestión de proyectos y de personas.

CAPÍTULO III. MODELOS Y NORMAS DE SEGURIDAD

III.1 INTRODUCCIÓN

La siguiente acción a realizar para garantizar la seguridad en los sistemas que se desarrollan actualmente se enfocan a la implementación de una gestión continua de la seguridad en los procesos de desarrollo de software, permitiendo la adopción de controles, salvaguardas y técnicas que garanticen aspectos tales como la continuidad de su correcto funcionamiento, la protección de la información que contienen, la conformidad con las normativas a las que se tenga que regir tanto la aplicación como la organización y también el lado contractual que se tenga. En general, a la satisfacción de aquellos requisitos que puedan contribuir al logro de los objetivos de la organización y permitan su desarrollo.

Lo anterior demanda la existencia de un conjunto articulado, sistemático, estructurado, coherente y lo más completo posible de normas que sirvan de vocabulario y lenguaje común, de unificación de criterios, de modelo, especificación y guía para su uso repetido que permitan realizar un desarrollo de software con un buen nivel de calidad de seguridad que permitan satisfacer las necesidades y expectativas por las cuales fue necesaria la creación del software, aportando a la vez racionalización, disminución de costes, mejoras en competitividad y calidad.

En los últimos años, se ha producido un incremento de la atención a la seguridad de los desarrollos de software ello por parte tanto de Organismos de normalización como Organizaciones de la comunidad informática; es así que se ha desarrollado una colección significativa de normas, modelos y manuales de referencia en el campo del desarrollo de software seguro, en la medida en que, junto con el enfoque tradicional de desarrollo se han unificado para poder involucrar valiosas áreas.

Este capítulo, persigue ofrecer un panorama general sobre las normas, modelos y manuales de referencia que permitan realizar un desarrollo de software con medidas de seguridad involucradas, ofreciendo una visión integrada y coherente posible de un escenario que habitualmente se presenta y se percibe como excesivamente fragmentado.

En la siguiente sección se encuentran aquellos marcos y estándares que se consideraron para la realización de la investigación, tomándose en cuenta la trayectoria que han tenido en el área, su implementación por parte de las organizaciones, así como el soporte técnico que brindan para su correcta implementación.

Describiendo su autor, año de creación y el número de la última versión estable disponible para implementarse. Adicionalmente se explica su funcionamiento básico y las consideraciones que se deben de tener en cuenta a la hora de implementarse.

III.2 MODELOS Y NORMAS DE SEGURIDAD APLICADAS A LA INGENIERÍA DE SOFTWARE

III.2.1 ISO 27001

Information technology - Security techniques - Information security management systems – Requirements
(ISO/IEC JTC1 /SC27, 2005)

Autor: ISO/IEC JTC1 /SC27

Año de creación: 2015

Última Versión: 2.0

La primera versión de esta norma se denominaba ISO/IEC 17799 "Tecnología de la Información. Código de Buenas Prácticas de la Gestión de la seguridad de la información" del año 2000, la cual tenía sus fundamentos en la norma inglesa BS 7799-2. Ambas normas tienen un punto de partida común, el ciclo de gestión, que propone el modelo Plan-Do-Check-Act (PDCA).

La utilización desde ese entonces de estas normas ha puesto de manifiesto el comienzo de la preocupación y concientización de las empresas de todos tamaños por proteger su información a través de la buena gestión de la misma, permitiendo garantizar a sus proveedores y clientes su correcta implementación a través del proceso de certificación por un tercero.

Este modelo enmarca las normas aplicables a la gestión de los sistemas de seguridad de la información, teniendo como objetivo:

> "Especificar los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) documentado dentro del contexto global de los riesgos de negocio de la organización. Especificando los requisitos para la implantación de los controles de seguridad hechos a medida de las necesidades de las organizaciones individuales o parte de las mismas"

El "enfoque de proceso" se refiere a la aplicación de un sistema de procesos dentro de una organización, junto con la identificación y la interacción de estos procesos, así como su gestión, adoptando el modelo PDCA, que se aplica para estructurar todos los procesos del SGSI, requiriendo:

1. Entender los requisitos de seguridad de la organización y la necesidad de establecer una política y unos objetivos para la seguridad de la información.
2. Implantar y poner en marcha los controles para gestionar los riesgos de seguridad de la información de la organización en el contexto de los riesgos globales del negocio de la organización.
3. Controlar y revisar el comportamiento y la eficacia de un SGSI.
4. Una mejora continua basada en mediciones objetivas.

Todo ello tiene como finalidad el garantizar que la seguridad de la información es gestionada correctamente, haciendo uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial.

Es así que en la ISO 27001 se enfoca en la creación del Sistema de Gestión de la Seguridad de la Información ya que este permite a la organización conocer los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

El SGI puede ser observado de la siguiente forma:

Donde:

- Manual de seguridad
  - Es el documento que administrar el sistema, donde se indican y determinan las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales.
- Procedimientos
  - Este permite administrar el sistema a nivel operativo, permitiendo que se realice adecuadamente la planificación, operación y control de los procesos de seguridad.
- Instrucciones / Formularios
  - Son todos aquellos documentos que especifican cómo se realizan las tareas y actividades específicas relacionadas con la seguridad.
- Registros
  - Son los documentos que servirán como evidencia del cumplimiento de los requisitos del SGSI.

III.2.2 SAMM

Software Assurance Maturity Model
(The Open Web Application Security Project, 2016)

Autor: OWASP

Año de creación: 2015

Última Versión: 2.0

SAMM es un marco de trabajo de código abierto que ayuda a las empresas a proponer, aplicar y medir una estrategia que incorpore la seguridad en el desarrollo de software, el cual toma como base los riesgos específicos a los que se enfrenta la organización en cuestión. Se construyó sobre una serie de prácticas de seguridad que están ligadas a las funciones de negocio centrales que están involucradas en el desarrollo de software.

Este marco de trabajo apoya el ciclo de vida de software de manera integral, incluyendo el desarrollo y adquisición; ello permite ser una respuesta directa a la aparición incesante de las brechas de seguridad en el software, lo que permite a los atacantes tener acceso a la información privada de los usuarios del software usado.

Su constitución permite que pueda ser utilizado por organizaciones de todos tamaños y con cualquier estilo de desarrollo. Ello se da en primer lugar gracias a que puede ser aplicado en toda la organización o en una sola línea de negocio y en segunda que no está ligado a un tipo de desarrollo en particular lo que permite que se utilice de acuerdo a la metodología seleccionada en la organización.

Algunos puntos clave que cubre el marco de trabajo son:

- Medible: El marco de trabajo proporciona niveles bien definidos y discretos para apoyar el aseguramiento eficaz de las actividades a realizar.
- Riesgo-Conducido: El modelo está construido alrededor de los riesgos de la organización, con la finalidad de optimizar el retorno de la inversión por el gasto realizado.
- Ciclo de vida completo.
- Evaluar las prácticas de seguridad de software existentes en la organización.
- Construir un programa balanceado de aseguramiento de la seguridad definido en iteraciones equilibradas.
- Demostrar las mejoras concretas en el programa realizado
- Definir y medir todas las actividades relacionadas con la seguridad en toda la organización

SAMM consiste en los siguientes componentes:

- Documento del Core del Modelo, en el que se explica el modelo de madurez.

- Guía práctica de orientación para la implementación.
- Guía de inicio rápido de diferentes medidas para mejorar la práctica de desarrollo de software seguro.
- Puntos de referencia de SAMM para realizar la comparación de madurez y observar el progreso en comparación de otras organizaciones u grupos de trabajo similares.

SAMM divide en 4 las diversas actividades que forman el núcleo de cualquier organización que desarrolla software a las cuales les nombra "Funciones de Negocio" las cuales son:

1. Gobierno
2. Construcción
3. Verificación
4. Desarrollo

Por cada una de las funciones de negocio se definen a su vez 3 Prácticas de seguridad, las cuales se encargan de cubrir todas las áreas relevantes para la calidad de la seguridad en el software desarrollado. Estas toman puntos clave de mejora en las 4 diferentes áreas para poder mejorar esos procesos con el fin de evitar los estados viciados que puedan llegar a afectar al software. Adicionalmente se incluyen detalles adicionales para poder medir el desempeño exitoso de estas actividades.

Figura III.1 "ESTRUCTURA DE SAMM" (OWASP, 2009)

Adicionalmente, SAMM fue diseñado para ser flexible, ello con la finalidad de que pueda ser adoptada por cualquier tamaño de organización y fue construido bajo los siguientes principios:

- Cambios paulatinos en la organización.
  - Un programa de seguridad exitoso debe ser implementado en pequeñas iteraciones, lo cual permitirá producir entregables tangibles y de valor para la organización en el corto plazo, los cuales se pueden ir incrementando para el logro de metas a largo plazo.
- No existe una receta única que funcione en todas las organizaciones.

- Un marco de trabajo de seguridad de software debe ser flexible y permitir poner en marcha los controles necesarios basándose en el nivel de riesgo de la organización.

- Establecimiento de una directriz de seguridad.
  - Las actividades de un programa de aseguramiento deben estar bien definidas, ser prácticas y medibles.

III.2.3 BSIMM

The Building Security in Maturity Model
(Arkin et al., 2016)

Autor: Consorcio de 95 empresas mundiales

Año de creación: 2006

Última Versión: 7ª Edición

BSIMM es un modelo que permite medir la seguridad del software, su uso principal se realiza comparando y contrastando la iniciativa de la empresa contra las acciones definidas en BSIMM; ello con la finalidad de identificar las metas y objetivos de la propia iniciativa, permitiendo determinar qué actividades adicionales se pueden incluir en ella para mejorar sus procesos.

En resumen, BSIMM no es una guía de cómo realizar las cosas ni, un modelo a la medida para las empresas, es más un reflejo del estado actual de la seguridad del software.

La validación de los procesos definidos en BSIMM provienen de 95 organizaciones participantes las cuales tienen la representación de diferentes ramos industriales, como son:

- Las empresas de servicios financieros
- Los proveedores de software independientes
- Cloud
- Internet de las cosas (IoT)
- Las compañías de seguros
- Empresas de salud

Las industrias con menor representación en el banco de datos BSIMM incluyen las telecomunicaciones, el comercio minorista y la energía.

BSIMM está organizado en un conjunto de 113 actividades implementadas dentro de un Marco de trabajo el cual está organizado en 4 dominios principales que contienen 12 prácticas, las cuales se describen a continuación:

1. Gobierno
    a. Las prácticas en este dominio ayudan a organizar, administrar y medir la iniciativa de la seguridad del software.
2. Inteligencia
    a. Las prácticas en este dominio constan de colecciones de conocimiento usado para incorporar actividades de seguridad dentro de la organización.
3. SSDL Touchpoints
    a. Las prácticas en este dominio están asociadas al análisis y aseguramiento del software, en lo respectivo a sus procesos y los artefactos creados.

4. Desarrollo
    a. Las prácticas en este dominio están asociadas a la configuración, mantenimiento y otras actividades que impactan al desarrollo de software seguro.

Las doce prácticas que reúnen en conjunto los 4 dominios son:

1. Gobierno
    a. Estrategia y métricas
    b. Cumplimiento y políticas
    c. Capacitación
2. Inteligencia
    a. Modelos de ataque
    b. Características y diseño de la seguridad
    c. Estándares y requerimientos
3. SSDL Touchpoints
    a. Análisis de la arquitectura
    b. Revisión del código
    c. Test de seguridad
4. Desarrollo
    a. Test de penetración
    b. Ambiente de software
    c. Configuración y administración de la vulnerabilidad

III.2.4 MICROSOFT SDL

Microsoft Security Development Lifecycle
(Microsoft, 2009)

Autor: Microsoft

Año de creación: 2004

Última Versión: 5.2

Este es un proceso de control de seguridad orientado al desarrollo de software, forma parte de una iniciativa corporativa y directiva obligatoria desde el 2004 por parte de Microsoft se ha desempeñado como un papel relevante para la integración de la seguridad y de la privacidad en el software y la cultura de la empresa. Tiene como objetivo reducir el número y la gravedad de las vulnerabilidades en el software desarrollado.

SDL se compone de medidas obligatorias que siguen el proceso de desarrollo de software tradicional, pero es lo suficientemente flexible como para permitir la adición de otras políticas y técnicas, creando así una metodología de desarrollo de software que sirva como una guía dentro de la empresa. La combinación de procesos, formación, y herramientas produce distintos beneficios: prevenir errores, mejor competencia técnica, optimización del software, lo que se traduce en un menor riesgo tanto para el producto como para el usuario del mismo.

Como todo producto Microsoft está orientado a integrase con lo suyo. Así dependiendo de la fase donde estemos ofrece plantillas o analizadores que se integran de manera perfecta con Visual Studio Team System.

Es por ello que la meta principal de SDL es el incrementar la calidad del software impulsado por la mejora de la seguridad en los procesos de desarrollo.

SDL está basado en tres conceptos básicos:

1. Educación
2. Mejora en el proceso continuo
3. Responsabilidad

Educación

La educación continua y la mejora de los miembros de un equipo de desarrollo de software es crítica. Invertir en formación ayuda a las empresas a estar preparadas ante los cambios tecnológicos y las amenazas que se deriven de ello. Porque el riesgo no es estático, SDL tiene un énfasis más fuerte en entender la causa y el efecto de las vulnerabilidades (bugs) en la seguridad. Necesita una evaluación periódica de los procesos SDL y una presentación de los cambios en respuesta a la tecnología o a las posibles amenazas. Se recogen los datos obtenidos para evaluar la efectividad de la prueba realizada (entrenamiento); se usan procesos de métricas para confirmar la conformidad del proceso y las métricas a posteriori (post-release) ayudan como una guía a futuros cambios. Finalmente, SDL almacenará todos los datos que podrán ser utilizados a posteriori. Cuando esto se combina con una respuesta detallada tanto de la seguridad de la aplicación como de los planes de comunicación, la

empresa puede proporcionar una orientación concisa y convincente a todas las partes afectadas con el problema.

El modelo de optimización de SDL ha sido diseñado para facilitar de manera gradual una implementación reduciendo los riesgos. El modelo permite hacer cosas tanto a los desarrolladores como a los administradores:

- Permite evaluar el estado de la seguridad del desarrollo mediante el uso de una escala de cuatro niveles de madurez
  1. Básico
     - La seguridad es reactiva
     - Los riesgos del cliente no están definidos
  2. Estandarizado
     - La seguridad es proactiva
     - Los riesgos del cliente están comprendidos
  3. Avanzado
     - La seguridad está integrada
     - Los riesgos del cliente están controlados
  4. Dinámico
     - La seguridad es especializada
     - Los riesgos del cliente están minimizados
- Crea una visión práctica y una hoja de ruta para ir avanzando por los niveles de SDL en cada una de las 6 áreas del desarrollo software:
  1. Entrenamiento
     - Entrenamiento en la seguridad del Core
     - Formación, normas y características a seguir.
  2. Requerimientos
     - Establecer los requerimientos de seguridad
     - Crear calidad
     - Realizar la evaluación de la seguridad y los riesgos encontrados
  3. Diseño
     - Establecer el diseño de los requerimientos
  4. Implementación
  5. Verificación
  6. Liberación
  7. Respuesta
- Mostrar un esquema práctico y las actividades rentables en cada una de las 5 fases teniendo en cuenta el presupuesto, la planificación y los esfuerzos del equipo de desarrollo del software.

Mejora en el proceso continuo

1. El modelo de optimización de SDL consiste en:

A. Introducción
   - Da una introducción a SDL y la forma de utilizarlo.

B. Guía para la autoevaluación
   - La guía consiste en un cuestionario para mostrar el estado actual de la seguridad del desarrollo en los niveles de SDL.

C. 3 guías de implementación
   - En la cual se muestran los pasos necesarios a realizar para ir avanzando en los distintos niveles de madurez en cada una de las 6 áreas de desarrollo
     i. Básico – Estandarizado
     ii. Estandarizado – Avanzado
     iii. Avanzado – Dinámico

Responsabilidad

SDL incluye criterios generales y descripciones para los roles que van a llevar la seguridad y la privacidad. Estos roles se indican durante de la Fase de Requisitos del proceso. Estos roles son de carácter consultivo y proporcionan a la empresa la estructura necesaria para identificar, catalogar y mostrar las cuestiones de seguridad presentes en el desarrollo de un producto software.

Estos roles incluyen:

- Rol de Asesorar, Revisar: estos roles se diseñan para tener una visión global acerca de la seguridad; con permisos para aceptar o rechazar los planes de seguridad del equipo
- Un Equipo formado por los mejores: estos roles son los que negocian, aceptan y marcan un mínimo en los requisitos de seguridad y el mantenimiento de las líneas claras de comunicación durante el desarrollo del producto software.

III.2.5 CISQ

Consortium for IT Software Quality
(Object Management Group, 2012)

Autor: Consortium for IT Software Quality

Año de creación: 2012

Última Versión: CISQ–TR–2012–01

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 costos.

Una de las últimas propuestas del CISQ es su estándar de calidad del producto. Este documento, toma el núcleo de la ISO 25000 (SQuaRE), que tiene como objetivo describir un estándar internacional que permita a las organizaciones automatizar la medición de cuatro características de la calidad del producto de software: confiabilidad, eficiencia de rendimiento, seguridad y mantenibilidad.

De todas las características de calidad del producto software que define la ISO 25010 (8 características), los participantes de distintos foros de CISQ eligieron que este documento recogería de momento sólo las 4 características mencionadas en el párrafo anterior, por ser las características más importantes y más susceptibles de poder ser medidas y automatizadas con distintas herramientas.

Para poder medir la calidad del producto software, en qué grado un producto software cumple esas características de calidad de producto, y desarrollar herramientas que automaticen ese proceso, los desarrolladores del estándar de CISQ trabajaron en definir distintas violaciones graves que se pueden encontrar en el código, relacionadas con cada una de esas cuatro características de calidad.

Por lo que se cuentan con cuatro características de calidad que se tomaron como base para poder tener un sistema adecuado a las cuales adicionalmente se les identificaron los puntos clave a ser considerados:

1. Confiabilidad
    a. Madurez
    b. Disponibilidad
    c. Tolerancia a Fallos
    d. Recuperabilidad
    e. Cumplimiento
2. Eficiencia de rendimiento
    a. Comportamiento de tiempo
    b. Recurso
    c. Utilización
    d. Cumplimiento

3. Seguridad
    a. Confidencialidad
    b. Integridad
    c. No repudio
    d. Autenticidad
    e. Responsabilidad
    f. Conformidad
4. Mantenibilidad
    a. Modularidad
    b. Reusabilidad
    c. Estabilidad a cambios
    d. Tolerante a test

Para la característica de Seguridad, CISQ identificó 19 temas de calidad relacionados con la seguridad que al considerarlos dentro del proceso de desarrollo permitirá reducir significativamente las 6 sub-características detectadas. Para cada uno de los 19 temas se especifican sus respectivas reglas de calidad que permiten guiar al usuario para su implementación así mismo se cuentan con elementos de verificación para conocer si efectivamente se satisficieron los temas de calidad de seguridad.

Por ejemplo:

CWE-89: Neutralización incorrecta de elementos especiales utilizados en un comando SQL ('SQL Injection')	Regla 2: Utilizar una biblioteca o un Framework que no permita que se produzca la inyección de SQL o proporcione construcciones que faciliten la utilización de estas capas de persistencia.	Medida 2: Número de instancias en las que se incluyen datos en sentencias SQL que no se pasan a través de las rutinas de neutralización.

III.2.6 MÉTRICA 3

Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información (Ministerio de Hacienda y Administraciones Públicas, n.d.-b)

Autor: Ministerio de Hacienda y Administraciones Públicas del Gobierno de España

Año de creación: 1989

Última Versión: V 3.0

El Gobierno de España a través del Ministerio de Hacienda y Administraciones Públicas realizó una metodología para la sistematización de las actividades que dan soporte al ciclo de vida del software.

Persiguiendo los siguientes objetivos:

- Proporcionar o definir Sistemas de Información que ayuden a conseguir los fines de la Organización mediante la definición de un marco estratégico para el desarrollo de los mismos.
- Dotar a la Organización de productos software que satisfagan las necesidades de los usuarios dando una mayor importancia al análisis de requisitos.
- Mejorar la productividad de los departamentos de Sistemas y Tecnologías de la Información y las Comunicaciones, permitiendo una mayor capacidad de adaptación a los cambios y teniendo en cuenta la reutilización en la medida de lo posible.
- Facilitar la comunicación y entendimiento entre los distintos participantes en la producción de software a lo largo del ciclo de vida del proyecto, teniendo en cuenta su papel y responsabilidad, así como las necesidades de todos y cada uno de ellos.

Contempla el desarrollo de Sistemas de Información para las nuevas tecnologías emergentes, así como los aspectos de gestión que permitan el aseguramiento de los objetivos en términos de calidad, coste y plazos.

Para poder cumplir los objetivos, Métrica 3 tiene en cuenta los métodos de desarrollo más extendidos, así como los últimos estándares de Ingeniería de Software y Calidad, además cuenta con referencias específicas en cuanto a seguridad y gestión de proyectos. Así mismo toma en cuenta las experiencias obtenidas en las versiones anteriores con la finalidad de solventar los problemas o deficiencias detectadas.

Está orientada hacia los procesos permitiendo abarcar el desarrollo completo de Sistemas de Información sea cual sea su complejidad y magnitud, lo realiza gracias a la metodología que utiliza debido a que descompone cada uno de los procesos en actividades y éstas a vez en tareas.

La estructura principal de MÉTRICA 3 son los siguientes

- Planificación de Sistemas de Información.

- Desarrollo de Sistemas de Información.
- Mantenimiento De Sistemas de Información.

La estructura de MÉTRICA 3 incluye también un conjunto de interfaces que definen una serie de actividades de tipo organizativo o de soporte al proceso de desarrollo y a los productos, que en el caso de existir en la organización se deberán aplicar para enriquecer o influir en la ejecución de las actividades de los procesos principales de la metodología y que si no existen habrá que realizar para complementar y garantizar el éxito del proyecto desarrollado.

La aplicación de MÉTRICA 3 proporciona sistemas con calidad y seguridad, no obstante, puede ser necesario en función de las características del sistema un refuerzo especial en estos aspectos, refuerzo que se obtendría aplicando la interfaz.
Las Interfaces descritas en la metodología son:

- Gestión de Proyectos (GP)
- Seguridad (SEG)
- Aseguramiento de la Calidad (CAL)
- Gestión de la Configuración (GC)

Interfaz de Seguridad

El objetivo de la interfaz de seguridad de MÉTRICA 3 es 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.

Haciendo posible incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad, completando el plan de seguridad vigente en la organización o desarrollándolo desde el principio, utilizando MAGERIT (Consejo Superior de Administración Electrónica, 2012) como metodología de análisis y gestión de riesgos en el caso de que la organización no disponga de su propia metodología.

Las valoraciones sobre la seguridad deben realizarse en función de las características del sistema sin perder de vista además que, al ser finitos los recursos, no pueden asegurarse todos los aspectos del desarrollo de los sistemas de información, por lo que habrá que aceptar un determinado nivel de riesgo concentrándose en los aspectos más comprometidos o amenazados, que serán diferentes según las circunstancias en que se maneje el proyecto.

III.2.7 NIST SDLC (800-64)

Security Considerations in the System Development Life Cycle (SDLC)
(Kissel et al., 2008)

Autor: National Institute of Standars and Technology (NIST)

Año de creación: 2008

Última Versión: 800-64 R2

El Departamento de Comercio del Gobierno de Estados Unidos a través del Instituto Nacional de Normas y Tecnología realizó la publicación 800-64 "Security Considerations in the System Development Life Cycle" con la finalidad de ayudar a las Agencias del Gobierno Federal a integrar procesos de seguridad esenciales en su ciclo de vida de desarrollo de software. Permitiendo servir de referencia para implementarse en conjunto con otras publicaciones de NIST que permitan un desarrollo integral.

La integración temprana de los principios de la seguridad en el SDLC permite a las agencias maximizar el retorno de la inversión en sus programas de seguridad, a través de:

- La identificación temprana y la mitigación de vulnerabilidades y configuraciones de seguridad incorrectas, lo que resulta en un menor costo de implementación del control de la seguridad y la mitigación de la vulnerabilidad;
- Conciencia de posibles problemas de ingeniería causados por controles obligatorios de seguridad;
- Identificación de los servicios de seguridad compartidos y reutilización de las estrategias y herramientas para reducir costos y programas de desarrollo al tiempo que mejora la postura de seguridad a través de métodos y técnicas probadas de seguridad.
- Facilitación de la toma de decisiones ejecutivas informadas a través de la gestión integral del riesgo de manera oportuna.

La manera más eficaz de lograr la integración de la seguridad dentro del ciclo de vida de desarrollo del sistema es planificar e implementar un programa integral de gestión de riesgos. Esto se traduce en costos y requisitos de seguridad integrados, así como en un proceso de autorización repetida y embebida que proporciona información de riesgo a los interesados y desarrolladores de TI en toda la agencia.

El SDLC que propone NIST contiene 5 fases:

1. Fase de Iniciación

Durante esta fase, las consideraciones de seguridad son esenciales para la integración diligente y temprana, asegurando de este modo que las amenazas, los requisitos y las posibles limitaciones en la funcionalidad y la integración sean consideradas.

2. Fase de desarrollo y adquisiciones

Durante esta fase, se abordarán las consideraciones de seguridad únicas para el proyecto, como lo es el análisis de los requisitos de seguridad y el diseño de la arquitectura de seguridad entre otros aspectos.

3. Fase de Implementación y Evaluación

Durante esta fase, el sistema se instalará y evaluará en el entorno operativo de la organización.

4. Fase de Operación y Mantenimiento

En esta fase, los sistemas están en su lugar y se están desarrollando, probando y mejorando y / o modificando y se agrega o reemplaza hardware y / o software.

5. Fase de Disposición

En esta fase, se prevé la disposición de un sistema al cierre de cualquier contrato vigente.

III.2.8 COMMON CRITERIA (CC)

Common Criteria for Information Technology Security Evaluation
("Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model," 2012)

Autor: CSE (Canadá), SCSSI (France), BSI (Alemania), NLNCSA (Holanda), CESG (Reino Unido), NIST (USA) y NSA (USA).

Año de creación: 1990

Última Versión: 3.1

Es un conjunto internacional que brinda las directrices y especificaciones desarrolladas con la finalidad de evaluar la seguridad de los sistemas desarrollados; ello principalmente para asegurar el cumplimiento de los estándares establecidos por los diversos países que realizaron los Common Criteria (CC).

El CC proporcionan un conjunto común de requisitos para la funcionalidad de seguridad de los productos de TI y para las medidas de garantía aplicadas a estos productos de TI durante una evaluación de seguridad. Estos productos de TI pueden implementarse en hardware, firmware o software.

El proceso de evaluación permite establecer un nivel de confianza de que la funcionalidad de seguridad de estos productos de TI y las medidas de aseguramiento aplicadas a estos productos de TI cumplen estos requisitos. Los resultados de la evaluación permiten a los consumidores determinar si estos productos de TI satisfacen sus necesidades de seguridad.

Los CC tienen dos componentes principales: Los perfiles de protección y los niveles del Aseguramiento de Evaluación.

Los perfiles de protección (PPro) define un conjunto de requisitos de seguridad para un tipo de producto.

Los niveles del Aseguramiento de Evaluación (EAL) define la medida en que el sistema es probado. Tiene una escala del 1 al 7, siendo uno la evaluación de nivel más bajo y siete el nivel más alto de evaluación. Cabe mencionar que una evaluación de nivel superior no significa que el producto tenga un nivel más alto de seguridad, sino que el producto pasó por más pruebas.

CAPÍTULO IV. LA ESENCIA

IV.1 INTRODUCCIÓN

En la segunda parte de la investigación, en primer lugar, se describe la forma de trabajar del Estándar "La Esencia" (Object Management Group, 2015) comenzando con conceptos principales hasta la forma en que se estructura su forma de trabajo, ello permitirá poder definir las bases para la implementación de las medidas de seguridad en ella, dando la creación de Essence Sec, en donde se define comó se implementará la inclusión de todos los aspectos de seguridad identificados. Así mismo se cuenta con una implementación que servirá de ejemplo para identificar como se ha aplicado la inclusión de temas de seguridad a un estándar de Ingeniería de software llamado Métrica 3 (Ministerio de Hacienda y Administraciones Públicas, n.d.-a, n.d.-b).

IV.2 LA ESENCIA (ESSENCE)

Kernel and Language for Software Engineering Methods (Object Management Group, 2015)

Autor: OMG (Estándar)

Año de creación: 2014

Última Versión: 1.1 (diciembre de 2015)

Se creó debido a un diagnóstico realizado por el "Software Engineering Method and Theory" (SEMAT) identificó que:

"La Ingeniería de Software estaba gravemente obstaculizada por prácticas inmaduras"

Lo que generaba que:

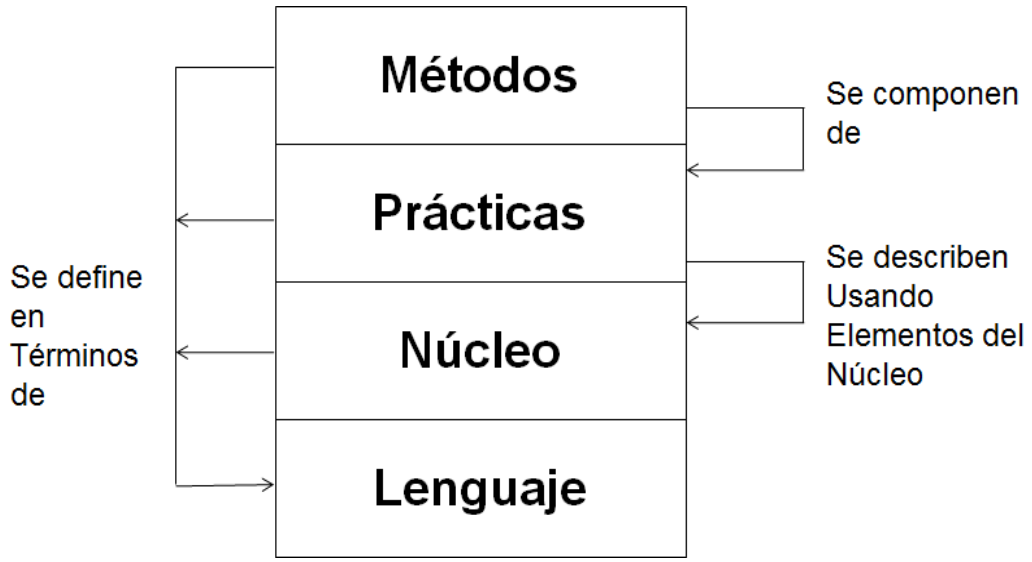
- Existiera una prevalencia de modas
- Falta de una base teórica
- Gran número de métodos distintos para actividades comunes
- Falta de validación experimental creíble
- División entre la práctica de la industria y la investigación académica

Por lo que se generó una propuesta que fue:

> "Apoyar un proceso para re-fundamentar la Ingeniería de Software basado en una teoría sólida, principios probados y mejores prácticas"

Y en 2011 se realiza la transferencia de la iniciativa al Object Management Group (OMG) creando La Esencia que define los conceptos principales que tienen en común todos los desarrollos de software. En conjunto forman un método, ciclo de vida, proceso e incluso filosofía por lo que puede aplicarse a cualquier tipo de desarrollo de software.

IV.2.1 CONCEPTOS DE LA ESENCIA



Método	Es una composición de prácticas, adicionalmente estos son accionables.
Práctica	Es un enfoque repetitivo para hacer algo con un propósito específico en mente. Facilitando una manera sistemática y verificable de tratar un aspecto particular del trabajo.
Núcleo	Incluye los elementos esenciales de la Ingeniería de Software.
Lenguaje	Es el lenguaje de dominio específico para definir métodos, prácticas y otros elementos esenciales del núcleo.

III.3 NÚCLEO DE LA ESENCIA

Proporciona los elementos comunes para entre otros aspectos, comparar métodos y ayudar en la toma de decisiones sobre las prácticas. Se organiza en tres áreas discretas de interés, cada una enfocada a un aspecto específico de la Ingeniería de Software:

Cliente	• Contiene todo lo relativo al uso actual y la explotación del sistema de software a producir
Solución	• Contiene todo lo relativo a la especificación y el desarrollo del sistema de software
Esfuerzo	• Contiene todo lo relativo al equipo y la manera como ellosse enfocan en su trabajo

Cada área tiene unas Alfas, Espacios de Actividades y Competencias específicas.

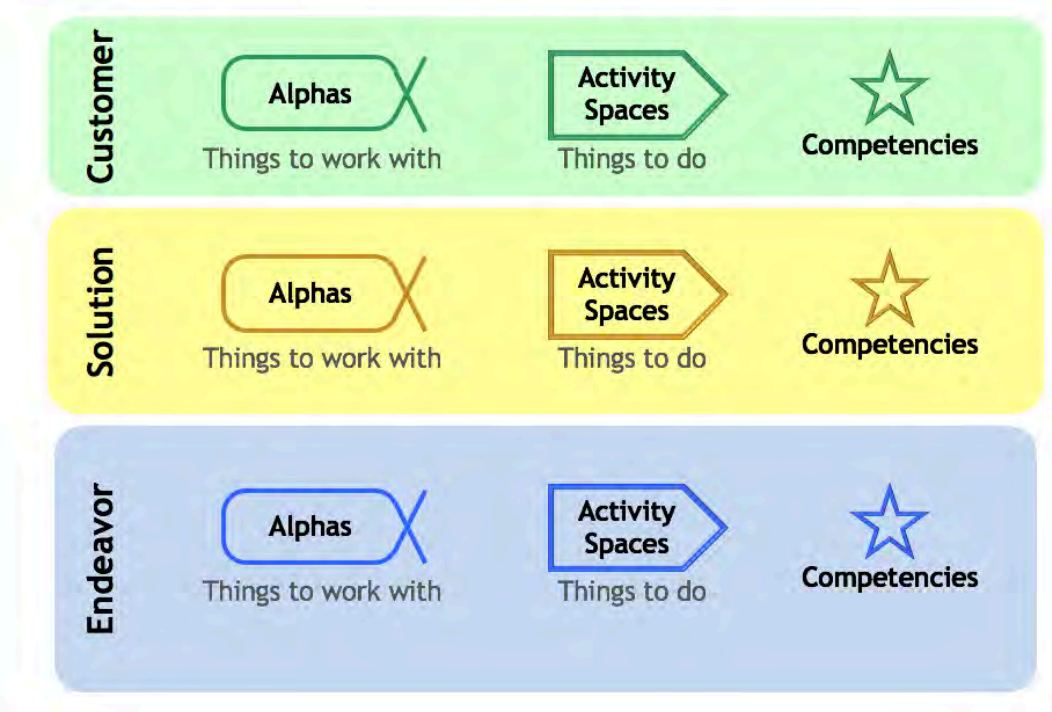


FIGURA IV.1 "ÁREA A TRABAJAR CON SUS RESPECTIVAS ALFAS, ESPACIOS DE ACTIVIDADES Y COMPETENCIAS" (Jacobson et al., 2013)

IV.4 ALFAS

Es un acrónimo del vocablo inglés ALPHA (Abstract-Level Progress Health Attribute).

Son representaciones del trabajo esencial a realizar proporcionando las descripciones necesarias para que los equipos desarrollen, mantengan y den soporte al software, así como permitir evaluar el progreso y salud que tenga el proyecto, realizado a través de un conjunto predefinido de estados que contienen una lista de verificación. En la figura V.2 se muestran los Alfas y sus relaciones.

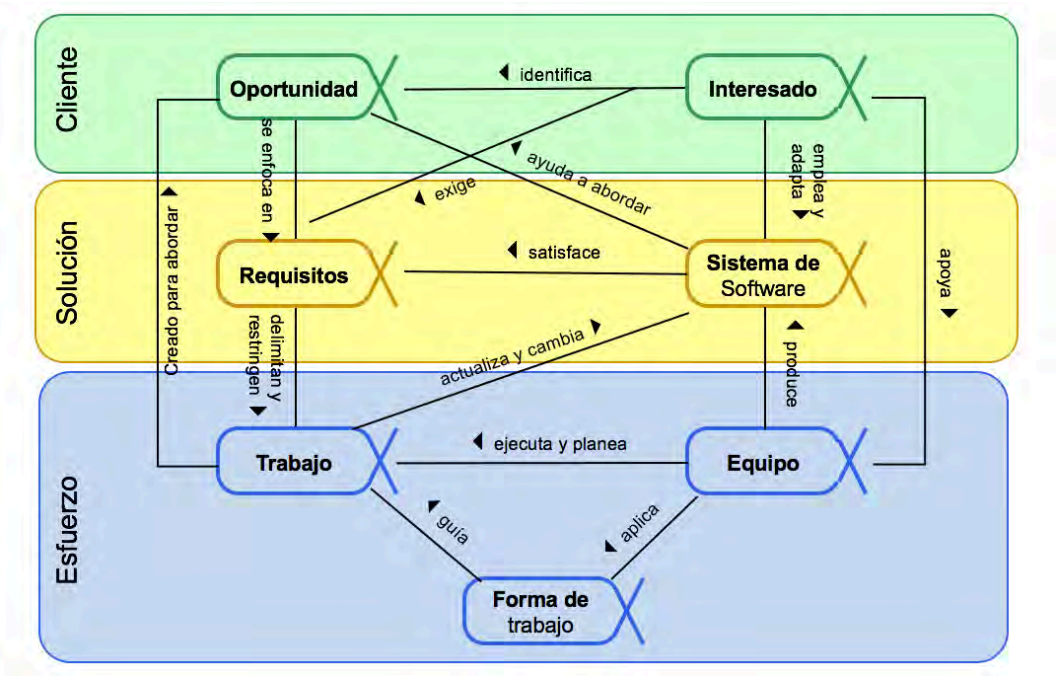


FIGURA IV.2 "COSAS A TRABAJAR EN LA ESENCIA" (Jacobson et al., 2013)

Como ya se mencionó anteriormente, cada Alfa contiene una serie de Estados independientes que deben ser cubiertos para poder cumplir con ella. A su vez los Estados contienen una lista de verificación donde se específica más a detalle las actividades y requisitos que se deben cumplir para que el estado se realice adecuadamente. Ello permite enfocarse en actividades importantes lo que evita desviarse del objetivo principal.

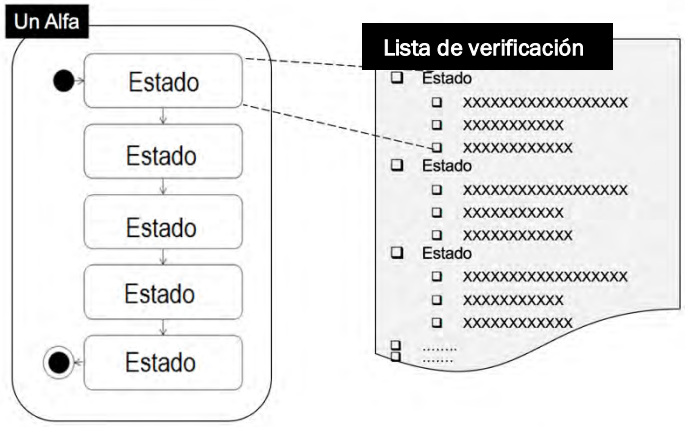


FIGURA IV.3 ESTRUCTURA DE UN ALFA (Jacobson et al., 2013)

Un ejemplo de Alfa es la de "Requisitos"

Esta Alfa "Requisitos" contiene 6 Estados:

- Concebido
- Acotado
- Coherente
- Aceptable
- Tratado
- Cumplido

Y cada Estado contiene su propia lista de verificación:

- Concebido
  - La necesidad de un nuevo sistema es clara
  - Se identificaron los usuarios
  - Se identificaron los promotores iniciales

- Acotado
  - Se acordaron el propósito y la extensión del sistema
  - Los criterios de éxito son claros
  - Se acordaron los mecanismos para manejar los requisitos
  - Se identificaron las restricciones y suposiciones

- Coherente
  - La visión general es clara y la comparten todos los involucrados
  - Se explicaron importantes escenarios de uso
  - Las prioridades son claras
  - Se trataron los conflictos
  - Se comprende el impacto

- Aceptable
  - Los requisitos describen una solución aceptable para los interesados
  - La tasa de cambio para acordar requisitos es baja
  - El valor es claro

- Tratado
  - Suficientes requisitos se implementaron par que el nuevo sistema sea aceptable
  - Los interesados acuerdan que el sistema vale la pena realizando trabajo operativo

- Cumplido
  - El sistema satisface completamente los requisitos y las necesidades
  - No hay ítems excepcionales de requisitos excepcionales que impidan que el sistema se considere completo

IV.5 ESPACIOS DE ACTIVIDADES

Representan lo esencial a hacer, describiendo los retos a los que se enfrenta un equipo a la hora de desarrollar, mantener o dar soporte a los sistemas de software, y el tipo de cosas a hacer para conseguirlos.

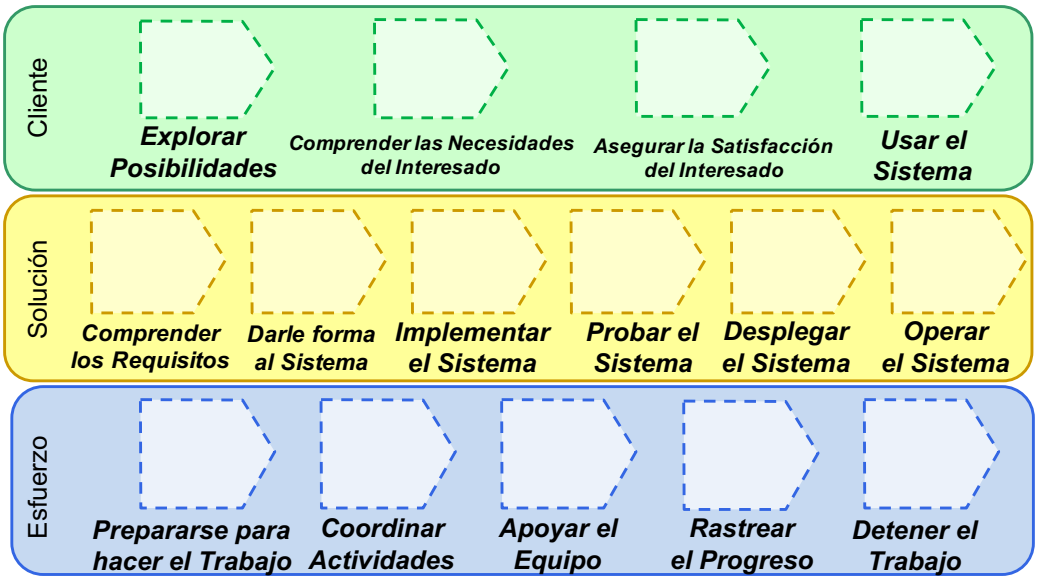


FIGURA IV.4 "ESPACIOS DE ACTIVIDADES BASE PARA CADA ÁREA DE LA ESENCIA" (Jacobson et al., 2013)

IV.6 COMPETENCIAS

Una competencia incluye 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).

Niveles de Competencia

- Nivel 1 - Asistir:
  Demuestra una comprensión básica de los conceptos y puede seguir las instrucciones.

- Nivel 2 - Aplicar:
  Capacidad de aplicar los conceptos en contextos simples por la aplicación rutinaria de la experiencia adquirida hasta la fecha.
- Nivel 3 - Experiencia:
  Capacidad de aplicar los conceptos en la mayoría de los contextos y tiene la experiencia de trabajar sin supervisión.
- Nivel 4 - Adaptar:
  Capacidad de aplicar juicio sobre cuándo y cómo aplicar los conceptos a los contextos más complejos. Puede capacitar a otros para que puedan aplicar los conceptos.
- Nivel 5 - Innovar:
  Un reconocido experto, capaz de extender los conceptos a nuevos contextos e inspirar a otros.

Las competencias o destrezas se basan en roles, de los cuales algunos son comunes a la mayoría de los esfuerzos o de los mismos roles.

Las competencias se valoran usando varios criterios, los cuales ayudan a determinar el nivel de competencia o destreza con la que cuenta el rol evaluado.

CAPÍTULO V. ARMONIZACIÓN DE ESTÁNDARES Y MODELOS

V.1 INTRODUCCIÓN

La búsqueda de asegurar la seguridad en los desarrollos de software por parte de las organizaciones tanto públicas como privadas ha dado como resultado que en la última década se tenga un gran aumento de propuestas para la inclusión de medidas de seguridad dentro del desarrollo del software, unas enfocadas en todo el ciclo de desarrollo y otras únicamente ven la inclusión de la seguridad al agregar o especificar más detalladamente las pruebas que se le realizan al software.

En (Sheard & Lake, 1998) destacan que la gran cantidad de marcos y estándares pueden convertir este campo en "una Ciénega en la que se empantanen los esfuerzos de mejora de procesos si una organización no es cuidadosa", lo que trae como consecuencia que las organizaciones pretendientes a implementar e institucionalizar múltiples propuestas por separado sin un conocimiento ni experiencia previa, estén condenadas al fracaso. Dado que cada una de estas propuestas cuenta con su propia estructura y terminología, teniendo como consecuencia que a las organizaciones se les dificulte el realizar comparaciones y uniones entre las diversas opciones con la finalidad de poder elegir los componentes que cubran las necesidades específicas del proyecto.

Es por ello que Pardo et al. (2010) plantea la necesidad de armonizar los marcos y estándares, teniendo como objetivo identificar las relaciones y darle solución a las diferencias que se encuentren (estructurales, sintácticas, semánticas etc.) entre los diversos modelos.

Sin embargo, hay que tener claro 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 para todos los procesos dentro del ciclo de vida del desarrollo del Sistema de Información (Piattini Velthuis & Hervada Vidal, 2007).

En este sentido, el propósito de esta parte de la investigación es el proponer una armonización de las diferentes propuestas de inclusión de la seguridad en el desarrollo de software que permita identificar y definir estrategias necesarias que conduzcan a su implementación dentro del ciclo de vida del desarrollo de software.

V.2 METODOLOGÍA

Para realizar la armonización de las diferentes propuestas, fue necesario ejecutar la estrategia propuesta por Pino et. Al (2012), comprendida en primer lugar por la homogeneización de las propuestas, posteriormente realizando la integración de los estándares y modelos y finalizando con el análisis general de los resultados.

Los pasos que se siguieron para realizar la homogeneización de las diversas propuestas fueron:

1. Alinear y definir los objetivos para la armonización.
2. Elegir las propuestas a incorporar.

3. Inspeccionar las diferentes estructuras de las propuestas para definir una que sirva de marco común.
4. Se realizó un mapeo de las propuestas seleccionadas basada en la estructura de la Esencia.
5. Se realizó un estudio de la correlación que tienen las diversas propuestas.
6. Posteriormente se llevó a cabo una categorización estratégica de las diversas similitudes encontradas en el análisis.
7. Una vez realizados los puntos anteriores se procedió a la construcción del modelo armonizado con las características principales obtenidas.

De manera que 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 arrojó un resumen de que se cuentan con diversas propuestas que se implementan 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
- Common Criteria
- NIST SDLC

Los marcos y estándares anteriormente listados es posible clasificarlos con base en (Piattini Velthuis et al., 2015) en:

Estándares y Guías	Establecen lo que se debería de hacer en una situación contractual, un ejemplo de ellas son las normas ISO 27001, 25010 y estándares como el NIST SDLC y Common Criteria.
Métodos de evaluación	Posibilitan juzgar y decidir sobre la capacidad de los procesos y la madurez de las organizaciones que están sujetas al análisis como BSIMM entre otros.
Modelos de referencia	Establecen una forma para describir las características y prácticas de los buenos procesos en diferentes aspectos organizacionales como lo es SAMM, Microsoft SDL, Métrica 3, CISQ, entre otros.

El objetivo general de la armonización para esta investigación es:

- Definir las áreas y funciones de seguridad utilizadas 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 específico 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.

Se estableció la necesidad de colocar identificadores únicos para cada una, permitiendo rastrear sus funciones y prácticas, un ejemplo es SAMM (S) (The Open Web Application Security Project, 2016), 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 de las 4 funciones de SAMM sus respectivas prácticas principales, por ejemplo, Gobierno (S – G) 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 que se señalan con un número consecutivo posterior al Id de la función a la que corresponde, por ejemplo “Estrategia y métricas (EM)” contiene 2 que son:

Estrategia y métricas	S G-EM
Establecimiento de un plan estratégico unificado para la	S – G-EM-1

Estrategia y métricas	S G-EM
seguridad del SW	
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 (S)
  - 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, dónde 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.

En una primera instancia, el análisis se realizó por cada una de las prácticas de las Funciones principales de los marcos y estándares establecidos, donde se observaron que las prácticas contenían similitudes entre las definiciones que tenían arrojando las tablas V.1, V.2 y V.3.

TABLA V.1 INTEGRACIÓN DE PRÁCTICAS DE LOS MARCOS Y ESTÁNDARES SELECCIONADOS. (MARCO / ESTÁNDARES [M/E EN TÍTULO DE LA TABLA]).

Relacionadas a el entrenamiento, la capacitación, y la formación

M / E	*Práctica*
MSDL	Entrenamiento
SAMM	Educación y Orientación
BSIMM	Entrenamiento
NIST	Garantizar el desarrollo del sistema de una forma segura
M3	Elaboración del plan de formación de seguridad

Relacionadas a la obtención de Amenazas, Riesgos y Requisitos de Seguridad

M / E	*Práctica*
MSDL	Requerimientos
SAMM	Evaluación de amenazas
SAMM	Requisitos de seguridad
BSIMM	Modelos de Ataque
BSIMM	Estándares y Requerimientos
M3	Planificación de SI
M3	Viabilidad del Sistema
M3	Estudio de la Seguridad Requerida en el proceso de análisis del SI
M3	Descripción de las funciones y mecanismos de seguridad
M3	Especificación de requisitos de seguridad del entorno tecnológico
M3	Requisitos de seguridad del entorno de construcción
M3	Definición de los criterios de aceptación de la seguridad

Relacionadas a la Arquitectura y Diseño

M / E	*Práctica*
MSDL	Diseño
SAMM	Arquitectura de Seguridad
SAMM	Revisión del Diseño
BSIMM	Diseño y características de seguridad
BSIMM	Análisis de la Arquitectura
M3	Diseño del sistema de información
M3	Diseño de pruebas de seguridad
NIST	Diseño de la arquitectura de seguridad

Relacionadas con Métricas y Estrategias

M / E	*Práctica*
S-B	Gobierno
SAMM	Política y cumplimiento
SAMM	Estrategia y Métricas
BSIMM	Política y cumplimiento
BSIMM	Estrategia y Métricas
NIST	Garantizar el desarrollo del sistema de una forma segura
S3	Selección del equipo de seguridad

Relacionadas a la implementación de un sistema

M / E	*Práctica*
MSDL	Implementación
SAMM	Administración de Vulnerabilidades
SAMM	Fortalecimiento de Ambientes
SAMM	Habilitación Operativa
M3	Construcción del SI
IAS-	Evaluación de resultados de pruebas de seguridad

SEG 3	
MSDL	Lanzamiento
M3	Implementación y aceptación del sistema

Relacionadas con Pruebas y Mantenimiento

M / E	*Práctica*
MSDL	Verificación
SAMM	Revisión del Código
SAMM	Pruebas de Seguridad
BSIMM	Revisión del Código
BSIMM	Test de Seguridad
BSIMM	Pruebas de Penetración
M3	Evaluación de los resultados de pruebas de seguridad
NIST	Pruebas de Conducta (Desarrollo, Funcional y Seguridad)
NIST	Evaluar la seguridad del sistema
MSDL	Respuesta
M3	Mantenimiento
M3	Mantenimiento de SI

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.

Es así que se obtuvo la Tabla V.2, en ella se desplegaron todas las actividades definidas en las prácticas de la Tabla IV.1 agrupándose en 8 áreas principales "Entrenamiento, Requerimientos, Diseño, Implementación, Verificación, Lanzamiento, Respuesta y Gobierno" y donde en cada una de ellas se especifican las actividades que realizan con su respectivo Marco / Estándar al que corresponde.

TABLA V.2 ASPECTOS DE SEGURIDAD CON SUS ACTIVIDADES.
[M/E EN TÍTULO DE LA TABLA]

Entrenamiento

M / E	Actividad
M-SDL	Capacitación básica de seguridad
S G-EO-1	Ofrecer acceso a temas de programación segura e implementación
S G-EO-2	Educar a todo el personal en el ciclo de vida del SW con lineamientos específicos en desarrollo seguro
S G-EO-3	Hacer obligatorio el entrenamiento integral
B G-SM-1.3	Educación
B G-T-1.1	Proporcionar entrenamiento
B G-T-1.7	Entrenamientos por áreas o específicos
B G-T-1.6	Tener un histórico de las experiencias obtenidas por la organización

B G-T-3.4	Actualizaciones de conocimiento anuales
CSI-SEG 3.1	Elaboración del plan de formación de seguridad

Requisitos

M / E	Actividad
M-SDL	Establecer los requerimientos de seguridad
M-SDL	Crear estaciones de calidad / Parámetros de Bugs
M-SDL	Valoración de los riesgos de seguridad y privacidad del proyecto
S C-EA-1	Identificar y comprender las amenazas
S C-EA-2	Aumentar la precisión de la evaluación y mejorar la granularidad de la comprensión por proyecto.
S C-EA-3	Comparar controles de compensación a cada amenaza contra otros desarrollos
S C-RS-1	Considerar explícitamente la seguridad durante el proceso de captura de requisitos
S C-RS-2	Aumentar la granularidad de los requisitos derivada de la lógica de negocio y riesgos conocidos
S C-RS-3	Exigir que se siga el proceso de requisitos de seguridad para todo el ciclo de vida del proyecto y 3ros
B I-MA-1.2	Crear un esquema de clasificación de datos e inventario.
B I-MA-1.3	Identificar potenciales atacantes
B I-MA-1.5	Reunir y usar la inteligencia de ataque.
B I-MA-2.1	Crear patrones de ataques y casos de abuso que pueden ser utilizados de acuerdo al análisis
B I-MA-2.7	Crear foros con todos los involucrados para discutir posibles ataques
B I-SR-1.1	Crear un estándar de seguridad
B I-SR-1.2	Crear un portal de ayuda sobre temas de seguridad
B I-SR-2.2	Crear una base de conocimientos a partir de estándares revisados
B I-SR-2.6	Usar estándares de codificación segura
B I-SR-3.1	Control de riesgos al uso de Open Source
B ST-AA-1.4	Usar un cuestionario para rankear el riesgo de la aplicación
EVS-SEG 3.1	Elaboración de Recomendaciones de Seguridad
EVS-SEG 4.1	Valoración y Evaluación de la Seguridad de las Alternativas de Solución
ASI-SEG 2.1	Estudio de las funciones y mecanismos de seguridad a implementar
DSI-SEG 2.1	Análisis de los Riesgos del Entorno Tecnológico
DSI-SEG 3.1	Identificación de los requisitos de seguridad del entorno de construcción
IAS-SEG 2.1	Revisión de medidas de seguridad del entorno de operación

Diseño

M / E	Actividad
M-SDL	Establecer requerimientos de diseño
M-SDL	Analizar la posible superficie de ataque
M-SDL	Modelado de amenazas
S C-AS-1	Insertar consideraciones para lineamientos proactivos de la seguridad en el proceso de diseño
S C-AS-2	Dirigir el proceso de diseño hacia servicios seguros conocidos y diseños seguros desde la concepción
S C-AS-3	Controlar formalmente el proceso de diseño y validar la utilización de componentes de

M / E	Actividad
	seguridad
S V-RD-1	Apoyar en las revisiones de diseño para asegurarse que existan los lineamientos de mitigación para riesgos conocidos
B I-SFD-2.1	Construir y publicar características de seguridad.
B I-SFD-1.2	Construir frameworks middleware y bibliotecas comunes para utilizarse en todos los desarrollos.
B ST-AA-1.1	Revisión de las funciones de seguridad
B ST-AA-1.2	Realizar revisión de diseño para aplicaciones de alto riesgo
B ST-AA-2.1	Definir y usar un análisis de la arquitectura
B ST-AA-2.2	Estandarizar las descripciones de la arquitectura (incluido el flujo de datos)
PSI-SEG 2.1	Estudio y Evaluación del riesgo de las Alternativas de Arquitectura Tecnológica
PSI-SEG 2.2	Revisión de la Evaluación del Riesgo de las Alternativas de Arquitectura Tecnológica

Implementación

M / E	Actividad
M-SDL	Uso apropiado de herramientas
M-SDL	Despreciar funciones inseguras
M-SDL	Análisis Estático
S I-AV-1	Identificar un punto de contacto para problemas de seguridad
S I-AV-3	Conducir análisis de causa raíz para incidentes
S I-FA-1	Entender el ambiente operativo de la aplicación y sus componentes
S I-HO-1	Habilitar las comunicaciones entre los equipos de desarrollo y los operadores de datos críticos
S I-HO-2	Mantener guías formales de seguridad de operaciones
S I-HO-3	Realizar firma de código para componentes de aplicaciones

Verificación

M / E	Actividad
M-SDL	Análisis dinámico
M-SDL	Pruebas de caja negra
M-SDL	Revisión del área de ataque
S V-RC-1	Encontrar oportunamente vulnerabilidades básicas a nivel de código y otros problemas de seguridad
S V-RC-2	Automatización de las revisiones de código
S V-RC-3	Revisiones integrales para descubrir riesgos específicos
S V-PS-1	Establecer el proceso para la realización de pruebas basándose en la implementación y los requisitos del software
S V-PS-2	Realizar pruebas de seguridad durante el desarrollo, pudiendo hacer uso de automatización
S V-PS-3	Realizar pruebas de seguridad específicas al desarrollo en cuestión para asegurarse que los lineamientos de seguridad están implementados antes de la publicación
B ST-CR-1.4	Utilizar herramientas automatizadas junto con una revisión manual.
B ST-CR-1.5	Hacer la revisión de código obligatorio para todos los proyectos
B ST-CR-3.5	Uso de estándares de codificación
B ST-CR-1.6	Utilizar los informes centralizados como medio para la obtener métricas e impulsar la

M / E	Actividad
	capacitación.
B ST-ST-	Asegurar control de calidad compatible con test EDGE / análisis de valores límites.
B ST-ST-1.3	Aplicar test con requerimientos y características de seguridad incluidas
B ST-ST-2.4	Integrar los resultados para obtener métricas que ayuden al proceso de QA
B ST-ST-3.5	Realización de test con base en los casos de abuso.
B ST-ST-2.1	Integrar pruebas de caja negra a los procesos de QA
B D-PT-1.1	Uso de testers de penetración externos para encontrar defectos
B D-PT-1.2	Alimentar los resultados al sistema de gestión y mitigación de defectos.
B D-PT-1.3	Uso de test de penetración internos
B D-PT-2.3	Realización periódica de test de penetración a lo largo del desarrollo
ASI-SEG 3.1	Actualización del Plan de Pruebas
DSI-SEG 4.1	Diseño de pruebas de seguridad
CSI-SEG 2.1	Estudio de los resultados de pruebas de seguridad
IAS-SEG 3.1	Estudio de los resultados de pruebas de seguridad de implantación del sistema

Lanzamiento

M / E	Actividad
M-SDL	Plan de respuestas a incidentes
M-SDL	Revisión final de seguridad
M-SDL	Archivo de lanzamiento

Respuesta

M / E	Actividad
M-SDL	Ejecución del plan de respuesta a incidentes
S I-AV-2	Establecer un proceso consistente de respuesta a incidentes
S I-FA-2	Administración de parches y actualizaciones de los componentes y monitoreo de la configuración

Gobierno

M / E	Actividad
B G-SM-1.1	Publicación del proceso (roles, responsabilidades, plan)
B G-SM-2.5	Identificación de métricas
B G-CP-1.1	Revisión de normas regulatorias
B G-CP-1.2	Identificación de información personal confidencial
B G-CP-1.3	Crear una política
B G-CP-2.2	Control de cumplimiento relacionado con los riesgos previstos
B G-CP-2.3	Tener un control de cumplimiento
B G-CP-2.5	Concientización de las obligaciones regulatorias y de privacidad
PSI-SEG 3.1	Determinación de la Seguridad en el Plan de Acción

TABLA V.3 RELACIÓN DE LOS ASPECTOS DE SEGURIDAD CON PRÁCTICAS DE LOS MARCOS Y ESTÁNDARES

Amenazas		Requisitos 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		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		Ni 2
	B I-MA-2.7	M 3	DSI-SEG 2.1	M-SDL	V 1		B G-T-1.7		Ni 3
	B ST-AA-1.4		DSI-SEG 3.1	M 3	ASI-SEG 3.1		B G-T-3.4		Ni 4
	B G-CP-2.2		IAS-SEG 2.1		DSI-SEG 4.1	M 3	CSI-SEG 3.1		Ni 5
	B ST-CR-1.5	**Diseño**			CSI-SEG 2.1	**Métricas y Apoyos**			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	**Pentesting**			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 V.3 se puede ver el resultado obtenido del análisis final, donde se pueden observar los aspectos de seguridad con las respectivas prácticas que fueron identificadas ya haciendo el proceso de depuración e integración de las actividades, así como su catalogación por aspectos de seguridad.

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
   - Donde se realizan actividades que permitirán la detección y administración de las Amenazas del sistema en cuestión.
2. Riesgos
   - Este aspecto administra todo lo relativo a los Riesgos a los que se enfrenta el sistema.
3. Superficie de Ataque
   - En este aspecto se pueden identificar las áreas y aspectos donde se puede sufrir algún tipo de vulnerabilidad en el sistema.

4. Requisitos de Seguridad
    - Para poder contar con un sistema con medidas de seguridad es necesario identificar adecuadamente los requisitos de seguridad que deberán formar parte del desarrollo del sistema por tal motivo se tiene este aspecto de seguridad.
5. Diseño de seguridad
    - Al contar con los requisitos del sistema ya sean funcionales o no, es necesario plasmarlos con el diseño del sistema, es así que se tienen prácticas en este aspecto que permitan realizarlo con medidas de seguridad adecuadas al proyecto.
6. Arquitectura de seguridad
    - Contar con una arquitectura adecuada al proyecto y que esta contenga una visión de seguridad adecuada es de vital importancia para lograr los objetivos de seguridad es así que se cuenta con este aspecto para coadyuvar a seleccionar la arquitectura adecuada.
7. Pruebas de seguridad
    - Una vez que se va desarrollando el sistema es de suma importancia que se le realicen pruebas que permitan verificar que el sistema contiene las medidas de seguridad pactadas, es por ello que se identifican actividades que pueden servir como guía para lograrlo.
8. Entrenamiento
    - El brindar a las personas que trabajaran en el sistema el entrenamiento adecuado no solo en temas específicos de seguridad permitirá que el sistema no contenga defectos adicionales.
9. Herramientas
    - Existen herramientas que pueden facilitar el trabajo para la inclusión de seguridad.
10. Marcos y Regulaciones
    - En los procesos de seguridad son de vital importancia el contar con Marcos y Regulaciones que nos permitan tener una base para lograr los objetivos, así como hacer frente a obligaciones gubernamentales o empresariales por ello este aspecto contiene actividades que ayudarán a realizarlo adecuadamente.
11. Estandarización de Procesos
    - Contar con una guía para que las actividades se realicen de forma estandarizada es importante para reducir los defectos de seguridad.
12. Automatizaciones
    - Algunas pruebas y análisis del sistema se pueden valer de sistemas automatizados para realizar de forma eficiente su trabajo.
13. Control de Procesos
    - El estar verificando que las actividades se están realizando de la forma que fueron pactados es necesario para brindar un trabajo de calidad y por ende el producto final.
14. Métricas
    - En este aspecto se observan todas aquellas actividades que permitirán tener mediciones sobre la seguridad, que en el futuro permitirán tener estadísticos más certeros.

Estos aspectos están fundamentados en diversas prácticas que se encontraron dentro de las propuestas analizadas donde perseguían objetivos en común por lo que se podían unificar,

logrando una homogeneización 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.

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.

SEGUNDA PARTE. ESSENCE SEC

CAPÍTULO VI MÉTRICA 3 COMO BASE PARA IMPLEMENTACIÓN DE ESSENCE SEC

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 (Ministerio de Hacienda y Administraciones Públicas, n.d.-a, n.d.-b) 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.

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 VI.1 se presenta en qué Alfas de la Esencia se podrían implementar las actividades de seguridad identificadas en Métrica 3.

Tabla VI.1 Comparación Esencia y Métrica 3

<table>
<tr><th>Interesados</th><th>Oportunidad</th><th>Requisitos</th><th>Sistema de Software</th><th>Trabajo</th><th>Forma de trabajo</th><th>Equipo</th><th>Esencia</th></tr>
<tr><td rowspan="4"></td><td rowspan="2">Viabilidad del Sistema</td><td rowspan="2">Análisis del Sistema</td><td>Diseño del Sistema</td><td rowspan="4"></td><td rowspan="2">Planificación</td><td rowspan="4"></td><td rowspan="4">Métrica 3</td></tr>
<tr><td>Construcción del Sistema</td></tr>
<tr><td></td><td>Implementación</td></tr>
<tr><td></td><td>Mantenimiento</td></tr>
</table>

VI.1DEFINICIÓN DE ALFAS CON LOS 14 ASPECTOS DE SEGURIDAD

Así mismo 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 VI.2 donde se presentan las relaciones.

Tabla VI.2 Integración Esencia y los Aspectos de Seguridad

<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 colspan="2" rowspan="5"></td><td>Amenazas</td><td>Diseño</td><td rowspan="2">Control de Procesos</td><td colspan="2">Entrenamiento</td><td rowspan="5">Aspectos de Seguridad</td></tr>
<tr><td>Riegos</td><td>Arquitectura</td><td>Herramientas</td><td>Control de Procesos</td></tr>
<tr><td>Superficie de Ataque</td><td>Pruebas</td><td colspan="2">Normas y Regulaciones</td><td rowspan="3"></td></tr>
<tr><td>Requisitos de Seguridad</td><td rowspan="2"></td><td colspan="2" rowspan="2">Estandarizaciones</td></tr>
<tr><td colspan="2">Automatizaciones</td></tr>
</table>

CAPÍTULO VII. LA ESENCIA EN EL DESARROLLO DE SOFTWARE SEGURO: ESSENCE SEC

VII.1 INTRODUCCIÓN

Al contar con el panorama general de la armonización de los marcos y estándares referidas en el Capítulo IV 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. Es así que se procedió a realizar el análisis para realizar esta extensión, a la que se llamará Essence Sec.

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 agregó una Sub-Alfa que se creyó necesaria para destacar sobre prácticas.

- 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 implementación.

Estos principios se consideraron con la finalidad de que los usuarios que actualmente hacen uso de la Esencia en su forma tradicional, puedan hacer uso de 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 de la Esencia, les permita incluir medidas de seguridad en sus desarrollos de una forma transparente desde el primer momento que la utilicen.

Adicionalmente 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 a llevar a cabo durante el proceso. Para los usuarios que se están familiarizando con los temas de seguridad, se especifican detalladamente los procedimientos en los Espacios de actividades, brindándoles lo necesario 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.

A continuación, se presentan cada una de las 4 Alfas seleccionadas, donde se añaden los aspectos de seguridad identificados para cada una de ellas, realizado de acuerdo a sus especificaciones y también haciendo uso del Anexo B "KUALI-BEH Kernel Extension" para especificar las actividades específicas de cada Alfa.

Para la inclusión de medidas de seguridad en el Alfa de Requisitos se propone incorporar elementos extras en las listas de verificación de los estados ya establecidos por la Esencia. También, se propone una Sub-Alfa, que permita considerar los requisitos de seguridad para el proyecto.

La inclusión de los elementos extras, permite a las personas que implementan la Esencia en sus proyectos, el hacer revisiones periódicas para la comprobación e inclusión de actividades de seguridad dentro de sus desarrollos favoreciendo la reducción de los fallos de seguridad.

Los aspectos principales de seguridad que se proponen para la incorporación de medidas de seguridad en el Alfa de Requisitos de la Esencia son:

- Riesgos
- Amenazas
- Requisitos de seguridad
- Superficie de ataque
- Normas y Regulaciones

Los riesgos y las amenazas de seguridad a los que se enfrenta el Sistema de Información se deben de considerar a la hora de crear un sistema de software, ya que de hacerlo se reducirían las brechas de seguridad a las que se enfrentarían de no considerarlos. Estas brechas pueden provocar problemas de tipo monetarios, regulatorios, pérdida de credibilidad o incluso pérdidas de vidas humanas, etc. Por tal motivo es importante conocer todas aquellas amenazas de seguridad que puedan producir que el Sistema de Información no trabaje de la forma adecuada.

Una vez que se cuenta con la información de los Riesgos y Amenazas, a los que se puede enfrentar el Sistema de Información, se puede realizar la obtención de los requisitos de seguridad que servirán como medidas de salvaguarda contra los efectos adversos que producen esos riesgos.

A continuación, en la Tabla VIII.1 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 VIII.1 "Lista de Verificación General y de Seguridad del Alfa de Requisitos"

Estados Requisitos	Verificación General	Verificación de Seguridad
Concebido	• Los stakeholders iniciales están de acuerdo con que el sistema se va a producir. • Se han identificado a los stakeholders que van a utilizar el nuevo sistema.	• 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

Estados Requisitos	Verificación General	Verificación de Seguridad
	• Se han identificado los stakeholders que van a financiar el trabajo inicial del nuevo sistema. • Es clara la oportunidad a la que hará frente el nuevo sistema.	el sistema.
Acotado	• Se han identificado a todos los stakeholders involucrados en el desarrollo del nuevo sistema. • Los stakeholders están de acuerdo en el objetivo del nuevo sistema. • Está claro cuál es el éxito para el nuevo sistema. • Los stakeholders comprender y están de acuerdo en la extensión de la solución propuesta. • Hay un acuerdo en la forma de describir los requerimientos. • Se han definido los mecanismos para la gestión de los requisitos. • Está claro el esquema de priorización. • Se han identificado y considerado las restricciones • Las hipótesis se han fijado claramente.	• Se ha realizado satisfactoriamente la evaluación de todos los Estados del Sub-Alfa "Evaluación de Riesgos" generando los requisitos de seguridad. • Se han incorporado los requisitos de seguridad a los requisitos establecidos en el proyecto.
Coherente	• La visión general es clara y la comparten todos los involucrados. • Se explicaron importantes escenarios de uso. • Las prioridades son claras. • Se trataron los conflictos. • Se comprende el impacto.	• Se identificaron las medidas de seguridad en el entorno de desarrollo
Aceptable	• Los requisitos describen una solución aceptable para los interesados. • La tasa de cambio para acordar requisitos es baja. • El valor es claro.	• 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	• Suficientes requisitos se implementaron par que el nuevo sistema sea aceptable • Los interesados acuerdan que el	• Se han monitoreado las medidas de seguridad en el entorno de operación.

Estados Requisitos	Verificación General	Verificación de Seguridad
	sistema vale la pena realizando trabajo operativo	
Cumplido	• El sistema satisface completamente los requisitos y las necesidades • No hay ítems excepcionales de requisitos excepcionales que impidan que el sistema se considere completo	• Los interesados reconocen el valor proporcionado por la implementación de la seguridad en el proyecto.

En el proceso de realizar la integración de la seguridad en el Alfa de Requisitos se vio la necesidad de incluir una Sub-Alfa que permita a los usuarios tener una mayor comprensión de los aspectos de seguridad incluidos en este proceso.

VIII.1 SUB-ALFA EVALUACIÓN DE RIESGOS DE SEGURIDAD

Introducción:

Esta extensión provee una Sub-Alfa "Evaluación de Riesgos de Seguridad" adicional que ayuda a los equipos a conocer y evaluar los riesgos a los que el Sistema de Información está expuesto. Una vez que se conocen los riesgos es posible obtener los requisitos de seguridad.

Descripción:

Evaluación de Riesgos de seguridad:	Se realiza un análisis para obtener los requisitos de seguridad vigentes para el proyecto.
Alfa de Orden Superior:	Requisitos[1]

Estados del Sub-Alfa:

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 más 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 integran los requisitos del sistema con los requisitos de seguridad obtenidos para aplicarlos en el desarrollo.

Integración de Requisitos con Evaluación de Riesgos

Asociaciones:

Impulsa: Requisitos	El progreso de Evaluación de Riesgos impulsa el progreso de los Requisitos.

Justificación: Porqué la Evaluación de Riesgos de Seguridad:

El contar con la Evaluación de Riesgos de Seguridad del Sistema de Información a implementar, permite identificar las fortalezas, debilidades, oportunidades y amenazas a las que se enfrentará el SI 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.

[1] Para mayor detalle consultar la Figura VIII.1

Ya que en primer lugar se hace un análisis de todos aquellos activos que están involucrados con el sistema a crear, permitirá identificar aquellas posibles amenazas que pueden ocasionar el mal funcionamiento del sistema. Así como, aquellas personas que estarán involucradas directa o indirectamente con su uso, esto permitirá conocer la interacción que tienen con el sistema y sus posibles acciones a realizar.

Seguidamente se procede a realizar la valoración de todas las amenazas detectadas para cada uno de los activos o grupo de activos, así como de su entorno. Posteriormente se realiza la valoración del riesgo que estas amenazas representan para determinar el nivel de riesgo que representan, teniendo la posibilidad de determinar su clasificación de acuerdo a la visión de seguridad establecida para el proyecto.

Una vez que se tienen identificados y clasificados los riesgos es posible el obtener los requisitos de seguridad para la creación de salvaguardas que permitan la reducción de esos riesgos para subsiguientemente realizar su priorización de acuerdo a las necesidades existentes y seguidamente realizar una inspección para detectar ambigüedades o duplicados en los requisitos, finalizando con la obtención de los requisitos de seguridad que permitan solventar la visión de seguridad.

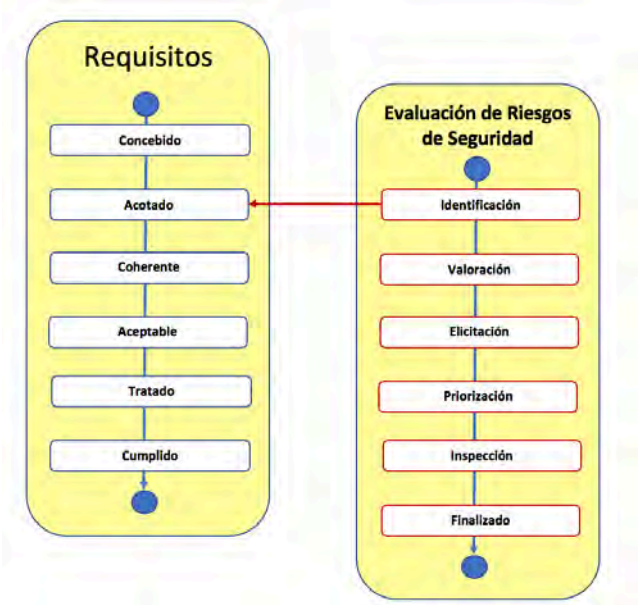


Figura VIII.1 "DEFINICIÓN DE LA UBICACIÓN EL SUB-ALFA *EVALUACIÓN DE RIESGOS DE SEGURIDAD* DENTRO DEL ALFA DE *REQUISITOS*"

Para conocer claramente el estado y progreso de la Evaluación de Riesgos, se proporciona en la Tabla VIII.2 la lista de verificación para cada estado de la Sub-Alfa, así como una lista con los aspectos de seguridad que se ven afectados en el proceso.

Tabla VIII.2 "Lista de Verificación General y de Seguridad del Sub-Alfa de **EVALUACIÓN DE RIESGOS DE SEGURIDAD**"

Estado	Verificación
Identificación	• Se identificaron los activos que están presentes en el sistema. • Las dependencias que tiene cada activo identificado fueron analizadas • Los usuarios involucrados en cada activo identificado fueron analizados. • Cada activo identificado forma parte de la visión de seguridad establecida. • La plataforma informática a la que pertenece el proyecto está clara. • La visión de seguridad para el proyecto está definida y alineada a las metas del negocio. • 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 estableció 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. • 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.

VIII.2 PRÁCTICAS ASOCIADAS A LA EVALUACIÓN DE RIESGOS DE SEGURIDAD

Para realizar correctamente la validación de los estados en la Evaluación de Riesgos de Seguridad a continuación se presentan 8 prácticas:

1. Identificación de los Interesados / Acuerdo de las definiciones
2. Identificación de activos
3. Identificación de objetivos de seguridad
4. Identificación de amenazas
5. Valoración del riesgo
6. Elicitación de requisitos
7. Priorización de requisitos
8. Inspección de requisitos

Cada una de ellas está creada con base en las necesidades que se muestran en las listas de verificación de cada estado (obtenidas a partir de las prácticas obtenidas de la armonización de los marcos y estándares, así como de los profesionales del área de acuerdo con su experiencia y conocimiento), expresando la forma que se debe de trabajar, describiendo las actividades y sus respectivas tareas a realizarse, así como los recursos de entrada que se necesitan para poder operar y los recursos de salida que se obtienen como resultado de la realización de la misma.

Todo ello permite que al realizarse de manera periódica se podrá incluir de manera natural a las prácticas de la organización, así como tener la posibilidad de adaptarse a otros métodos implementados ya por la organización.

Las prácticas están descritas según en el Anexo B: KUALI-BEH Extensión del Kernel de la Esencia (Object Management Group, 2015) que puede observar en la Tabla VIII.3.

Tabla VIII.3 "Ejemplo de Práctica descrita en Kuali-Beh"

# Práctica	Práctica
Nombre de práctica	
Propósito	
Se específica el propósito de la práctica	
Entrada	Resultado
Se especifican los ítems de entrada para que se realice de manera adecuada la práctica.	Se especifican los ítems de salida que se obtienen al realizar la práctica.
Criterios de finalización	
Se especifican los criterios que se deben de cumplir para que la práctica finalice de manera	

<table>
<tr><td colspan="4">adecuada.</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad #</td><td colspan="3">Nombre de la actividad</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Se especifican los ítems de entrada para que se realice de manera adecuada la actividad.</td><td colspan="2">Se especifican los ítems de salida que se obtienen al realizar la actividad.</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>Se definen las tareas a realizarse dentro de la actividad</td><td>Se definen las herramientas que pueden servir para realizar la actividad</td><td>Se describen las competencias que se deben de tener para realizar la actividad</td><td>Se especifican las medidas que se deben considerar para la realización de la actividad.</td></tr>
</table>

VIII.2.1 IDENTIFICACIÓN DE LOS INTERESADOS / ACUERDO DE LAS DEFINICIONES

TABLA VIII.4 "PRÁCTICA IDENTIFICACIÓN DE LOS INTERESADOS / ACUERDO DE LAS DEFINICIONES"

<table>
<tr><td colspan="2">1</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Identificación de los Interesados / Acuerdo de las definiciones</td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Identificar a los interesados que están involucrados con el funcionamiento del nuevo SI, conociendo la influencia que tienen sobre éste y las características que debe de tener el SI para lograr sus metas</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos del Trabajo:
• Descripción del dominio del Sistema de Información
• Documento de funcionalidad del sistema Especificación del alcance funcional del SI (Requisitos funcionales y no, casos de uso y escenarios, etc.)</td><td colspan="2">Productos del Trabajo:
• Documento: Visión de Seguridad</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se cuenta con un documento donde se presentan las características de seguridad que deberá tener el Sistema de Información, las políticas y legislaciones que se aplicarán a la creación, las restricciones que se tienen a nivel de arquitectura, diseño y finalmente la definición de los criterios de aceptación/evaluación de seguridad.</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 1.1</td><td colspan="3">Identificación de los interesados</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos del Trabajo:
• Descripción del dominio del SI
• Documento de funcionalidad del sistema</td><td colspan="2">Productos del Trabajo:
• Documento: Visión de Seguridad
o Definición de los interesados
Que harán uso del sistema, las principales acciones que realizarán y los posibles usuarios que estarían interesados en que fallara el sistema.</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Identificación del entorno en el que se desarrollará el SI
• Definir los interesados que están ligados al funcionamiento del sistema.
• Identificación de los posibles interesados en que el sistema no</td><td>• Entrevistas</td><td></td><td>• Interesados:
oPersonal interno
oExterno con uso frecuente u ocasional
oEtc.</td></tr>
</table>

<table>
<tr><td colspan="2">1</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="2">funcione correctamente.</td><td colspan="2"></td></tr>
<tr><td>Actividad 1.2</td><td colspan="3">Acuerdo de Política de Seguridad</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos del Trabajo:
• Descripción del dominio del SI
• Documento: Funcionalidad del Sistema
• Definición de los interesados
• Documento: Política de seguridad de la Organización</td><td colspan="2">Productos del Trabajo:
• Documento: Visión de Seguridad
o Definición de las políticas y legislaciones que se deben de considerar en el proyecto</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Identificar las políticas y legislaciones que puedan afectar al SI
• Acordar una serie de definiciones de seguridad y requisitos.
• Definir las políticas de seguridad que se deberán seguir para el desarrollo e implementación del SI.
• Definir los criterios de seguridad que se deben de considerar en el sistema.</td><td>• Niveles de seguridad de Common Criteria
• Marcos y estándares
• Evaluation Assurance Level de CC</td><td></td><td></td></tr>
</table>

VIII.2.2 IDENTIFICACIÓN DE ACTIVOS DEL SISTEMA

TABLA VIII.5 "PRÁCTICA IDENTIFICACIÓN DE ACTIVOS DEL SISTEMA"

<table>
<tr><td colspan="2">2</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Identificación de Activos del Sistema</td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Identificar claramente cada activo que tenga el Sistema de Información para accionar una medida de seguridad para su protección.</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de trabajo:
• Documento: Visión de Seguridad
• Documento: Funcionalidad del Sistema</td><td colspan="2">Productos del Trabajo:
• Documento: Activos de seguridad</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se tienen definidos los activos que se encuentran inmiscuidos en el Sistema de Información que necesitan contar con medidas de seguridad para su protección</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 2.1</td><td colspan="3">Identificación de los activos</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos del Trabajo:
• Documento: Visión de Seguridad
• Documento: Funcionalidad del Sistema</td><td colspan="2">Productos del Trabajo:
• Documento: Activos de Seguridad</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Identificación de los activos de seguridad para cada activo (tangible e intangible).
• Análisis de dependencias existentes entre activos.
• Valorar la importancia del activo dentro del sistema.</td><td>• Normas y regulaciones para la seguridad de la información de acuerdo a la ubicación donde se implementará el Sistema de Información.</td><td></td><td></td></tr>
</table>

VIII.2.3 IDENTIFICACIÓN DE OBJETIVOS DE SEGURIDAD

TABLA VIII.6 "PRÁCTICA IDENTIFICACIÓN DE OBJETIVOS DE SEGURIDAD"

<table>
<tr><td colspan="2">3</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Identificación de Objetivos de Seguridad</td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Obtener los objetivos de seguridad necesarios para cumplir con las metas de seguridad establecidas</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de trabajo:
• Documento: Visión de Seguridad
• Documento: Activos de Seguridad
• Especificación de los objetivos o metas del negocio</td><td colspan="2">Productos del Trabajo:
• Documento: Objetivos de Seguridad</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se tienen claros los objetivos de seguridad que permitirán cumplir con las metas establecidas</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 3.1</td><td colspan="3">Identificación de los objetivos de seguridad</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos de trabajo:
• Documento: Visión de Seguridad
• Documento: Activos de Seguridad
• Especificación de los objetivos o metas del negocio</td><td colspan="2">Productos del Trabajo:
• Documento: Objetivos de Seguridad</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Identificar los objetivos de seguridad para cada uno de los activos o grupo de activos identificados de acuerdo a las políticas y restricciones/ requisitos que se tienen
• Establecer las relaciones de trazabilidad entre las partes (activos - objetivos de seguridad - objetivos del negocio)
• Identificar los objetivos de seguridad del entorno
• Establecer su valoración inicial respecto a la probabilidad de ocurrencia, dependencias existentes, etc.</td><td>• Clase ASE de Common Criteria.
• Términos de probabilidad.</td><td></td><td>• Valoración:
o Alta, Media y Baja</td></tr>
</table>

VIII.2.4 IDENTIFICACIÓN DE AMENAZAS DE SEGURIDAD

TABLA VIII.7 "PRÁCTICA IDENTIFICACIÓN DE AMENAZAS DE SEGURIDAD"

<table>
<tr><td colspan="2">4</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Identificación de Amenazas de Seguridad</td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Obtener las amenazas de seguridad a las que se enfrenta el sistema</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de trabajo:
• Documento: Objetivos de Seguridad
• Documento: Activos de Seguridad
• Especificación de los objetivos o metas del negocio
• Informes de ataques o brechas de seguridad en la organización
• Informes de vulnerabilidades de la tecnología base a utilizar</td><td colspan="2">Productos del Trabajo:
• Documento: Especificación de Amenazas
Especificación y modelado de amenazas
Suposiciones y afirmaciones de conformidad
Relaciones de trazabilidad con los objetivos y activos de seguridad.</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se obtienen las amenazas que ponen en riesgo el logro de las metas de seguridad definidas anteriormente.</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 4.1</td><td colspan="3">Detección de amenazas</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos de trabajo:
• Documento: Objetivos de Seguridad
• Documento: Activos de Seguridad
• Especificación de los objetivos o metas del negocio
• Informes de ataques o brechas de seguridad en la organización
• Informes de vulnerabilidades de la tecnología base a utilizar</td><td colspan="2">Productos de trabajo:
• Documento: Especificación de Amenazas</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Identificación de potenciales tipos de atacantes y ataques
• Análisis de las amenazas relacionadas a los objetivos y activos de seguridad
• Análisis de las vulnerabilidades encontradas en el sistema
(En caso que ya esté iniciado el proyecto)
• Análisis de perfiles de</td><td>•Foros con todos los involucrados para discutir posibles ataques
(B I-MA-2.7)
•Requisitos de aseguramiento de los CC
(AVA-VAN 5.2E)</td><td></td><td></td></tr>
</table>

4		Práctica	
protección a implementar • Establecimiento de las relaciones de trazabilidad entre las partes (activos - amenazas - objetivos de seguridad.			
Actividad 4.2	Modelado de amenazas		
Entrada		Salida	
Productos de trabajo: • Documento: Especificación de Amenazas		Productos de trabajo: • Documento Especificación de Amenazas Modelado de las amenazas detectadas	
Tareas	Herramientas	Competencias	Medidas
• Modelado de las amenazas identificadas • Identificación de los casos de mal uso	•Uso de árboles de ataque		

VIII.5 VALORACIÓN DEL RIESGO DE SEGURIDAD

TABLA VIII.8 "PRÁCTICA VALORACIÓN DEL RIESGO DE SEGURIDAD"

<table>
<tr><td colspan="2">5</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Valoración del Riesgo de Seguridad</td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Realizar una valoración general de las amenazas que se identificaron para el Sistema de Información, a fin de obtener la probabilidad de que se materialice cada una de ellas, estimando su impacto y su riesgo asociado aproximado.</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento: Especificación de Amenazas</td><td colspan="2">Productos del Trabajo:
• Documento: Valoración del Riesgo [VF].</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Obtener un documento que contenga una identificación de cómo se ve afectada la tolerancia a los riesgos del Sistema de Información con respecto a cada amenaza.</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 5.1</td><td colspan="3">Valorar las amenazas y determinar su relevancia frente al nivel de seguridad necesario para el cumplimiento de los objetivos de seguridad.</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento: Especificación de Amenazas</td><td colspan="2">Productos del Trabajo:
• Documento de Valoración del Riesgo [v1]
o Identificación de amenazas</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Establecer las amenazas relevantes según el nivel de seguridad especificado por los objetivos de seguridad.</td><td>• Tablas de análisis de MAGERIT v.2
• Usar un cuestionario para rankear el riesgo de la aplicación (B ST-AA-1.4)
• Revisiones integrales para descubrir riesgos específicos (S V-RC-3)</td><td>• El equipo consiste en los interesados y los miembros de desarrollo.</td><td></td></tr>
<tr><td>Actividad 5.2</td><td colspan="3">Estimar el riesgo de las amenazas relevantes, según su potencialidad de ocurrencia e impacto negativo sobre el Sistema de Información.</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos del Trabajo:
• Documento: Valoración del Riesgo [v1].</td><td colspan="2">Productos del Trabajo
• Documento: Valoración del Riesgo[v2]
o Identificación de los riesgos del sistema [v1].</td></tr>
</table>

<table>
<tr><td colspan="2">5</td><td colspan="2">Práctica</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Realizar la estimación de las amenazas relevantes.</td><td></td><td></td><td>• Escalas para el análisis: Muy bajo, bajo, medio, alto y muy alto.
• Frecuencia de las amenazas: Muy Frecuente(Diario), frecuente (Mensual), normal (anual), poca frecuencia (cada vez varios años</td></tr>
<tr><td>Actividad 5.3</td><td colspan="3">Se completa la Tabla de Amenazas, Ataques y Riesgos.</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento: Valoración del Riesgo [v2]</td><td colspan="2">Productos del Trabajo:
• Documento de Valoración del Riesgo [v3]
• Identificación de los riesgos del sistema [v2].</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Especificación de tablas de amenazas
• Revisión de ataques a través de Casos de Mal Uso.
• Valoración del impacto y riesgo según las amenazas identificadas</td><td></td><td></td><td></td></tr>
</table>

VIII.2.6 ELICITACIÓN DE REQUISITOS DE SEGURIDAD

TABLA VIII.9 "PRÁCTICA ELICITACIÓN DE REQUISITOS DE SEGURIDAD"

<table>
<tr><td colspan="2">6</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Elicitación de Requisitos de Seguridad</td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Obtener los requisitos que permitan lograr los objetivos de seguridad identificados</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento visión de seguridad
• Documento de activos de seguridad
• Documento de objetivos de seguridad
• Documento de Valoración del Riesgo [VF]</td><td colspan="2">Productos de Trabajo:
• Documento de especificación de Requisitos de Seguridad
--Descripción de contramedidas/medidas de salvaguarda
--Criterios de seguridad y métricas de seguridad
--Pruebas de seguridad</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se tienen descritos todos los requisitos de seguridad, sus criterios y métricas a lograr, así como las respectivas pruebas para determinar que efectivamente se lograron implementar las medidas de seguridad.</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 6.1</td><td colspan="3">Relevancia de Amenazas</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos del Trabajo:
• Documento : Visión de Seguridad
• Documento: Activos de Seguridad
• Documento Objetivos de Seguridad
• Documento de valoraciones del SI</td><td colspan="2">Productos del Trabajo:
• Documento con los objetivos priorizados</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Analizar la relevancia de cada objetivo de seguridad junto con sus amenazas que impliquen más riesgo</td><td>• Foros con todos los involucrados para discutir la relevancia de la amenaza</td><td></td><td></td></tr>
<tr><td>Actividad 6.2</td><td colspan="3">Identificación de Requisitos que mitiguen las amenazas</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos del Trabajo:
• Documento visión de seguridad
• Documento de activos de seguridad
• Documento de objetivos de seguridad
• Documento con las valoraciones realizadas</td><td colspan="2">Productos del Trabajo:
• Documento de Requisitos</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Revisar las posibles restricciones sobre las operaciones que se</td><td>• Repositorios con requisitos de seguridad</td><td></td><td></td></tr>
</table>

<table>
<tr><td colspan="2">6</td><td colspan="2">Práctica</td></tr>
<tr><td>podrían aplicar
• Revisar qué requisitos pueden mitigar las amenazas identificadas</td><td></td><td></td><td></td></tr>
<tr><td>Actividad 6.3</td><td colspan="3">Especificación y modelación de requisitos</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos del Trabajo:
• Documento de Requisitos</td><td colspan="2">Productos del Trabajo:
• Documento de requisitos de seguridad [V2]</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Modelar los requisitos de seguridad obtenidos con el sistema
• Identificar las relaciones de trazabilidad y dependencias que pudiera arrojar el modelado</td><td>• Casos de uso de seguridad
• Casos de mal uso</td><td></td><td></td></tr>
<tr><td>Actividad 6.4</td><td colspan="3">Redacción del documento de especificación de requisitos de seguridad</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos del Trabajo:
• Documento de requisitos de seguridad [V2]</td><td colspan="2">Productos del Trabajo:
• Documento de especificación de requisitos</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Determinación de los criterios de seguridad para verificar los requisitos
• Establecimiento de métricas de seguridad y su nivel mínimo aceptable
• Especificación de pruebas para la validación
• Esbozar las medidas de salvaguarda / contramedidas</td><td>• Realización de pruebas con base en los casos de abuso.
(B ST-ST-3.5)
• Uso de Pen Testing</td><td></td><td>• Realizar pruebas de seguridad durante el desarrollo, pudiendo hacer uso de automatización.
(S V-PS-2)
• Análisis dinámico (Tiempo real) -- (M-SDL)</td></tr>
</table>

VIII.2.7 PRIORIZACIÓN DE REQUISITOS DE SEGURIDAD

TABLA VIII.10 "PRÁCTICA PRIORIZACIÓN DE REQUISITOS DE SEGURIDAD"

<table>
<tr><td colspan="2">7</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Priorización de Requisitos de Seguridad</td></tr>
<tr><td colspan="4">Prácticas Relacionadas de los marcos y estándares:</td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Obtener los requisitos de seguridad categorizados y priorizados de acuerdo a los objetivos de seguridad</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento visión de seguridad
• Documento de valoración del riesgo
• Documento de requisitos de seguridad [V2]</td><td colspan="2">Productos de Trabajo:
• Documento de requisitos de seguridad [V3]</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se tiene un documento con los requisitos de seguridad categorizados y priorizados</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 7.1</td><td colspan="3">Priorización de requisitos</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento de valoración del riesgo
• Documento de requisitos de seguridad [V2]</td><td colspan="2">Productos de Trabajo:
• Documento de requisitos de seguridad [V3]</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Priorizar los requisitos de seguridad de acuerdo a las medidas provistas por la actividad.
• Resolver y negociar los conflictos que haya entre los requisitos</td><td>• Asignación numérica
• Técnicas de clasificación de requisitos de seguridad</td><td></td><td>• Clasificación de los requisitos de seguridad por categoría
• Priorización en función del impacto y probabilidad de ocurrencia
• Impacto económico de las medidas de salvaguarda a implementar
• Grupos de requisitos: Crítico, estándar y óptimo</td></tr>
</table>

VIII.2.8 INSPECCIÓN DE REQUISITOS DE SEGURIDAD

TABLA VIII.11 "PRÁCTICA INSPECCIÓN DE REQUISITOS DE SEGURIDAD"

<table>
<tr><td colspan="2">8</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Inspección de requisitos de Seguridad</td></tr>
<tr><td colspan="4">Prácticas Relacionadas de los marcos y estándares:</td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Analizar los requisitos de seguridad para comprobar que estén estructurados adecuadamente</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento: Requisitos de seguridad [V3]
• Documento visión de seguridad</td><td colspan="2">Productos de Trabajo:
• Documento: Requisitos de seguridad [V4]</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se cuenta con los requisitos de seguridad consistentes sin redundancias ni ambigüedades.</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 8.1</td><td colspan="3">Análisis de los requisitos</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento: Requisitos de seguridad [V3]</td><td colspan="2">Productos de Trabajo:
• Documento: Requisitos de seguridad [V4]</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Revisar los requisitos para encontrar redundancias y ambigüedades.
• Redacción del documento de fundamentación de requisitos de seguridad</td><td>• Clases de aseguramiento de los CC (ASE)
• IEEE 830-1998</td><td></td><td>• Los requisitos deben de ser correctos, no ambiguos, completos y consistentes, ordenados por importancia, verificables, modificables y trazables.</td></tr>
</table>

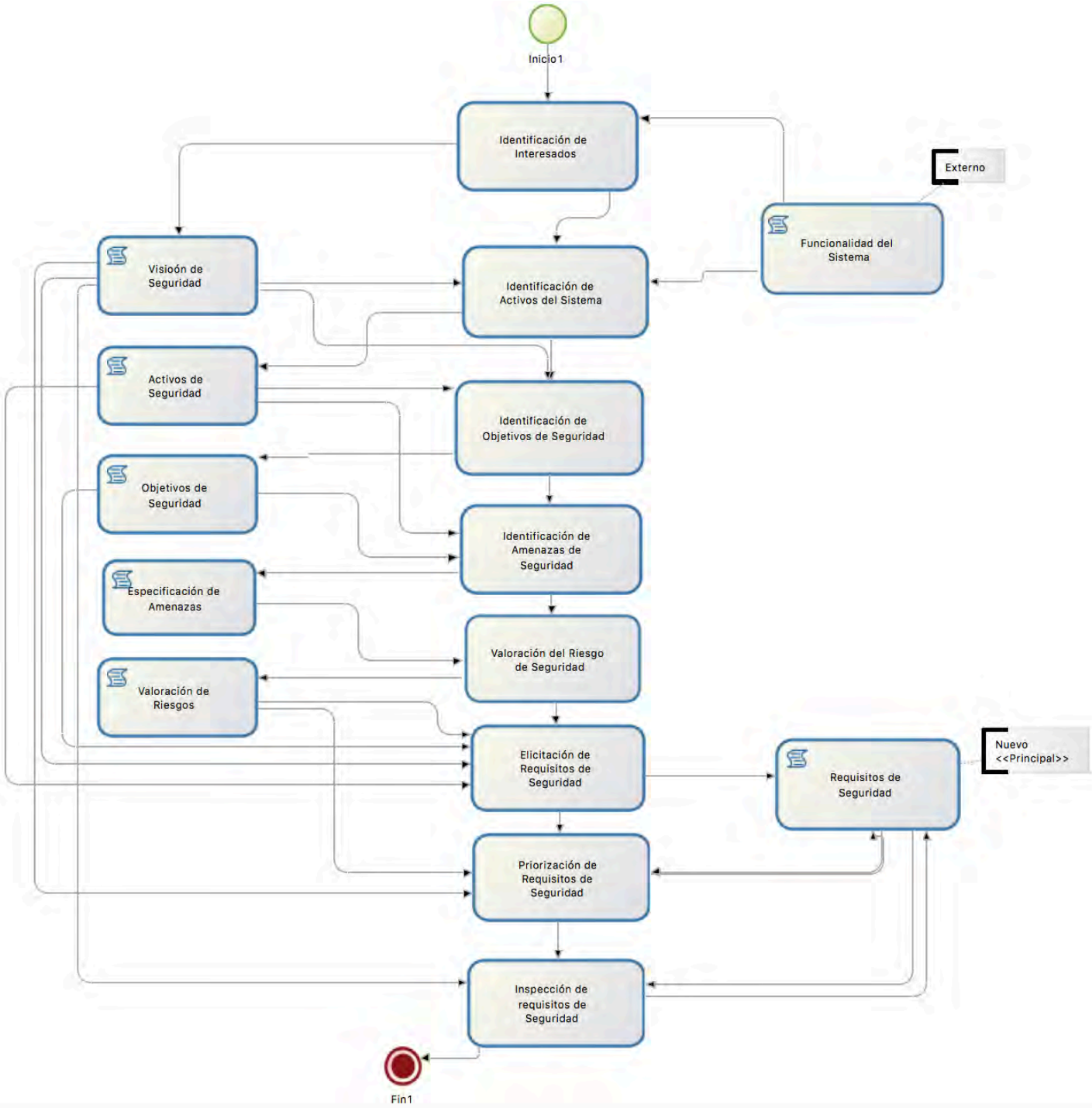


Figura VIII.2 "RELACIÓN ENTRE LAS ACTIVIDADES DEL SUB-ALFA *EVALUACIÓN DE RIESGOS DE SEGURIDAD*"

CAPÍTULO IX. ALFA: SISTEMA DE SOFTWARE

Para la inclusión de medidas de seguridad en el *Alfa de Sistema de Software* se propone agregar ítems extras en las listas de verificación 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 con medidas de seguridad incluidas y adicionalmente cuenta con la verificación en las fases de liberación, operación y concluyen con el retirado seguro del software

Se proporciona a continuación la lista de verificación con aspectos de seguridad que deben ser cubiertos para cada Estado, así como los aspectos de seguridad que se ven inmiscuidos en su realización:

TABLA IX.1 "LISTA DE VERIFICACIÓN GENERAL Y DE SEGURIDAD DEL ALFA DE SISTEMA DE SOFTWARE"

Estados Sistema de Software	Verificación General	Verificación de Seguridad
Con arquitectura seleccionada	• Se seleccionó la arquitectura que trata los riesgos técnicos clave. • Se acordaron los criterios para seleccionar la arquitectura. • Se seleccionaron las plataformas, tecnologías y lenguajes. • Se tomaron las decisiones de compra, construcción y rehusó.	• 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

Estados Sistema de Software	Verificación General	Verificación de Seguridad
		y preciso
Demostrable	• Se demostraron las características clave de la arquitectura. • Los interesados relevantes acordaron que la arquitectura es apropiada. • Se ejercieron la interfaz crítica y las configuraciones del sistema.	• 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 o Se revisaron las funciones, despreciando las inseguras
Usable	• El sistema es usable y tiene las características de calidad deseadas. • Los usuarios pueden operar el sistema. • Se aceptaron los niveles de defectos. • Se conoció el contenido de liberación.	• 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	• Se puso a disposición la documentación de usuario. • Los representantes de los interesados aceptaron el sistema. • Los representantes de los interesados quieren que se haga operacional el sistema.	• 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
Operacional	• El sistema se usó en un ambiente operacional. • El sistema está disponible para los usuarios previstos. • Al menos un ejemplo del sistema está completamente operacional.	• La documentación de seguridad está actualizada y verificada • Las actualizaciones y monitoreo de la configuración se realizan periódicamente • La ejecución del plan de

Estados Sistema de Software	Verificación General	Verificación de Seguridad
	• El sistema es compatible con los niveles de servicio acordados.	respuesta a incidentes se ha realizado satisfactoriamente de acuerdo a los lineamientos
Retirado	• No se da más soporte al sistema. • No se producirán más actualizaciones al sistema. • Se reemplazó o se descontinuó el sistema.	• 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

Donde estas dos actividades impactan en tres de los catorce aspectos de seguridad identificados anteriormente, siendo:

1. Normativas y Regulaciones
2. Control de Procesos
3. Requisitos

IX.1 PRÁCTICAS ASOCIADAS A LA ALFA SISTEMA DE SOFTWARE

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. Retirado Seguro del Sistema

Ellas permiten a los usuarios poder comprender a fondo las actividades necesarias a realizar para poder lograr con éxito el estado del Alfa.

-

IX.1.1 SELECCIÓN DE LA ARQUITECTURA DE SEGURIDAD

TABLA IX.2 "PRÁCTICA SELECCIÓN DE LA ARQUITECTURA DE SEGURIDAD"

<table>
<tr><td colspan="2">9</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Selección de la Arquitectura de Seguridad</td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Seleccionar la arquitectura a utilizar en el sistema de acuerdo a las necesidades identificadas.</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento visión de seguridad</td><td colspan="2">Productos de Trabajo:
• Arquitectura de seguridad seleccionada</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se tiene la arquitectura que se implementara en el sistema.</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 9.1</td><td colspan="3">Selección de la Arquitectura</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Documento visión de seguridad</td><td colspan="2">Productos de Trabajo:
• Arquitectura de seguridad seleccionada</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Revisión de las funciones de seguridad
• Realizar la revisión del diseño para el sistema
• Definir y usar un análisis de la arquitectura</td><td>• Estandarización de las descripciones de la arquitectura
(B ST-AA-2.2)</td><td></td><td></td></tr>
</table>

IX.1.2 IMPLEMENTACIÓN DEL SISTEMA

TABLA IX.3 "PRÁCTICA IMPLEMENTACIÓN DEL SISTEMA"

<table>
<tr><td colspan="2">10</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Implementación del sistema</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Realizar la implementación del sistema a su entorno de acuerdo a las medidas de seguridad establecidas</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Plan de seguridad</td><td colspan="2">Productos de Trabajo:
• Plan de seguridad [V2]
• Documento de Implementación del Sistema
• Sistema implementado en su entorno</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se implementó el sistema de forma segura y se aseguró su correcta implantación en su entorno de acuerdo a los parámetros establecidos.</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 10.1</td><td colspan="3">Implantación del sistema</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Plan de seguridad
(Que identifica a los actores clave, las restricciones del proyecto, los componentes básicos, el alcance de las pruebas y el nivel de rigor esperado.)</td><td colspan="2">Productos de Trabajo:
• Documento de Implementación del Sistema
o Informe de evaluación de seguridad
o Informe de autorización final de seguridad de la implementación
o Sistema implantado en su entorno</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Revisión de medidas de seguridad del entorno de operación
• Evaluación de resultados de pruebas de seguridad de implantación del sistema
• Revisión de medidas de seguridad en el entorno de producción
• Autorización documentada para la implantación del sistema</td><td>• Lista verificada de controles operativos de seguridad
(N I 3.2.1)</td><td></td><td></td></tr>
</table>

IX.1.3 RETIRADO SEGURO DEL SISTEMA

TABLA IX.4 "PRÁCTICA RETIRADO SEGURO DEL SISTEMA"

<table>
<tr><td colspan="2">11</td><td colspan="2">Práctica</td></tr>
<tr><td colspan="4">Retirado Seguro del Sistema</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Propósito</td></tr>
<tr><td colspan="4">Realizar el retiro del sistema de manera adecuada</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Resultado</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Plan de seguridad
→Plan de disposición / Transición</td><td colspan="2">Productos de Trabajo:
• Documento del cierre del sistema
• Sistema retirado de su entorno</td></tr>
<tr><td colspan="4">Criterios de finalización</td></tr>
<tr><td colspan="4">Se retiró el sistema de forma segura y se tiene la documentación respectiva</td></tr>
<tr><td colspan="4">Guía</td></tr>
<tr><td>Actividad 11.1</td><td colspan="3">Retiro del sistema</td></tr>
<tr><td colspan="2">Entrada</td><td colspan="2">Salida</td></tr>
<tr><td colspan="2">Productos de Trabajo:
• Plan de seguridad
→Plan de disposición / Transición</td><td colspan="2">Productos de Trabajo:
• Documento cierre del sistema
o Registros de sanitización de medios
o Registros de disposición del Hardware y Software
o Registros de verificación del cierre del sistema
• Sistema retirado de su entorno</td></tr>
<tr><td>Tareas</td><td>Herramientas</td><td>Competencias</td><td>Medidas</td></tr>
<tr><td>• Asegurar la preservación de la información
• Desinfectar los medios
• Deshacerse del hardware y software
• Cerrar el sistema</td><td>•</td><td></td><td>•</td></tr>
</table>

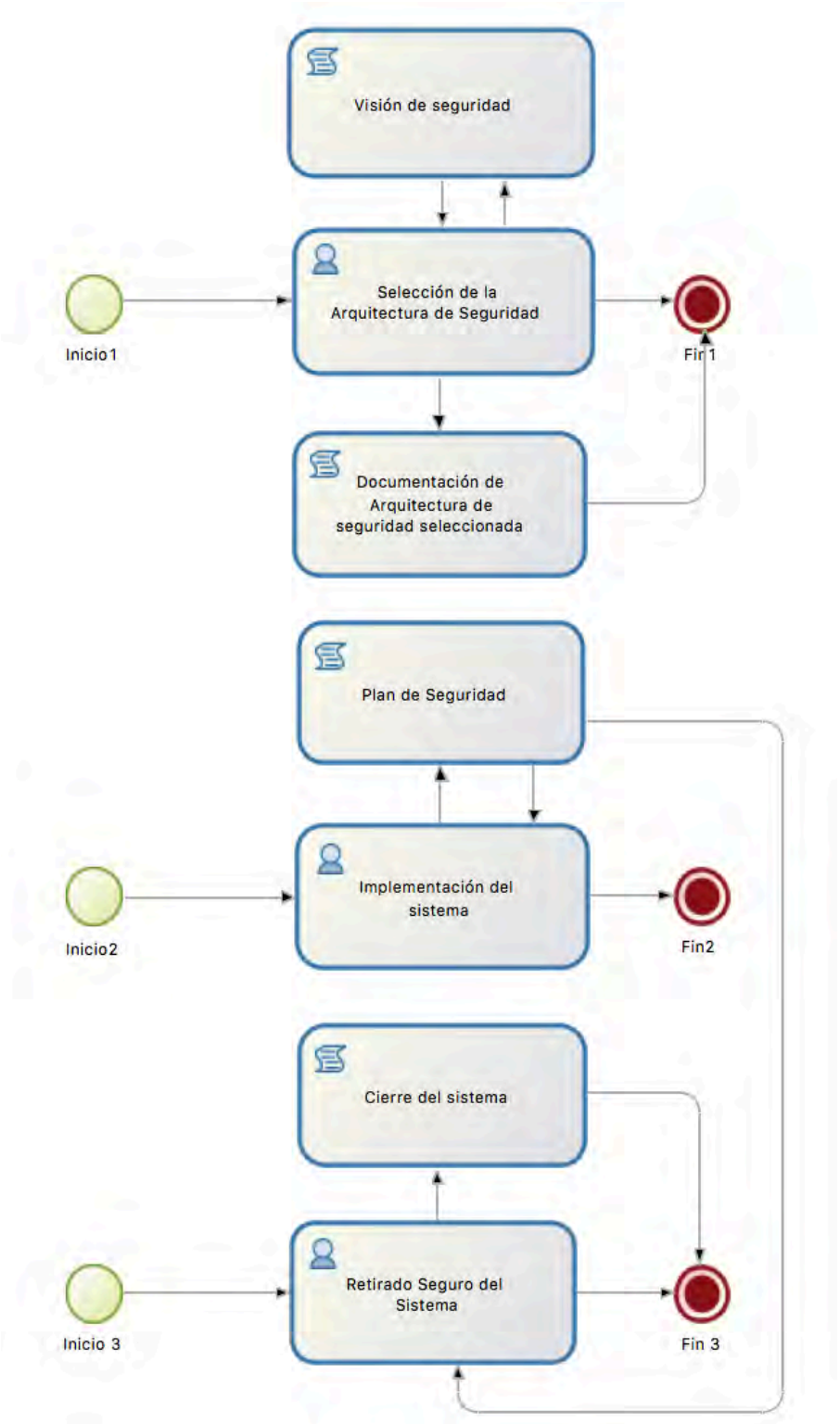


FIGURA IX.3 "RELACIÓN ENTRE LAS ACTIVIDADES DEL ALFA *SISTEMA DE SOFTWARE*"

CAPÍTULO X. ALFA: TRABAJO

Para la inclusión de medidas de seguridad en el Alfa de Trabajo se propone la inclusión de ítems extras en las listas de verificación de los Estados a los ya establecidos por la Esencia, permitiendo establecer los principios con los que trabajará el equipo, permitiendo realizar una capacitación y orientación de acuerdo a los principios establecidos; así mismo se verifica la correcta selección de herramientas de desarrollo, middlewares y bibliotecas para que no representen algún riesgo de seguridad para el proyecto.

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

- Entrenamiento
- Normas y Regulaciones
- Estandarizaciones

La selección de esta Alfa para la inclusión de aspectos de seguridad es vital dado que es en ella donde se define lo que debe de realizar para cumplir con todos objetivos para producir un sistema que esté conforme a los requisitos pactados y represente una solución clara para los interesados. Esto se logra gracias a las prácticas que conforman la selección de herramientas que ayudarán al equipo de desarrollo a realizar de forma segura el desarrollo del sistema.

Se proporciona a continuación la lista de verificación con aspectos de seguridad para cada estado del Alfa de Trabajo, así como una lista con los aspectos de seguridad que se ven inmiscuidos en el proceso.

TABLA X.1 "LISTA DE VERIFICACIÓN GENERAL Y DE SEGURIDAD DEL ALFA DE TRABAJO"

Estados Trabajo	Verificación General	Verificación de Seguridad
Iniciado	• Es claro el resultado esperado del trabajo que se iniciará. • Están identificadas claramente las limitaciones en la ejecución del trabajo. • Se conoce a los Stakeholders que financiarán el trabajo. • Está claramente identificado el inicio de las labores. • Se conoce a los Stakeholders que validarán los resultados. • La fuente de financiamiento es clara. • La prioridad del trabajo es clara.	• Se tiene claro las normas regulatorias que se deben de considerar • Se identificaron los operadores de datos críticos • Se comprende el ambiente operativo del sistema de software y sus componentes.
Preparado	• Se ha hecho el compromiso. • Se ha estimado costo y el esfuerzo del trabajo. • Se ha entendido la	• Se publica y explica el proceso que se seguirá (roles, responsabilidades, plan) • Se entiende el esquema de

Estados Trabajo	Verificación General	Verificación de Seguridad
	disponibilidad recursos • Son claras las políticas y procedimientos de gobernanza. • Los riesgos a los que se expone el trabajo son claros. • Los criterios de aceptación están definidos y acordados con el cliente. • Se ha dividido el trabajo lo suficiente para dar inicio al trabajo productivo. • Las tareas se han identificado y priorizado por el equipo y los stakeholders. • Se ha definido un plan confiable • Se tienen los recursos financieros para iniciar el trabajo. • El equipo o algunos miembros están listos para iniciar trabajo. • Se han definido los puntos de integración y entrega.	clasificación de datos y funciones del sistema • El desarrollo del sistema se está realizando de una forma segura por parte del grupo
Comenzado	• Se comenzó el trabajo de desarrollo • Se monitorea el proceso de desarrollo. • Se hizo la división en ítems accionables con una clara definición. • Los miembros del equipo están aceptando y progresando en los ítems de trabajo.	• Se monitorea el desarrollo del sistema de acuerdo al plan de acción • Se está implementando la estandarización de codificación segura
Bajo control	• El trabajo va bien; se están manejando los riesgos. • El trabajo y el re-trabajo no planeados están bajo control. • Se completaron los ítems de trabajo dentro de los estimados. • Se hizo seguimiento de las mediciones.	
Concluido	• Se terminó el trabajo que produce resultados. • Se están consiguiendo los resultados del trabajo. • El cliente aceptó el sistema de software resultante.	• Los interesados han validado que las medidas de seguridad pactadas han sido correctamente implementadas en el sistema de software
Cerrado	• Todas las tareas de limpieza de remanentes se completaron y el	

Estados Trabajo	Verificación General	Verificación de Seguridad
	trabajo se cerró oficialmente • Todo se archivó • Se dispone de lecciones aprendidas y métricas	

Cabe mencionar que para esta Alfa en particular no es necesaria la profundización de las listas de verificación dado su contenido, es por ello que no se muestran ninguna Sub-Alfa o prácticas asociadas.

CAPÍTULO XI. ALFA: FORMA DE TRABAJO

Para la inclusión de medidas de seguridad en el Alfa de Forma de Trabajo se propone la inclusión de ítems extras en las listas de verificación de los Estados a los ya establecidos por la Esencia, donde se revisa principalmente todas las normas a considerar a la hora de desarrollar el software como son las regulatorias y los estándares, la definición de roles, responsabilidades, revisa la correcta manipulación de los datos críticos que utilizara el sistema y se realiza el seguimiento integral para verificar su implementación.

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

- Entrenamiento
- Herramientas
- Normas y Regulaciones
- Estandarizaciones
- Automatizaciones

Todos estos aspectos son necesarios de considerar en esta Alfa ya que en ella el equipo desarrolla su forma de trabajar junto con la comprensión de su misión en el proyecto y su entorno de trabajo, lográndose gracias al conjunto de prácticas y herramientas seleccionadas por el equipo para guiar y apoyar su trabajo. Teniendo la posibilidad que a medida que su trabajo va avanzando, se tenga la posibilidad de reflexionar continuamente sobre su manera de trabajar, adaptándose a su contexto actual y de ser necesario modificar su proceder.

Se proporciona a continuación la lista de verificación con aspectos de seguridad para cada estado del Alfa de Forma de Trabajo, así como una lista con los aspectos de seguridad que se ven inmiscuidos en el proceso.

TABLA XI.1 "LISTA DE VERIFICACIÓN GENERAL Y DE SEGURIDAD DEL ALFA DE FORMA DE TRABAJO"

Estados Trabajo	Verificación General	Verificación de Seguridad
Con principios establecidos	• El equipo asume los principios y limitaciones. • Los stakeholders están de acuerdo con los principios y limitaciones establecidas. • Se han acordado a las prácticas de trabajo utilizadas con los stakeholders. • Se han acordado las herramientas de trabajo utilizadas con los stakeholders. • Si tiene una propuesta de acercamiento. • Se entiende el contexto de trabajo del equipo. • Se conocen las limitaciones que	• Se tienen claras cuáles son las funciones al ser inseguras no pueden implementarse en el proyecto • Se realizó la capacitación integral de acuerdo al tipo de proyecto identificado. • Se tiene un repositorio de consulta de temas de programación segura y su correcta implementación • Se acordó el plan de formación de seguridad

Estados Trabajo	Verificación General	Verificación de Seguridad
	se aplican en el uso de prácticas y herramientas. • Se conocen las limitaciones del equipo que definen la adquisición de prácticas y herramientas.	
Con bases establecidas	• Se han seleccionado las prácticas y herramientas clave de la forma de trabajo. • El equipo ha acordado todas las prácticas de trabajo. • El equipo ha identificado todas las prácticas y herramientas no-negociables. • Se han analizado los vacíos que existen entre la capacidad que se necesita para ejecutar la forma de trabajo deseada y los niveles de capacidad del equipo. • Las prácticas y herramientas seleccionadas se han integrado para formar una forma de trabajo factible.	• Se realizó la capacitación integral de acuerdo al tipo de proyecto identificado. • Las herramientas seleccionadas cubren las medidas de seguridad requeridas • Se cuenta con alguna herramienta para la automatización de la revisión del código • Se hace uso marcos de trabajo middleware y bibliotecas comunes para utilizarse en todos los desarrollos. • El equipo de trabajo comparte la necesidad del entrenamiento integral
En uso	• Algunos miembros del equipo están usando la forma de trabajo • Se inspeccionó regularmente el uso de prácticas y herramientas • El equipo está adaptado y apoyando las prácticas y herramientas • Los procedimientos están en su lugar para manejar retroalimentación	• Se alimenta con los resultados al sistema de gestión y mitigación de defectos.
En su lugar	• Todos los miembros del equipo están usando la forma de trabajo • Todos los miembros tienen acceso a las prácticas y herramientas para hacer su trabajo • El equipo completo se involucró en la inspección y adaptación de la forma de trabajo	
Trabajando bien	• Todos los miembros del equipo están usando la forma de trabajo. • Todos los miembros tienen	

Estados Trabajo	Verificación General	Verificación de Seguridad
	acceso a las prácticas y herramientas para hacer su trabajo. • El equipo completo se involucró en la inspección y adaptación de la forma de trabajo.	
Retirado	• El equipo no usa más la forma de trabajo • Se compartieron las lecciones aprendidas para el uso futuro	

Cabe mencionar que para esta Alfa en particular no es necesaria la profundización de las listas de verificación dado su contenido, es por ello que no se muestran ninguna Sub-Alfa o prácticas asociadas.

RESUMEN ESSENCE SEC

Al concluir de definir las bases que presenta Essence Sec el lector tendrá la posibilidad de detectar aquellos aspectos de seguridad que se tienen que considerar a lo largo de todo el ciclo de vida de desarrollo y haciendo énfasis en la necesidad de implementarlo desde un inicio del desarrollo ya que esto incrementa el éxito de la inclusión de las medidas de seguridad además que reduce el re-trabajo posterior lo que incrementaría exponencialmente los gastos de desarrollo.

Es así que se cuentan con 4 Alfas donde se implementaron los 14 aspectos de seguridad identificados en Capítulo IV que son:

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

Dentro del Alfa de *Requisitos* se cuentan con:

- 10 aspectos de verificación dentro de los Estados del Alfa.
- 1 Sub-Alfa llamada "*Evaluación de Riesgos de Seguridad*".
    - 23 aspectos de verificación dentro de los Estados del Sub-Alfa
- Se cuentan con 8 prácticas
    1. Identificación de los Interesados / Acuerdo de las definiciones
    2. Identificación de activos
    3. Identificación de objetivos de seguridad
    4. Identificación de amenazas
    5. Valoración del riesgo
    6. Elicitación de requisitos
    7. Priorización de requisitos
    8. Inspección de requisitos

Dentro del Alfa de *Sistema de Software* se cuentan con:

- 21 aspectos de verificación dentro de los Estados del Alfa.
- Se cuentan con 3 prácticas
    1. Selección de la Arquitectura de Seguridad

2. Implementación del sistema
3. Retirado Seguro del Sistema

Dentro del Alfa de *Sistema de Software* se cuentan con:

- 9 aspectos de verificación dentro de los Estados del Alfa.

Dentro del Alfa de *Forma de Trabajo* se cuentan con:

- 9 aspectos de verificación dentro de los Estados del Alfa.

En total forman 72 aspectos que se tienen que considerar a lo largo de las 4 Alfas y 1 Sub-Alfa, así mismo se tienen 11 prácticas complementarias que servirán de apoyo para la correcta aplicación de los aspectos de seguridad dentro del proceso de desarrollo del software.

CAPÍTULO XII. CASO PRÁCTICO

En este Capítulo se presenta el método de trabajo que se ha utilizado para conseguir los objetivos planteados para este trabajo de investigación. Se ha considerado el uso del Método Investigación-Acción (Action - Research) por ser uno de los principales métodos de investigación cualitativa en el campo de los sistemas de información y en la Ingeniería de software (Ruiz et al., 2002), este servirá para realizar la verificación de Essence Sec descrita en el Capítulo VII , el cuál es el producto fundamental de este trabajo de investigación .

XII.1 OBJETIVO DEL CASO PRÁCTICO

Los objetivos del caso se centraron en la evaluación de que tan pertinente, factible y competente es Essence Sec. Estas características se evaluaron a través de la resolución de las siguientes preguntas:

- ¿Los conceptos presentados en las listas de verificación de seguridad de las Alfas fueron pertinentes?
- ¿Los conceptos presentados en las listas de verificación de seguridad de las Alfas fueron adecuados?
- ¿Los conceptos presentados en las listas de verificación de seguridad de las Alfas están expresados en términos que se utilizan en el contexto cotidiano?
- ¿Es necesario la inclusión de otros aspectos de verificación no especificados actualmente?

Esta serie de preguntas permitirán definir si se aceptan o rechazan los ítems de las listas de verificación de Essence Sec, permitiendo conocer la factibilidad de uso dentro de las organizaciones.

XII.2 MÉTODO INVESTIGACIÓN - ACCIÓN

En la actualidad existen diversos métodos de investigación cualitativa, pero el que comúnmente se utiliza en los Sistemas de Información e Ingeniería de Software es “Investigación - Acción”. El término proviene del Autor Kurt Lewin (1946) con el que describía una forma de investigación que podía enlazar el enfoque experimental de las ciencias sociales con programas de acción social que respondieran a los problemas sociales de aquella época. Mediante el método, Lewin argumentaba que se podían lograr de forma simultánea avances teóricos y cambios en la sociedad; es así que este método ha obtenido una amplia aceptación y aplicación en la investigación en la Ingeniería de Software en los últimos años , desde que fue introducida por Wood-Harper (1985).

Existen diversas definiciones de Investigación - Acción. Algunas de las más significativas son las siguientes:

> Para Wadsworth (1998) consiste en la participación de “todas las partes involucradas en la investigación, examinando la situación existente (Problemática), con los objetivos que cambiarla y mejorarla”.
>
> Para French y Bell (1999) es el “Proceso de recopilar de forma sistemática datos de investigación acerca de un sistema actual en relación con algún objetivo, meta o

necesidad de ese sistema; de alimentar de nuevo con esos datos al sistema; de emprender acciones por medio de variables alternativas seleccionadas dentro del sistema, basándose tanto en los datos como en las hipótesis; y de evaluar los resultados de la acciones, recopilando datos adicionales".

Realizando un análisis a profundidad, Wadsworth (1998) realiza una identificación de cuatro tipos de roles que se utilizan dentro de este método (Cabe mencionar que en ocasiones la misma persona o equipo puede desempeñar más de un rol):

- El investigador, es aquel individuo o grupo que lleva a cabo de forma activa el proceso investigador.
- El objeto investigado, es decir, el problema a resolver.
- El grupo crítico de referencia, aquel para quien se investiga desde la perspectiva de que se tiene un problema que necesita ser resuelto y que también participa en el proceso de investigación. En el existen personas que saben que están participando en la investigación, como otras que participan sin saberlo.
- El beneficiario, es aquel para quien se investiga en el sentido de que puede beneficiarse del resultado de la investigación, aunque no participa directamente en el proceso. Puede ser el receptor de documentos, informes, etc.

Un proceso de investigación que emplea Investigación - Acción se compone de grupos de actividades organizadas formando un ciclo característico. Padak y Padak (1994) identifican los siguientes pasos, que deben seguirse en las investigaciones que utilicen este método:

1. Planificación:

   Identificar las cuestiones relevantes, que guiarán la investigación, que deben estar directamente relacionadas con el objeto que se está investigando y ser susceptibles de encontrarles respuesta. En esta actividad se buscan caminos alternativos, líneas a seguir o reforzar algo existente. El resultado es que se definen claramente otros problemas o situaciones a tratar.
2. Acción:

   Variación de la práctica, cuidadosa, deliberada y controlada. Se efectúa una simulación o prueba de la solución. Es cuando el investigador interviene sobre la realidad.
3. Observación:

   Es recoger información, tomar datos, documentar lo que ocurre. Esta información puede proceder prácticamente de cualquier sitio (bibliografía, medidas, resultados de pruebas, observaciones entrevistas, documentos, etc.). También se le conoce como "Evaluación".
4. Reflexión

   Es el compartir y analizar los resultados con el resto de los interesados, de tal manera que se invierte el planteamiento de nuevas cuestiones relevantes y, como añade Wadsworth (1998), "A profundizar en la materia que se está investigando para proporcionar conocimientos nuevos que puedan mejorar las prácticas, modificando éstas como parte del propio proceso investigador, para luego volver a investigar

sobre estas prácticas una vez modificadas". También conocida COMO "Especificación del aprendizaje"

XII.3 DESCRIPCIÓN GENERAL DEL CASO PRÁCTICO

En este apartado se presenta un Caso de Práctico realizado donde se aplica Essence Sec anteriormente descrito, siguiendo el método de Investigación-Acción. En primer lugar, el Paso de Planificación, describirá el propósito del Caso Práctico, posteriormente se presentará a la organización que ayudará a realizar el Caso; esta organización fue seleccionada ya que se dedica al desarrollo de sistemas en un entorno crítico por lo que es factible el validar el funcionamiento de Essence Sec. En paso de Acción se presenta el estudio realizado a la Esencia a través de la revisión de las actividades que realiza la organización. Posteriormente en el punto de Observación se podrá revisar los resultados obtenidos en el proceso de acción y finalmente en el punto de Reflexión se obtendrán las conclusiones y lecciones aprendidas gracias al Caso Práctico.

XII.3.1 PLANIFICACIÓN

Debido al tipo de proyecto presentado en el caso práctico, es necesario mantener la confidencialidad en ciertos detalles de la forma de trabajar de la organización, se omitirán detalles específicos de los aspectos de seguridad existentes, de la forma de trabajar, así como el detalle de algunos resultados obtenidos al hacer uso de Essence Sec.

El Caso Práctico que se presenta es un caso representativo de la forma en que se desarrollan los proyectos para la creación y mantenimiento de Sistemas de Información donde la seguridad es un aspecto crucial, debido a la criticidad de los datos que se manejan dentro de la organización dedicada a temas de justicia; ello permite que con la experiencia que se tiene al desarrollar sistemas con características de seguridad incluidas puedan hacer una verificación de Essence Sec con la finalidad de mejorar la propuesta así como identificar si es factible su uso en las organizaciones de TI.

El Área de Tecnologías de la Información y Comunicaciones tiene como objetivo el apoyar a través de la implantación y utilización de nuevas tecnologías en todas las áreas de la organización. Con base en la utilización de las herramientas tecnológicas y de la sistematización, se busca lograr un mayor control y seguridad de la información, generando también oportunidad en la misma, y una mejora en la toma de decisiones, para en general, coadyuvar en una mejor impartición de justicia y en el mejoramiento de los procedimientos administrativos.

Entre las actividades que lleva a cabo, están las relacionadas a implementación de infraestructura tecnológica, redes, desarrollo de sistemas, sitios Web, servicios y mantenimiento a equipos, diseño y atención a eventos y audiencias apoyando con audio y video, entre otras.

El Departamento de Desarrollo de Software es el encargado de diseñar, programar e implementar software para las diversas áreas de la Institución. Así como mantener, modificar y añadir módulos a sistemas implementados anteriormente. Además de atender todos los servicios solicitados por usuarios, relacionados al uso de los programas desarrollados.

Es parte del objetivo del Departamento asegurar el buen uso de los sistemas y el control de usuarios y que dichos sistemas solucionen de una manera óptima los requerimientos de las áreas usuarias en cuanto a captura, organización, consultas y reportes de su información.

Este Caso Práctico se hará el análisis de la pertinencia de lo propuesto por Essence Sec y la forma de trabajo del Departamento de Desarrollo de Software. Se verificarán cuáles de las actividades identificadas en Essence Sec son realizadas por el departamento; eso permitirá comparar y determinar aquellos aspectos que se realizan, aquellos que ocasionalmente se cumplen y también poder determinar las posibles mejoras a Essence Sec.

XII.3.2ACCIÓN "ANÁLISIS DEL PROCESO ESSENCE SEC"

Para llevar a cabo el proceso de análisis y validación de Essence Sec a través del Departamento de Desarrollo se procedió a realizar una serie de entrevistas donde se revisó la estructura que tiene Essence Sec, sus procesos y la secuencia que sigue para poder verificar que efectivamente forman parte de una solución para la adición de aspectos de seguridad a los procesos de Ingeniería de Software.

En la primera entrevista se abordó la explicación de la forma de trabajo de la Esencia para conocer el contexto del trabajo de investigación y posteriormente se presentó la propuesta de investigación "Essence Sec" para su primera revisión.

En la segunda entrevista se realizaron una serie de preguntas para cada una de las Alfas y Sub-Alfas presentadas en Essence Sec con la finalidad de que el Departamento identificara todas aquellas actividades relativas a la inclusión de la seguridad en los procesos de desarrollo de software.

Y se finalizó con una entrevista para realizar la validación de Essence Sec a través de una revisión de cada una de las Alfas y Sub-Alfas expresadas, para identificar si estas se implementan dentro de un proceso de desarrollo, si estas son demasiado específicas y solo corresponderían a un sistema con necesidades más específicas así como las posibles mejoras que se pueden realizar a los aspectos de validación como lo es el orden en que aparecen, mejoramiento de la sintaxis y la segmentación de aspectos para mejorar su comprensión. Por tal motivo se establecieron 3 valores posibles para cada aspecto de verificación:

- Si

  Es factible su implementación y es realizado por el departamento tal y como se presenta actualmente.
- NA

  No es aplicable genéricamente a todos los proyectos, por lo que es necesario revisarlo para aplicarse.
- Mejora

  Existe algún tipo de mejora a realizar al aspecto de verificación

Al finalizar la validación se podrá observar la factibilidad de Essence Sec para su implementación dentro de entornos de desarrollo y se contara con una nueva versión con todas las recomendaciones identificadas.

SUB-ALFA EVALUACIÓN DE RIESGOS DE SEGURIDAD

Estado	Verificación		Comentarios / Modificaciones
Identificación	La visión de seguridad para el proyecto está definida y alineada a las metas del negocio.	Si	
	Se identificaron los activos que están presentes en el sistema.	Si	
	Las dependencias y usuarios que tiene cada activo identificado fueron analizadas.	Si	No todos los usuarios identifican sus dependencias.
	Cada activo identificado forma parte de la visión de seguridad establecida.	Si	
	Se identificaron y comprendieron las amenazas.	Si	En la mayoría de los casos.
	Se modelaron las amenazas identificadas	Si	En la mayoría de los casos.
Valoración	Se estimó el riesgo de las amenazas identificadas.	Si	
	Se realizó un ranking para definir los riesgos prioritarios para el proyecto.	Si	
	Los interesados están de acuerdo con el ranking establecido.	Si	Se expone el riesgo y sus consecuencias, pero ellos tienen la última palabra.
	Los interesados tienen claro la forma en que se mitigarán los riesgos de seguridad identificados.	Si	
	Se estableció las métricas que se deberán cumplir para verificar que se mitigaron los riesgos.	Si	

FIGURA XII.1 "Fragmento de una encuesta realizada en el proceso"

XII.3.3 OBSERVACIÓN

Por tal motivo a continuación se describen el resultado de cada una de las 4 Alfas.

Dentro del Alfa de *Requisitos* se cuentan con:

- 10 aspectos de verificación dentro de los Estados del Alfa.

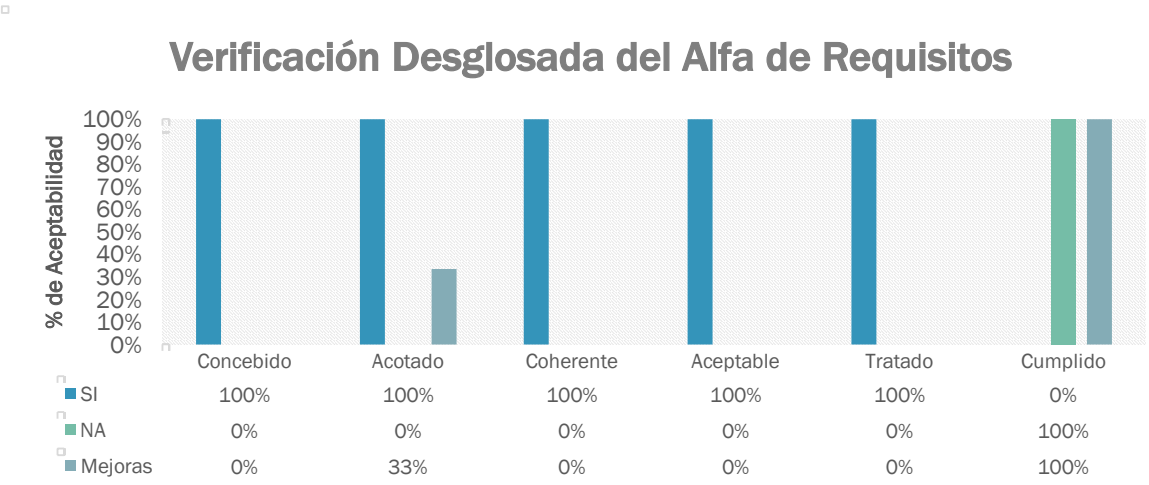


FIGURA XII.1 "RESULTADOS DE LA VERIFICACIÓN DEL ALFA DE REQUISITOS"

De los cuales basados en la figura XII.1:

- El 90% son aceptados tal y como se presentan actualmente.
- El 10% restante, es necesario realizarle algunas adecuaciones.
- Así mismo, se tienen recomendaciones generales de mejora para el 20% de los aspectos de verificación.
- Entre las adecuaciones realizadas fueron:
    - Refinamiento del texto

Por parte del Sub-Alfa *Evaluación de Riesgos de Seguridad*.

- Se cuentan con 23 aspectos de verificación dentro de los Estados del Sub-Alfa

De los cuales basados en la figura XII.2:

- El 83% son aceptados tal y como se presentan actualmente.
- El 17% restante, es necesario realizarle algunas adecuaciones.
    - Siendo el Estado de "Inspección" el que requiere más atención.
- Así mismo, se tienen recomendaciones generales de mejora por el 48% de los aspectos de verificación.
- Entre las adecuaciones realizadas fueron:
    - Cambio de lugar de un punto de verificación.
    - Separación de un punto de verificación para su mejor comprensión.
    - Refinamiento del texto

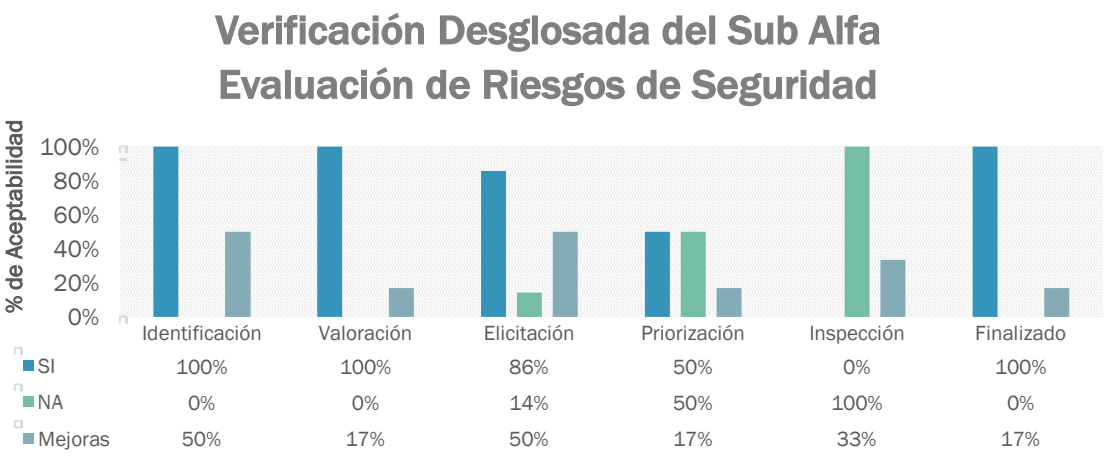


FIGURA XII.2 "RESULTADOS DE LA VERIFICACIÓN DEL SUB ALFA DE EVALUACIÓN DE RIESGOS DE SEGURIDAD¨

Dentro del Alfa de *Sistema de Software* se cuentan con:

- 22 aspectos de verificación dentro de los Estados del Alfa.

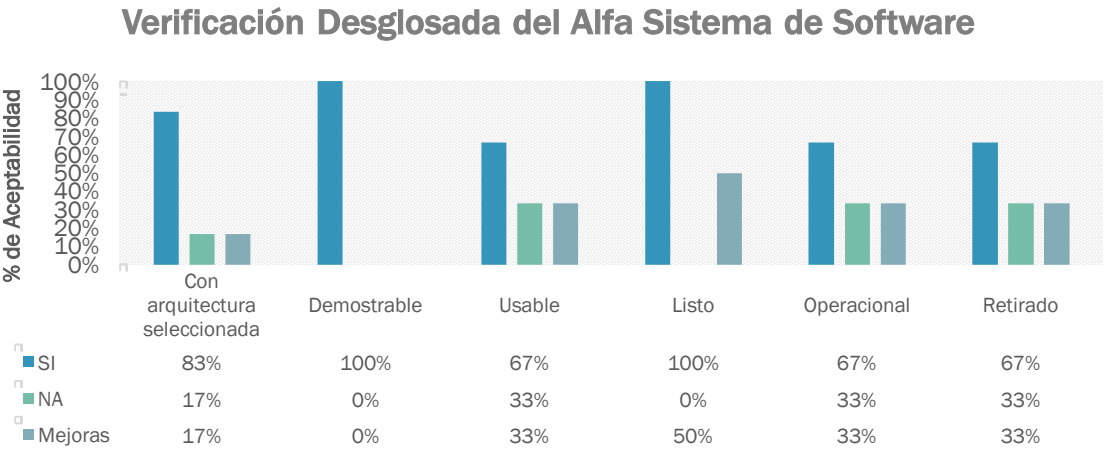


FIGURA XII.3 "RESULTADOS DE LA VERIFICACIÓN DEL ALFA DE SISTEMA DE SOFTWARE¨

De los cuales basados en la figura XII.3:

- El 82% son aceptados tal y como se presentan actualmente.
- El 18% restante, es necesario realizarle algunas adecuaciones.
    - Teniendo 3 Estados que pueden ser refinados para tener una propuesta ad hoc con el trabajo cotidiano, estos son: Usable, Operacional y Retirado.
- Así mismo, se tienen recomendaciones generales de mejora por el 23% de los aspectos de verificación.
- Entre las adecuaciones realizadas fueron:
    - Cambio de lugar de un punto de verificación.
    - Separación de un punto de verificación para su mejor comprensión.

- Refinamiento del texto

Dentro del Alfa de *Sistema de Software* se cuentan con:

- 9 aspectos de verificación dentro de los Estados del Alfa.

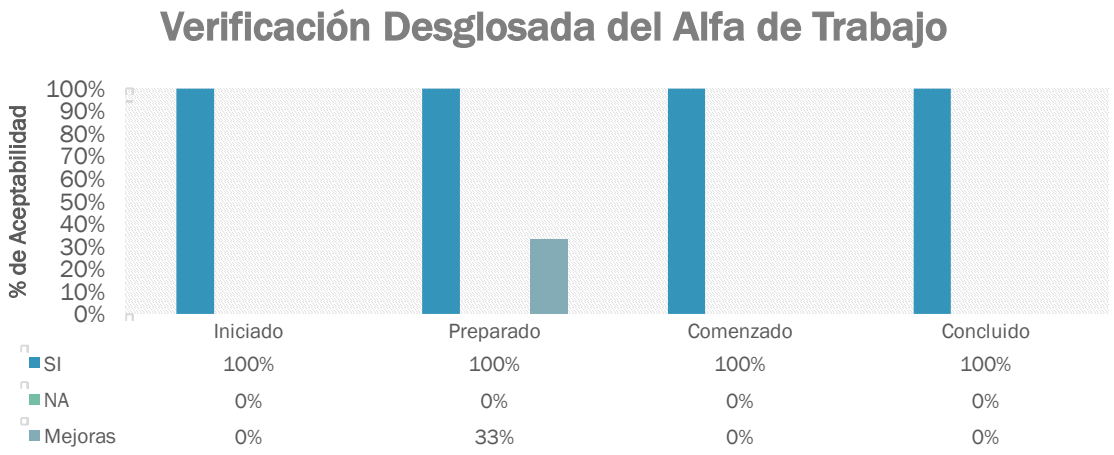


FIGURA XII.4 "RESULTADOS DE LA VERIFICACIÓN DEL ALFA DE TRABAJO"

De los cuales basados en la figura XII.4:

- El 100% son aceptados tal y como se presentan actualmente.
- Así mismo cabe mencionar que se tienen recomendaciones generales de mejora por el 23% de los aspectos de verificación.
- Entre las adecuaciones realizadas fueron:
  - Refinamiento del texto

Dentro del Alfa de *Forma de Trabajo* se cuentan con:

- 9 aspectos de verificación dentro de los Estados del Alfa.

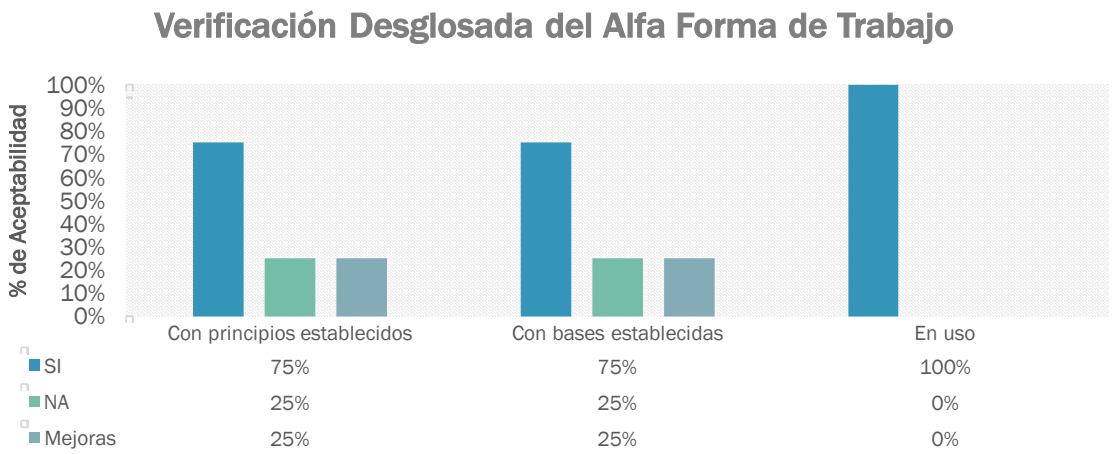


FIGURA XII.5 "RESULTADOS DE LA VERIFICACIÓN DEL ALFA DE FORMA DE TRABAJO"

De los cuales basados en la figura XII.5:

- El 78% son aceptados tal y como se presentan actualmente.
- El 22% restante, es necesario realizarle algunas adecuaciones.
- Así mismo cabe mencionar que se tienen recomendaciones generales de mejora por el 22% de los aspectos de verificación.
- Entre las adecuaciones realizadas fueron:
    - Refinamiento del texto

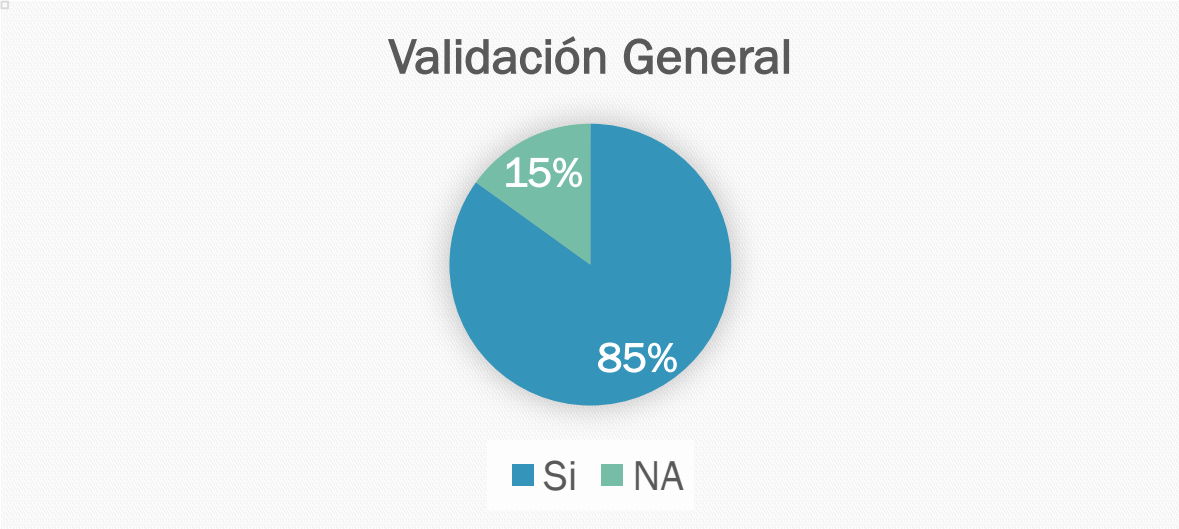


FIGURA XII.6 "RESULTADOS DE LA VERIFICACIÓN GENERAL DE LAS ALFAS DE ESSENCE SEC"

Para finalizar, en la validación general se obtuvo que de un total de 73 aspectos de verificación que se identificaron para las 4 Alfas y la Sub-Alfa, se puede observar en la Figura XII.6 el 85% de ellas proporcionaba un valor agregado y el otro 15% representaba aspectos que se podrían mejorar.

Cabe resaltar que de los 73 aspectos que se verificaron se encontró que el 29% de ellos podría mejorar significativamente como lo es el orden en que aparecen, mejoramiento de la sintaxis y la segmentación de aspectos para mejorar su comprensión.

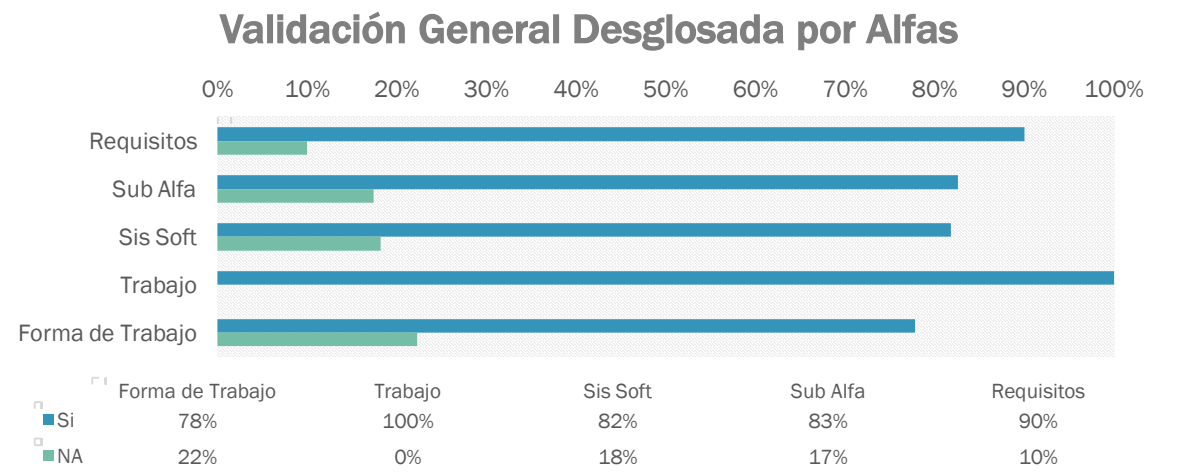


FIGURA XII.7 "RESULTADOS DE LA VERIFICACIÓN GENERAL DESGLOSADO DE LAS ALFAS DE ESSENCE SEC"

En una visión más a profundidad del análisis de validación podemos observar en la Figura XII.7 que el nivel más bajo se encuentra en el Alfa "*Forma de Trabajo*" con un 78% debido a que se comentaba, que esa Alfa depende demasiado del entorno de trabajo de la organización donde se esté aplicando, ocasionando que se tengan que realizar una serie de mejoras para estandarizarlo a un nivel más bajo.

En el proceso se observación también se pudieron identificar ciertos aspectos que son necesario destacar:

- El proceso de análisis permitió a la organización en primer lugar identificar las actividades que realizan cotidianamente sin que se percaten que representan aspectos de seguridad inmiscuidos en los procesos de ingeniería de software.
- Permitió detectar que sin contar con un área especializada en seguridad contienen medidas en su entorno que permiten su inclusión en cada proyecto realizado.
- Al realizar el proceso se identificaron ciertas áreas de mejora para los procesos que actualmente se llevan a cabo y también aquellos que por su criticidad no pueden implementarse ya que podrían ser perjudiciales.
- Existen características que no pueden ser implementadas debido a la baja visión de seguridad que tienen los Directivos ya que estos tienen las últimas decisiones.

XII.3.4 REFLEXIÓN

XII.3.4.1CONCLUSIONES

Al finalizar el análisis, se puede concluir que los aspectos de verificación que propone Essence Sec para la inclusión de la seguridad a los procesos de Ingeniería de Software son viables, dado que se cuenta con un 85% de aceptabilidad inicial tal y como se encuentra en esta primera instancia, adicionalmente se tiene una identificación total del 29% de esos aspectos de verificación para ser mejorados lo que brindaría un porcentaje mayor de aceptabilidad.

Es así que para el Departamento de desarrollo le parece viable la aplicación de Essence Sec ya que no es muy compleja de implementarse en sus procesos que actualmente se realizan, dado que no se modifican radicalmente.

Las Listas de verificación con las modificaciones por recomendaciones, en la columna "Verificación de Seguridad 1.0" se presenta la versión inicial y en "Verificación de Seguridad 2.0" se muestran los cambios realizados, donde el color Amarillo representa "Cambio de ubicación en la lista de verificación", el Verde indica "Modificación del texto original" y por último el Azul representa "La división del texto original para su mejor comprensión", estas se pueden observar en la tabla XII.1, XII.2, XII.3, XII.4 y XII.5 respectivamente para cada Alfa y Sub-Alfa.

-

ALFA REQUISITOS

TABLA XII.1 "LISTA DE VERIFICACIÓN DE SEGURIDAD 1.0 Y DE SEGURIDAD 2.0 DEL ALFA DE REQUISITOS"

Estados Requisitos	Verificación de Seguridad 1.0	Verificación de Seguridad 2.0	Cambios
Concebido	• La plataforma informática a la que pertenece el proyecto está clara.	Se cambió al Sub-Alfa *Evaluación de Riesgos de Seguridad* en el Estado *Identificación*.	• ***Cambio de ubicación***
Acotado	• ***Se han acotado los requisitos de seguridad..***	• ***Se han incorporado los requisitos de seguridad a los requisitos establecidos en el proyecto.***	• Modificación del texto
Coherente	• ***Se identificaron las medidas de seguridad en el entorno de desarrollo***	• ***Se identificaron las medidas de seguridad a considerar en el entorno de desarrollo***	• ***Modificación del texto***
Aceptable			
Tratado			
Cumplido			

SUB ALFA EVALUACIÓN DE RIESGOS DE SEGURIDAD

TABLA XII.2 "LISTA DE VERIFICACIÓN DE SEGURIDAD 1.0 Y DE SEGURIDAD 2.0 DEL SUB ALFA DE EVALUACIÓN DE RIESGOS DE SEGURIDAD"

Estado	Verificación de Seguridad 1.0	Verificación de Seguridad 2.0	Modificaciones
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 y 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	• ***Se identificaron los activos que están involucrados en el sistema.*** • ***Las dependencias que tiene cada activo identificado fueron analizadas*** • ***Los usuarios involucrados en cada activo identificado fueron analizados.*** • La plataforma informática a la que pertenece el proyecto está clara. • Cada activo identificado forma parte de la visión de seguridad establecida. • ***La visión de seguridad para el proyecto está definida y alineada a las metas del***	• ***División de texto*** • ***Cambio de ubicación*** • ***Modificación del texto***

-

Estado	Verificación de Seguridad 1.0	Verificación de Seguridad 2.0	Modificaciones
	identificadas	*negocio.* • Se identificaron y comprendieron las amenazas. • Se modelaron las amenazas identificadas	
Valoración			
Elicitación	• *Se identificaron suficientes requisitos para cumplir la visión de seguridad establecida para el proyecto.* • *Se identificaron y resolvieron las dependencias y conflictos entre los requisitos (Funcionales y no Funcionales).*	• *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).*	• *Modificación del texto*
Priorización			
Inspección			
Finalizado	• *Los requisitos de seguridad describen una solución aceptable para resolver los objetivos definidos para los interesados relevantes.*	• *Los requisitos de seguridad describen una solución aceptable para resolver los objetivos definidos.*	• *Modificación del texto*

ALFA SISTEMA DE SOFTWARE

TABLA XII.3 "LISTA DE VERIFICACIÓN DE SEGURIDAD 1.0 Y DE SEGURIDAD 2.0 DEL ALFA DE SISTEMA DE SOFTWARE"

Estados Sistema de Software	Verificación de Seguridad 1.0	Verificación de Seguridad 2.0	Modificaciones
Con arquitectura seleccionada	• *Los servicios compartidos y sistemas dependientes al nuevo proyecto son claros y bien definidos* • *Las descripciones de la arquitectura están estandarizadas* • *Se cuenta con un esquema de integración de la seguridad claro y preciso*	• *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.* • *La definición de la arquitectura está alineada con la visión de seguridad.*	• *División de texto* • *Modificación del texto*

-

Estados Sistema de Software	Verificación de Seguridad 1.0	Verificación de Seguridad 2.0	Modificaciones
		• *Se cuenta con un esquema de integración de la seguridad a la arquitectura claro y preciso*	
Demostrable	• *La revisión integral de seguridad ha sido realizada con éxito*	• Las descripciones de la arquitectura están estandarizadas • *Después de realizar una revisión integral, el sistema cumple con las normas de seguridad establecidas*	• *Cambio de ubicación* • *Modificación del texto*
Usable	• *Se han efectuado las pruebas previstas para comprobar la seguridad en el sistema y se encuentran dentro de los parámetros aceptados.*	• *Se han efectuado las pruebas definidas para comprobar la seguridad en el sistema y se encuentran dentro de los parámetros aceptados.*	• *Modificación del texto*
Listo			
Operacional			
Retirado			

-

ALFA TRABAJO

TABLA XII.4 "LISTA DE VERIFICACIÓN DE SEGURIDAD 1.0 Y DE SEGURIDAD 2.0 DEL ALFA DE TRABAJO"

Estados Trabajo	Verificación de Seguridad 1.0	Verificación de Seguridad 2.0	Modificaciones
Iniciado			
Preparado	• Se tiene garantizado el desarrollo del sistema de una forma segura por parte del grupo	• *El desarrollo del sistema se está realizando de una forma segura por parte del grupo*	• *Modificación del texto*
Comenzado	• Se está implementando la estandarización de codificación segura	• *Se está implementando la estandarización de codificación segura por parte del grupo*	• *Modificación del texto*
Bajo control			
Concluido			
Cerrado			

ALFA FORMA DE TRABAJO

TABLA XII.5 "LISTA DE VERIFICACIÓN DE SEGURIDAD 1.0 Y DE SEGURIDAD 2.0 DEL ALFA DE FORMA DE TRABAJO"

Estados F Trabajo	Verificación de Seguridad 1.0	Verificación de Seguridad 2.0	Modificaciones
Con principios establecidos			
Con bases establecidas	• *Se cuenta con alguna herramienta para la automatización de la revisión del código*	• Se realizó la capacitación integral de acuerdo al tipo de proyecto identificado. • *Se cuenta con alguna herramienta para la automatización de la revisión del código y pruebas*	• *Cambio de ubicación* • *Modificación del texto*
En uso	• *Se alimenta con los resultados al sistema de gestión y mitigación de defectos.*	• *Se alimenta con los resultados al repositorio de consulta para su mejora.*	• *Modificación del texto*
En su lugar			
Trabajando bien			
Retirado			

XII.4 LECCIONES APRENDIDAS

Respecto a los beneficios obtenidos de la revisión de los procesos con Essence Sec, se ha conseguido identificar las áreas de oportunidad que pueden mejorarse para brindar un mejor soporte y normalizar las actividades durante el proceso de desarrollo, así como incluir actividades y tareas que anteriormente no estaban establecidas en sus procesos.

Podemos destacar como lecciones aprendidas más importantes en este Caso Práctico son las siguientes:

- Se apreció que es difícil hacer conciencia de que un riesgo mal gestionado puede impactar seriamente el funcionamiento del sistema en cuestión o en muchos casos sistemas ligados por parte de los altos directivos.
- A través de la implementación del caso de uso se permitió mejorar y refinar las listas de verificación de las Alfas y Sub-Alfas debido a que se presentaban algunas ambigüedades en algunos puntos.
- Es importante realizar una campaña de concientización de la importancia de la seguridad por parte, en primer lugar, de los directivos y jefes de departamento, para que puedan ayudar en el proceso de implementación con el demás personal.
- También la implementación de ciertas herramientas de automatización y gestión de procesos en el desarrollo de los sistemas brindaría un mejor soporte para la administración de los sistemas debido al número de proyectos, artefactos manejados, las dependencias que existentes entre ellos y las diversas iteraciones que se tienen que realizar.
- Un punto a refinar es lo referente a Documentación de los procesos de seguridad ya que en el análisis resultó un punto crítico a ser mejorado.
- Ver la posibilidad de incluir a los Altos directivos dado que, en la actualidad, aunque se les expone el requerimiento e impacto en la seguridad, aun así, no se aplica o promueven su aplicación.

CAPÍTULO XIII. CONCLUSIONES

XIII.1 ANÁLISIS DE CONSECUCIÓN DE LOS OBJETIVOS Y APORTACIONES

En este capítulo se analiza la consecución de los objetivos planeados para este trabajo de investigación, describiendo a la vez sus principales aportaciones. Finalmente se muestran las líneas abiertas y la investigación futura.

Al finalizar la presente investigación se identificó que, existen diversas propuestas que tienen como finalidad incluir la seguridad en el desarrollo de software en diversos niveles y con enfoques definidos, es así que cuando las organizaciones requieren hacer uso de alguno de ellos, no pueden identificar adecuadamente cuál propuesta es la más idónea para su uso y necesidades. Es así que en primer lugar se obtuvo una armonización de los diversos marcos y estándares identificados donde se identificaron 14 aspectos de seguridad que son importantes de considerar a lo largo de todo el ciclo de vida ya que estos permiten a la organización poder identificar, catalogar, crear salvaguardas y mitigar los riesgos de seguridad asociados a la aplicación a desarrollar. Adicionalmente a los aspectos se tienen asociadas sus respectivas actividades que sirven de ejemplo para su aplicación.

Una vez que se identificaron los aspectos importantes de seguridad a considerar en el desarrollo se obtuvo la unión de estos con la Esencia logrando Essence Sec una propuesta que permitirá a las organizaciones que cuentan o no con un área de seguridad específica el poder implementar aspectos de seguridad a sus procesos de Ingeniería de Software ya que hace uso de las características de la Esencia incorporando los criterios de seguridad que son necesarios de contemplar a la hora de realizar un sistema, permitiendo a las organizaciones dominar sus métodos de producción, para posteriormente producir sus desarrollos de forma repetible y organizada con aspectos de seguridad incluidos.

Logrado a través del análisis e implementación de las listas de verificación de seguridad asociadas a cada una de las 4 Alfas seleccionadas para la presente investigación, así como sus respectivas actividades que en conjunto forman una base de conocimientos sólida para la inclusión de procesos de seguridad en el desarrollo de software, logrando obtener un software más estable y, por tanto, poder reducir el número de vulnerabilidades de seguridad con las que sale a producción el software.

Brindando a través del uso de Essence Sec un software con un aspecto de calidad adicional ya que cubre los puntos de la característica de Seguridad de CISQ (Object Management Group, 2012) y así poder reducir a niveles aceptables los riesgos de seguridad con sus respectivas vulnerabilidades que en la actualidad pueden significar la vida o la muerte.

En resumen:

Objetivo 1. Desarrollar y presentar un modelo del proceso de desarrollo de software que permita la reducción de estados con anomalías que afecten las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas a realizar; proporcionando una guía sobre cómo planificar, gestionar y ejecutar los

procesos de desarrollo; proporcionando valor agregado a los productos desarrollados a través de medidas proactivas en las fases iniciales del ciclo de vida del desarrollo.

El objetivo se logró al presentar Essence Sec, el cual es una adición de seguridad al estándar La Esencia, la cual brinda la inclusión de todos aquellos aspectos a considerar para la reducción de los estados del CIA.

Así mismo el trabajo de investigación perseguía los siguientes objetivos específicos:

Objetivo Especfico 1. Desarrollar una base de conocimientos para la inclusión de procesos de seguridad en el desarrollo de software, permitiendo tener un software más estable y, por tanto, reduciendo el número de vulnerabilidades del software.

La base de conocimientos se presenta con el resultado del Análisis de los marcos y estándares de seguridad establecidos en el Capítulo IV.

Objetivo Especfico 2. Proporcionar un valor agregado al software creado a través de la implementación proactiva de calidad a los procesos.

El valor agregado se logrará a través de la implementación de Essence Sec a los procesos de desarrollo tradicionales realizados por las organizaciones.

Objetivo Especfico 3. Proporcionar una guía y dirección sobre la implementación de la seguridad en los procesos de desarrollo de software.

Este objetivo específico se logra con la generación de Essence Sec.

XIII.2 LÍNEAS DE TRABAJO FUTURO

Las principales líneas futuras de investigación abiertas como resultado del trabajo presentado y que se quedan abiertas:

- Respecto al proceso es el poder integrar las tres Alfas restantes para tener una integración global a la Esencia.
- También se podrían realizar automatizaciones en el seguimiento del ciclo de vida para poder llevar una mejor trazabilidad del proyecto con la inclusión de la seguridad a través de Essence Sec.
- En cuanto a la aplicación práctica del trabajo de investigación, aplicar el proceso Essence Sec evolucionado para líneas de producto en casos de estudio para demostrar la utilidad del futuro proceso en dicho campo.
- Ya que en estos momentos únicamente se tienen las bases y las revisiones de expertos en las áreas de Ingeniería de software y de Seguridad, pero sería ideal el poder contrastarlo dentro de un proyecto en desarrollo.

REFERENCIAS

Arkin, A. B., Routh, A. J., Marchallek, A. N., Jim, A., Ferguson, C. K., Sars, F. C., … Derdouri, S. (2016). Building Security In Maturity Model - Version 7.0.

Brooks, F. P. (1986). No Silver Bullet —Essence and Accident in Software Engineering.

Castellaro, M., Romaniz, S., Ramos, J. C., Feck, C., & Gaspoz, I. (2016). Aplicar el Modelo de Amenazas para incluir la Seguridad en el Modelado de Sistemas, (October).

Castellaro, M., Romaniz, S., Ramos, J., & Pessolani, P. (2009). Hacia la Ingeniería de Software Seguro. *Facultad Regional Santa Fe - Universidad Tecnológica Nacional*, *610*, 10.

Common Criteria for Information Technology Security Evaluation Part 1 : Introduction and general model. (2012), (September), 1–95.

Consejo Superior de Administración Electrónica. (2012). MAGERIT - versión 3.0, 42. Retrieved from http://administracionelectronica.gob.es/ctt/resources/Soluciones/184/Area descargas/Libro-III-Guia-de-Tecnicas.pdf?idIniciativa=184&idElemento=87&idioma=en

Corrales Hermoso, A. L., Beltrán Pardo, M., & Guzmán Sacristán, A. (2006). *Diseño e implantación de arquitecturas informáticas seguras: Una aproximación práctica*. Madrid, España: Dykinson.

Fernández-Medina Patón, E., Moya Quiles, R., & Piattini Velthuis, M. G. (2003). *Seguridad de las tecnologías de la información : la construcción de la confianza para una sociedad conectada*. AENOR.

French, W. L., & Bell, C. (1999). *Organization development : behavioral science interventions for organization improvement*. Prentice Hall. Retrieved from https://books.google.com.mx/books/about/Organization_Development.html?id=De8JAQAAMAAJ&redir_esc=y

Garfinkel, S., Spafford, G., Daltabuit Godas, E., Gonzalez Velazquez, A. E., & Mallen Fullerton, G. M. (1999). *Seguridad práctica en UNIX e Internet*. México : McGraw-Hill Interamericana. Retrieved from http://pbidi.unam.mx:8080/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cat02025a&AN=lib.MX001000850455&lang=es&site=eds-live

ISO/IEC_JTC1/SC27. (2005). *ISO/IEC 25000 SQuaRE (System and Software Quality Requirements and Evaluation)*.

ISO/IEC_JTC1/SC27. (2016). *ISO/IEC 27000:2016 Information technology — Security techniques — Information security management systems — Overview and vocabulary* (Vol. 4th Editio). Retrieved from http://standards.iso.org/ittf/PubliclyAvailableStandards/c066435_ISO_IEC_27000_2016(E).zip

ISO/IEC JTC1 /SC27. (2005). *ISO/IEC 27001:2005 Information technology -- Security techniques -- Specification for an Information Security Management System*. Geneva, Switzerland.

Jacobson, I., Ng, P.-W., McMahon, P. E., Spence, I., & Lidman, S. (2013). *The Essence of Software Engineering*. USA: Addison - Wesley.

Kissel, R., Stine, K., Scholl, M., Rossman, H., Fahlsing, J., & Gulick, J. (2008). NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle. NIST. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-64r2.pdf

Knight, E. (2000). Computer Vulnerabilities, 1–66.

Lewin, K. (1946). Action Research and Minority Problems. *Journal of Social Issues*, *2*(4), 34–46. https://doi.org/10.1111/j.1540-4560.1946.tb02295.x

Manadhata, P. K. (2008). *An Attack Surface Metric*. Carnegie Mellon University.

Microsoft. (2009). Security Development Lifecycle for Agile Development. Microsoft. Retrieved from http://www.blackhat.com/presentations/bh-dc-10/Sullivan_Bryan/BlackHat-DC-2010-Sullivan-SDL-Agile-wp.pdf

Microsoft. (2013). Threat Analysis and Modeling.

Ministerio de Hacienda y Administraciones Públicas. (n.d.-a). Métrica 3 Interfaz de Seguridad. Retrieved April 25, 2017, from http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Metricav3/METRICA_V3_Seguridad.pdf

Ministerio de Hacienda y Administraciones Públicas. (n.d.-b). Métrica 3 Introducción. https://doi.org/10.1038/nn.2703

Object Management Group. (2012). Specifications for Automated Quality Characteristic Measures CISQ. USA: OMG.

Object Management Group. (2015). Kernel and Language for Software Engineering Methods (Essence). *SMSC/15-12-02*. USA: OMG. https://doi.org/http://www.omg.org/spec/Essence/1.0/PDF/

OWASP. (2009). Software Assurance Maturity Model - Version 1.0. Retrieved from http://www.opensamm.org/downloads/SAMM-1.0.pdf

Padak, N., & Padak, G. (1994). Research To Practice: Guidelines for Planning Action Research Projects. *Kent State Univ., OH. Ohio Literacy Resource Center*. Retrieved from http://literacy.kent.edu/Oasis/Pubs/0200-08.htm

Pardo, C. (2012). *A Framework to Support the Harmonization between Multiple Models and Standards*. Universidad de Castila la Mancha.

Pardo, C., Pino, F. J., García Rubio, F., Piattini Velthuis, M., & Rosado, J. (2010). Apoyando la armonización de múltiples marcos de referencia de procesos (pp. 299–304). Cuenca: XIII Ibero-American Conference on Software Engineering (CIbSE 2010).

Piattini Velthuis, M., García Rubio, F., García Rodríguez de Guzmán, I., & Pino, F. J. (2015). *Calidad de Sistemas de Información*.

Piattini Velthuis, M., & Hervada Vidal, F. (2007). *Gobierno de las Tecnologías y los Sistemas de Información*. Ra~Ma.

Real Academia Española. (2017). RAE - Seguro. Retrieved May 1, 2017, from http://dle.rae.es/srv/fetch?id=XTrgHXd%0D

Ruiz, F., Polo, M., Piattini, M., & Alarcos Research Group. (2002). Utilización de Investigación-Acción en la Definición de un Entorno para la Gestión del Proceso de Mantenimiento del Software. … *La Ingeniería Del Software Y* …. Retrieved from http://www.researchgate.net/publication/228599712_Utilizacin_de_Investigacin-

Accin_en_la_Definicin_de_un_Entorno_para_la_Gestin_del_Proceso_de_Mantenimiento_del_Software/file/e0b49521465332b8a6.pdf

Schneier, B. (2004). *Secrets and lies : digital security in a networked world*. Wiley.

Sheard, S., & Lake, J. G. (1998). Systems engineering standards and models compared. *International Symposium on Systems Engineering,*.

The Open Web Application Security Project. (2016). Software Assurance Maturity Model - Version 1.5. OWASP. Retrieved from https://www.owasp.org/images/6/6f/SAMM_Core_V1-5_FINAL.pdf

Trustwave. (2016). *Trustwave Global Security Report*.

Trustwave Holdings Inc. (2017). *Trustwave Global Security Report*.

Wadsworth, Y. (1998). What is Participatory Action Research? *Action Research International*, *Paper 2*(November), 1–23. Retrieved from www.scu.edu.au/schools/gcm/ar/ari/p-ywadsworth98.html

Wood Harper, T. (1985). Research Methods in Information Systems: Using Action Research.

Young, C. S. (2010). *Metrics and methods for security risk management*. Syngress/Elsevier.

LISTAS DE VERIFICACIÓN INICIALES DE ESSENCE SEC

ALFA REQUISITOS

Estados Requisitos	Verificación General	Verificación de Seguridad
Concebido	• Los stakeholders iniciales están de acuerdo con que el sistema se va a producir. • Se han identificado a los stakeholders que van a utilizar el nuevo sistema. • Se han identificado los stakeholders que van a financiar el trabajo inicial del nuevo sistema. • Es clara la oportunidad a la que hará frente el nuevo sistema.	• 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 han identificado a todos los stakeholders involucrados en el desarrollo del nuevo sistema. • Los stakeholders están de acuerdo en el objetivo del nuevo sistema. • Está claro cuál es el éxito para el nuevo sistema. • Los stakeholders comprender y están de acuerdo en la extensión de la solución propuesta. • Hay un acuerdo en la forma de describir los requerimientos. • Se han definido los mecanismos para la gestión de los requisitos. • Está claro el esquema de priorización. • Se han identificado y considerado las restricciones • Las hipótesis se han fijado claramente.	• 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	• La visión general es clara y la comparten todos los involucrados. • Se explicaron importantes escenarios de uso. • Las prioridades son claras.	• Se identificaron las medidas de seguridad en el entorno de desarrollo

Estados Requisitos	Verificación General	Verificación de Seguridad
	• Se trataron los conflictos. • Se comprende el impacto.	
Aceptable	• Los requisitos describen una solución aceptable para los interesados. • La tasa de cambio para acordar requisitos es baja. • El valor es claro.	• 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	• Suficientes requisitos se implementaron par que el nuevo sistema sea aceptable • Los interesados acuerdan que el sistema vale la pena realizando trabajo operativo	• Se han monitoreado las medidas de seguridad en el entorno de operación.
Cumplido	• El sistema satisface completamente los requisitos y las necesidades • No hay ítems excepcionales de requisitos excepcionales que impidan que el sistema se considere completo	• Los interesados reconocen el valor proporcionado por la implementación de la seguridad en el proyecto.

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 y 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 estableció 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 suficientes requisitos para cumplir la visión de seguridad establecida para el proyecto. • Se identificaron y resolvieron las dependencias y conflictos entre los requisitos (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. • 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 para los interesados relevantes.

ALFA SISTEMA DE SOFTWARE

Estados Sistema de Software	Verificación General	Verificación de Seguridad
Con arquitectura seleccionada	• Se seleccionó la arquitectura que trata los riesgos técnicos clave. • Se acordaron los criterios para seleccionar la arquitectura. • Se seleccionaron las plataformas, tecnologías y lenguajes. • Se tomaron las decisiones de compra, construcción y rehusó.	• Se tienen claras las particularidades del proyecto que impactan al diseño y arquitectura del sistema • Los servicios compartidos y sistemas dependientes al nuevo proyecto son claros y bien definidos • Se han identificado claramente los posibles escenarios a los que se enfrentará el sistema • Las descripciones de la arquitectura están estandarizadas • Los procesos de diseño son dirigidos hacia servicios y diseños seguros conocidos desde el inicio • Se cuenta con un esquema de integración de la seguridad claro y preciso
Demostrable	• Se demostraron las características clave de la arquitectura. • Los interesados relevantes acordaron que la arquitectura es apropiada. • Se ejercieron la interfaz crítica y las configuraciones del sistema.	• La integración con otros sistemas cumple las normas de seguridad establecidas • La revisión integral de seguridad ha sido realizada con éxito • El sistema aprobó los posibles escenarios de vulnerabilidades o limitaciones conocidas • Los servicios compartidos y el riesgo compartido resultante han sido revisados o Se revisaron las funciones, despreciando las inseguras
Usable	• El sistema es usable y tiene las características de calidad deseadas. • Los usuarios pueden operar el sistema. • Se aceptaron los niveles de defectos. • Se conoció el contenido de liberación.	• 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

Estados Sistema de Software	Verificación General	Verificación de Seguridad
		aceptación de la seguridad del sistema está completa
Listo	• Se puso a disposición la documentación de usuario. • Los representantes de los interesados aceptaron el sistema. • Los representantes de los interesados quieren que se haga operacional el sistema.	• 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
Operacional	• El sistema se usó en un ambiente operacional. • El sistema está disponible para los usuarios previstos. • Al menos un ejemplo del sistema está completamente operacional. • El sistema es compatible con los niveles de servicio acordados.	• 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	• No se da más soporte al sistema. • No se producirán más actualizaciones al sistema. • Se reemplazó o se descontinuó el sistema.	• 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 o La preservación de seguridad se ha realizado de acuerdo a las políticas de seguridad

ALFA TRABAJO

Estados Trabajo	Verificación General	Verificación de Seguridad
Iniciado	• Es claro el resultado esperado del trabajo que se iniciará. • Están identificadas claramente las limitaciones en la ejecución del trabajo. • Se conoce a los Stakeholders que financiarán el trabajo. • Está claramente identificado el inicio de las labores. • Se conoce a los Stakeholders que validarán los resultados. • La fuente de financiamiento es clara. • La prioridad del trabajo es clara.	• Se tiene claro las normas regulatorias que se deben de considerar • Se identificaron los operadores de datos críticos • Se comprende el ambiente operativo del sistema de software y sus componentes.
Preparado	• Se ha hecho el compromiso. • Se ha estimado costo y el esfuerzo del trabajo. • Se ha entendido la disponibilidad recursos • Son claras las políticas y procedimientos de gobernanza. • Los riesgos a los que se expone el trabajo son claros. • Los criterios de aceptación están definidos y acordados con el cliente. • Se ha dividido el trabajo lo suficiente para dar inicio al trabajo productivo. • Las tareas se han identificado y priorizado por el equipo y los stakeholders. • Se ha definido un plan confiable • Se tienen los recursos financieros para iniciar el trabajo. • El equipo o algunos miembros están listos para iniciar trabajo. • Se han definido los puntos de integración y entrega.	• Se publica y explica el proceso que se seguirá (roles, responsabilidades, plan) • Se entiende el esquema de clasificación de datos y funciones del sistema • Se tiene garantizado el desarrollo del sistema de una forma segura por parte del grupo
Comenzado	• Se comenzó el trabajo de desarrollo • Se monitorea el proceso de desarrollo. • Se hizo la división en ítems accionables con una clara	• Se monitorea el desarrollo del sistema de acuerdo al plan de acción • Se está implementando la estandarización de codificación

Estados Trabajo	Verificación General	Verificación de Seguridad
	definición. • Los miembros del equipo están aceptando y progresando en los ítems de trabajo.	segura
Bajo control	• El trabajo va bien; se están manejando los riesgos. • El trabajo y el re-trabajo no planeados están bajo control. • Se completaron los ítems de trabajo dentro de los estimados. • Se hizo seguimiento de las mediciones.	
Concluido	• Se terminó el trabajo que produce resultados. • Se están consiguiendo los resultados del trabajo. • El cliente aceptó el sistema de software resultante.	• Los interesados han validado que las medidas de seguridad pactadas han sido correctamente implementadas en el sistema de software
Cerrado	• Todas las tareas de limpieza de remanentes se completaron y el trabajo se cerró oficialmente • Todo se archivó • Se dispone de lecciones aprendidas y métricas	

ALFA FORMA DE TRABAJO

Estados Trabajo	Verificación General	Verificación de Seguridad
Con principios establecidos	• El equipo asume los principios y limitaciones. • Los stakeholders están de acuerdo con los principios y limitaciones establecidas. • Se han acordado a las prácticas de trabajo utilizadas con los stakeholders. • Se han acordado las herramientas de trabajo utilizadas con los stakeholders. • Si tiene una propuesta de acercamiento. • Se entiende el contexto de trabajo del equipo. • Se conocen las limitaciones que se aplican en el uso de prácticas y herramientas. • Se conocen las limitaciones del equipo que definen la adquisición de prácticas y herramientas.	• Se tienen claras cuáles son las funciones al ser inseguras no pueden implementarse en el proyecto • Se realizó la capacitación integral de acuerdo al tipo de proyecto identificado. • Se tiene un repositorio de consulta de temas de programación segura y su correcta implementación • Se acordó el plan de formación de seguridad
Con bases establecidas	• Se han seleccionado las prácticas y herramientas clave de la forma de trabajo. • El equipo ha acordado todas las prácticas de trabajo. • El equipo ha identificado todas las prácticas y herramientas no-negociables. • Se han analizado los vacíos que existen entre la capacidad que se necesita para ejecutar la forma de trabajo deseada y los niveles de capacidad del equipo. • Las prácticas y herramientas seleccionadas se han integrado para formar una forma de trabajo factible.	• Las herramientas seleccionadas cubren las medidas de seguridad requeridas • Se cuenta con alguna herramienta para la automatización de la revisión del código • Se hace uso marcos de trabajo middleware y bibliotecas comunes para utilizarse en todos los desarrollos. • El equipo de trabajo comparte la necesidad del entrenamiento integral
En uso	• Algunos miembros del equipo están usando la forma de trabajo • Se inspeccionó regularmente el uso de prácticas y herramientas • El equipo está adaptado y apoyando las prácticas y	• Se alimenta con los resultados al sistema de gestión y mitigación de defectos.

Estados Trabajo	Verificación General	Verificación de Seguridad
	herramientas • Los procedimientos están en su lugar para manejar retroalimentación	
En su lugar	• Todos los miembros del equipo están usando la forma de trabajo • Todos los miembros tienen acceso a las prácticas y herramientas para hacer su trabajo • El equipo completo se involucró en la inspección y adaptación de la forma de trabajo	
Trabajando bien	• Todos los miembros del equipo están usando la forma de trabajo. • Todos los miembros tienen acceso a las prácticas y herramientas para hacer su trabajo. • El equipo completo se involucró en la inspección y adaptación de la forma de trabajo.	
Retirado	• El equipo no usa más la forma de trabajo • Se compartieron las lecciones aprendidas para el uso futuro	• Se tienen claras cuáles son las funciones al ser inseguras no pueden implementarse en el proyecto • Se realizó la capacitación integral de acuerdo al tipo de proyecto identificado. • Se tiene un repositorio de consulta de temas de programación segura y su correcta implementación Se acordó el plan de formación de seguridad

BSIMM 7 (Arkin et al., 2016)

Gobierno	
B G-SM	Estrategia y Métricas
B G-CP	Política y Cumplimiento
B G-T	Entrenamiento

Estrategia y Métricas		Política y Cumplimiento		Entrenamiento	
SM		CP		T	
B G-SM-1.1	Publicación del proceso (roles, responsabilidades, plan)	B G-CP-1.1	Revisión de normas regulatorias	B G-T-1.1	Proporcionar entrenamiento
B G-SM-1.3	Educación	B G-CP-1.2	Identificación de información personal confidencial	B G-T-1.7	Entrenamientos por áreas o específicos
B G-SM-2.5	Identificación de métricas	B G-CP-1.3	Crear una política	B G-T-1.6	Tener un histórico de las experiencias obtenidas por la organización
		B G-CP-2.2	Control de cumplimiento relacionado con los riesgos previstos	B G-T-3.4	Actualizaciones de conocimiento anuales
		B G-CP-2.3	Tener un control de cumplimiento		
		B G-CP-2.5	Concientización de las obligaciones regulatorias y de privacidad		

Inteligencia	
B I-AM	Modelos de ataque
B I-SFD	Diseño y características de seguridad

Modelos de ataque		Diseño y características de seguridad		Estándares y requerimientos	
AM		SFD		SR	
B I-AM-1.2	Crear un esquema de clasificación de datos e	B I-SFD-1.1	Construir y publicar características de seguridad.	B I-SR-1.1	Crear un estándar de seguridad

Inteligencia	
B I-SR	Estándares y requerimientos

Modelos de ataque		Diseño y características de seguridad		Estándares y requerimientos	
	inventario.				
B I-AM-1.3	Identificar potenciales atacantes	B I-SFD-2.1	Construir marcos de trabajo middleware y bibliotecas comunes para utilizarse en todos los desarrollos.	B I-SR-1.2	Crear un portal de ayuda sobre temas de seguridad
B I-AM-1.5	Reunir y usar la inteligencia de ataque.			B I-SR-2.2	Crear una base de conocimientos a partir de estándares revisados
B I-AM-2.1	Crear patrones de ataques y casos de abuso que pueden ser utilizados de acuerdo al análisis			B I-SR-2.6	Usar estándares de codificación segura
B I-AM-2.7	Crear foros con todos los involucrados para discutir posibles ataques			B I-SR-3.1	Control de riesgos al uso de Open Source

SSDL Touchpoints	
B ST-AA	Análisis de la Arquitectura
B ST-CR	Revisión del código
B ST-ST	Test de seguridad

Análisis de la Arquitectura		Revisión del código		Test de seguridad	
AA		CR		ST	
B ST-AA-1.1	Revisión de las funciones de seguridad	B ST-CR-1.4	Utilizar herramientas automatizadas junto con una revisión manual.	B ST-ST-?.?	Asegurar control de calidad compatible con test EDGE / análisis de valores límites.
B ST-AA-1.2	Realizar revisión de diseño para aplicaciones de alto riesgo	B ST-CR-1.5	Hacer la revisión de código obligatorio para todos los proyectos	B ST-ST-1.3	Aplicar test con requerimientos y características de seguridad incluidas
B ST-AA-1.4	Usar un cuestionario para rankear el	B ST-CR-3.5	Uso de estándares de codificación	B ST-ST-2.4	Integrar los resultados para obtener métricas

SSDL Touchpoints	

Análisis de la Arquitectura		Revisión del código		Test de seguridad	
	riesgo de la aplicación				que ayuden al proceso de QA
B ST-AA-2.1	Definir y usar un análisis de la arquitectura	B ST-CR-1.6	Utilizar los informes centralizados como medio para la obtener métricas e impulsar la capacitación.	B ST-ST-3.5	Realización de test con base en los casos de abuso.
B ST-AA-2.2	Estandarizar las descripciones de la arquitectura (incluido el flujo de datos)			B ST-ST-2.1	Integrar pruebas de caja negra a los procesos de QA

Desarrollo	
S D-PT	Pruebas de penetración
S D-SE	Entorno del software
S D-CMVM	Gestión de configuraciones y vulnerabilidades

Pruebas de penetración		Entorno del software		Gestión de configuraciones y vulnerabilidades	
PT		SE		CMVM	
S D-PT-1.1	Uso de testers de penetración externos para encontrar defectos				
S D-PT-1.2	Alimentar los resultados al sistema de gestión y mitigación de defectos.				
S D-PT-1.3	Uso de test de penetración internos				
S D-PT-2.3	Realización periódica de test de penetración a lo largo del desarrollo				

MICROSOFT SDL (Microsoft, 2009)

		Entrenamiento							
		M T 1	Capacitación básica de seguridad						
		Requerimientos		**Diseño**		**Implementación**		**Verificación**		**Lanzamiento**	
		M R 1	Establecer los requerimientos de seguridad	M D 1	Establecer requerimientos de diseño	M I 1	Uso apropiado de herramientas	M V 1	Análisis dinámico	M L 1	Plan de respuestas a incidentes
		M R 2	Crear estaciones de calidad / Parámetros de Bugs	M D 2	Analizar la posible superficie de ataque	M I 2	Despreciar funciones inseguras	M V 2	Pruebas de caja negra	M L 2	Revisión final de seguridad
		M R 3	Valoración de los riesgos de seguridad y privacidad del proyecto	M D 3	Modelado de amenazas	M I 3	Análisis Estático	M V 3	Revisión del área de ataque	M L 3	Archivo de lanzamiento
		Respuesta							
		M Re 1	Ejecución del plan de respuesta a incidentes						

NIST SDLC (Kissel et al., 2008)

Iniciación		Iniciar el plan de seguridad del proyecto		Categorizar la información del sistema		Evaluación del impacto sobre el negocio		Evaluación del impacto de privacidad		Garantizar el desarrollo del sistema de una forma segura			
N I 1.1	Iniciar el plan de seguridad del proyecto	N I 1.1.1	Identificar los roles de seguridad en el desarrollo del sistema	N I 1.2.1	El resultado es un fuerte vínculo entre la misión, la información y los sistemas de información con una seguridad de la información rentable.	N I 1.3.1	Identificar líneas de negocio implementadas por el sistema y revisar cómo serán afectadas esas líneas de negocios;	N I 1.4.1	Identificación del Impacto de la Privacidad, la cual proporcione detalles sobre dónde y hasta qué grado se recopila, almacena o crea la información sobre la privacidad dentro del sistema.	N I 1.5.1	Plan para el entrenamiento de las fases de seguridad		
N I 1.2	Categorizar la información del sistema	N I 1.1.2	Identificar las fuentes de requisitos de seguridad, tales como leyes, reglamentos y Normas	N I 1.2.2	Requisitos de seguridad de alto nivel	N I 1.3.2	Identificar los componentes principales del sistema necesarios para mantener la funcionalidad mínima.			N I 1.5.2	Técnicas planificadas de aseguramiento de la calidad, con sus entregables e hitos.		

Iniciación		Iniciar el plan de seguridad del proyecto		Categorizar la información del sistema		Evaluación del impacto sobre el negocio		Evaluación del impacto de privacidad		Garantizar el desarrollo del sistema de una forma segura			
N I 1.3	Evaluación del impacto sobre el negocio	N I 1.1.3	Asegurar que los interesados tengan un entendimiento común, incluidas las implicaciones de seguridad, consideraciones y requisitos del sistema	N I 1.2.3	Nivel de esfuerzo estimado	N I 1.3.3	Identificar el tiempo que el sistema puede caer antes de que el negocio se vea impactado			N I 1.5.3	Normas de desarrollo y codificación, incluido el entorno de desarrollo.		
N I 1.4	Evaluación del impacto de privacidad	N I 1.1.4	Esbozar las ideas iniciales sobre los hitos clave de seguridad, incluyendo marcos de tiempo o desencadenadores de desarrollo que señalan que un paso de seguridad se acerca.			N I 1.3.4	Identificar la tolerancia del negocio para la pérdida de datos (idea inicial Necesario para definir el Objetivo de Punto de Recuperación).						
N I 1.5	Garantizar el desarrollo del sistema de una forma segura												

Desarrollo y Adquisición		Evaluación del riesgo para el sistema		Seleccionar y documentar los controles de seguridad		Diseño de la arquitectura de seguridad		Ingeniero en Seguridad y Desarrollo de Controles		Desarrollo de la documentación de seguridad		Pruebas de Conducta (Desarrollo, Funcional y Seguridad)	
N I 2.1	Evaluación del riesgo para el sistema	N I 2.1.1	Refinada evaluación del riesgo que refleje con más precisión los riesgos potenciales	N I 2.2.1	Obtención del plan de seguridad para el sistema.	N I 2.3.1	Esquema de integración de seguridad que proporciona detalles sobre dónde, dentro del sistema, la seguridad se implementa y comparte.	N I 2.4.1	Implementación de controles con especificación documentada para su inclusión en el plan de seguridad.	N I 2.5.1	Documentación de seguridad adicional que apoye al plan de seguridad del sistema	N I 2.6.1	Documentación de los resultados de la prueba, incluyendo cualquier variación inesperada descubierta durante la prueba.
N I 2.2	Seleccionar y documentar los controles de seguridad	N I 2.1.2	Debilidades conocidas en el diseño, limitaciones de proyectos identificadas y amenazas conocidas tanto para los componentes como de TI. Además, los requisitos anteriores ahora están pasando a controles específicos	N I 2.2.2	Especificación de los controles de seguridad identificados, mencionando cuáles, dónde y comó serán aplicados los controles.	N I 2.3.2	Listado de servicios compartidos y el riesgo compartido resultante.	N I 2.4.2	Lista de variaciones en el control de seguridad derivadas de decisiones de desarrollo y compensaciones.				

Desarrollo y Adquisición		Evaluación del riesgo para el sistema		Seleccionar y documentar los controles de seguridad		Diseño de la arquitectura de seguridad		Ingeniero en Seguridad y Desarrollo de Controles		Desarrollo de la documentación de seguridad		Pruebas de Conducta (Desarrollo, Funcional y Seguridad)	
			del sistema.										
N I 2.3	Diseño de la arquitectura de seguridad					N I 2.3.3	Identificación de controles de seguridad comunes usados en el sistema	N I 2.4.3	Posibles escenarios de evaluación para probar vulnerabilidades o limitaciones conocidas.				

Desarrollo y Adquisición		Evaluación del riesgo para el sistema		Seleccionar y documentar los controles de seguridad		Diseño de la arquitectura de seguridad		Ingeniero en Seguridad y Desarrollo de Controles		Desarrollo de la documentación de seguridad		Pruebas de Conducta (Desarrollo, Funcional y Seguridad)	
NI 2.4	Ingeniero en Seguridad y Desarrollo de Controles					NI 2.3.4	Las arquitecturas de seguridad deben ser representadas gráficamente y detalladas en la medida en que el lector pueda ver dónde se aplican los controles de seguridad básicos y cómo.						
NI 2.5	Desarrollo de la documentación de seguridad												
NI 2.6	Pruebas de Conducta (Desarrollo, Funcional y Seguridad)												

Implementación / Evaluación		Crear un plan detallado para C&A		Integrar la seguridad dentro de los ambientes establecidos o sistemas		Evaluar la seguridad del sistema		Autorizar el SI					
N I 3.1	Crear un plan detallado para C&A	N I 3.1.1	Un documento de planificación que identifica a los actores clave, las restricciones del proyecto, los componentes básicos, el alcance de las pruebas y el nivel de rigor esperado.	N I 3.2.1	Lista verificada de controles operativos de seguridad	N I 3.3.1	Paquete de Acreditación de Seguridad, que incluye el Informe de Evaluación de Seguridad, el POA & M, y el Plan de Seguridad del Sistema actualizado.	N I 3.4.1	Decisión de Autorización de Seguridad, documentada y transmitida por el Oficial Autorizado al Propietario del Sistema				
N I 3.2	Integrar la seguridad dentro de los ambientes establecidos o sistemas			N I 3.2.2	Completar la documentación del sistema			N I 3.4.2	Paquete de autorización final de seguridad				
N I 3.3	Evaluar la seguridad del sistema												
N I 3.4	Autorizar el SI												

Operación / Mantenimiento		Análisis de aptitud operativa		Realizar gestión y control de configuración		Monitoreo continuo							
N I 4.1	Análisis de aptitud operativa	N I 4.1.1	Evaluación de las implicaciones de seguridad debido a cualquier cambio en el sistema	N I 4.2.1	Verificación del control de cambios	N I 4.3.1	Documento de los resultados del monitoreo continuo						
N I 4.2	Realizar gestión y control de configuración			N I 4.2.2	Documentación de seguridad actualizada (Plan de seguridad del sistema y POA&M)	N I 4.3.2	Revisión del POA&M						
N I 4.3	Monitoreo continuo			N I 4.2.3	Evaluación de los cambios de seguridad documentados en el sistema	N I 4.3.3	Revisiones de seguridad, métricas, medidas y análisis de tendencias						
						N I 4.3.4	Actualizar la documentación de seguridad para la re acreditación de las decisiones de ser necesario						

Retiro		Construir y Ejecutar un Plan de Disposición / Transición		Asegurar la preservación de la información		Desinfectar los medios		Deshacerse del hardware y del software		Cierre del sistema			
N I 5.1	Construir y Ejecutar un Plan de Disposición / Transición	N I 5.1.1	Plan documentado de eliminación / transición para el cierre o la transición del sistema y/o su información.	N I 5.2.1	Índice de información conservada, y sus atributos de ubicación y retención.	N I 5.3.1	Registros de sanitización de medios	N I 5.4.1	Registros de la disposición del Hardware y Software	N I 5.5.1	Documentación que se verifique el cierre del sistema.		
N I 5.2	Asegurar la preservación de la información												
N I 5.3	Desinfectar los medios												
N I 5.4	Deshacerse del hardware y del software												
N I 5.5	Cierre del sistema												

MÉTRICA 3 (Ministerio de Hacienda y Administraciones Públicas, n.d.-a)

Planificación de SI		Planificación de la seguridad requerida en el proceso planificación de SI		Evaluación del riesgo para la Arquitectura Tecnológica		Determinación de la seguridad en el plan de acción		Catalogación de los productos generados durante el proceso de planificación de SI					
PSI-SEG 1	Planificación de la seguridad requerida en el proceso planificación de SI	PSI-SEG 1.1	Estudio de la Seguridad Requerida en el Proceso Planificación de SI	PSI-SEG 2.1	Estudio y Evaluación del riesgo de las Alternativas de Arquitectura Tecnológica	PSI-SEG 3.1	Determinación de la Seguridad en el Plan de Acción	PSI-SEG 4.1	Clasificación y Catalogación de los Productos Generados durante el Proceso de Planificación de SI				
PSI-SEG 2	Evaluación del riesgo para la Arquitectura Tecnológica	PSI-SEG 1.2	Organización y planificación	PSI-SEG 2.2	Revisión de la Evaluación del Riesgo de las Alternativas de Arquitectura Tecnológica								
PSI-SEG 3	Determinación de la seguridad en el plan de acción												

Planificación de SI		Planificación de la seguridad requerida en el proceso planificación de SI		Evaluación del riesgo para la Arquitectura Tecnológica		Determinación de la seguridad en el plan de acción		Catalogación de los productos generados durante el proceso de planificación de SI					
PSI-SEG 4	Catalogación de los productos generados durante el proceso de planificación de SI												

Viabilidad del Sistema		Estudio de la seguridad requerida en el proceso estudio de viabilidad del sistema		Selección del equipo de seguridad		Recomendaciones adicionales de seguridad para el sistema de información		Evaluación de la seguridad de las alternativas de solución		Evaluación detallada de la seguridad de la solución propuesta		Evaluación detallada de la seguridad de la solución propuesta	
EVS-SEG 1	Estudio de la seguridad requerida en el proceso estudio de viabilidad del sistema	EVS-SEG 1.1	Estudio de la Seguridad Requerida en el Proceso Estudio de Viabilidad del Sistema	EVS-SEG 2.1	Selección del Equipo de Seguridad	EVS-SEG 3.1	Elaboración de Recomendaciones de Seguridad	EVS-SEG 4.1	Valoración y Evaluación de la Seguridad de las Alternativas de Solución	EVS-SEG 5.1	Descripción detallada de la seguridad de la solución propuesta	EVS-SEG 6.1	Catalogación de los productos generados durante el proceso de estudio de viabilidad del sistema
EVS-SEG 2	Selección del equipo de seguridad												

Viabilidad del Sistema		Estudio de la seguridad requerida en el proceso estudio de viabilidad del sistema		Selección del equipo de seguridad		Recomendaciones adicionales de seguridad para el sistema de información		Evaluación de la seguridad de las alternativas de solución		Evaluación detallada de la seguridad de la solución propuesta		Evaluación detallada de la seguridad de la solución propuesta	
EVS-SEG 3	Recomendaciones adicionales de seguridad para el sistema de información												
EVS-SEG 4	Evaluación de la seguridad de las alternativas de solución												
EVS-SEG 5	Evaluación detallada de la seguridad de la solución propuesta												
EVS-SEG 6	Evaluación detallada de la seguridad de la solución propuesta												

Análisis del SI		Estudio de la seguridad requerida en el proceso de análisis del SI		Descripción de las funciones y mecanismos de seguridad		Definición de los criterios de aceptación de la seguridad		Catalogación de los productos generados durante el proceso de análisis del SI					
ASI-SEG 1	Estudio de la seguridad requerida en el proceso de análisis del SI	ASI-SEG 1.1	Estudio de la seguridad requerida en el Proceso de Análisis del SI	ASI-SEG 2.1	Estudio de las funciones y mecanismos de seguridad a implementar	ASI-SEG 3.1	Actualización del Plan de Pruebas	ASI-SEG 4.1	Clasificación y catalogación de los productos generados durante el proceso de análisis del Sistema de información				
ASI-SEG 2	Descripción de las funciones y mecanismos de seguridad												
ASI-SEG 3	Definición de los criterios de aceptación de la seguridad												
ASI-SEG 4	Catalogación de los productos generados durante el proceso de análisis del												

Análisis del SI	
	SI

Estudio de la seguridad requerida en el proceso de análisis del SI		Descripción de las funciones y mecanismos de seguridad		Definición de los criterios de aceptación de la seguridad		Catalogación de los productos generados durante el proceso de análisis del SI					

Diseño del sistema de información	
DSI-SEG 1	Estudio de la seguridad requerida en el proceso de diseño del SI
DSI-SEG 2	Especificación de requisitos de seguridad del entorno tecnológico

Estudio de la seguridad requerida en el proceso de diseño del SI		Especificación de requisitos de seguridad del entorno tecnológico		Requisitos de seguridad del entorno de construcción		Diseño de pruebas de seguridad		Catalogación de los productos generados durante el proceso de diseño del SI			
DSI-SEG 1.1	Estudio de la seguridad requerida en el proceso de diseño del SI	DSI-SEG 2.1	Análisis de los Riesgos del Entorno Tecnológico	DSI-SEG 3.1	Identificación de los requisitos de seguridad del entorno de construcción	DSI-SEG 4.1	Diseño de pruebas de seguridad	DSI-SEG 5.1	Clasificación y Catalogación de los Productos Generados durante el proceso de Diseño del SI		

Diseño del sistema de información	
DSI-SEG 3	Requisitos de seguridad del entorno de construcción
DSI-SEG 4	Diseño de pruebas de seguridad
DSI-SEG 5	Catalogación de los productos generados durante el proceso de diseño del SI

Estudio de la seguridad requerida en el proceso de diseño del SI		Especificación de requisitos de seguridad del entorno tecnológico		Requisitos de seguridad del entorno de construcción		Diseño de pruebas de seguridad		Catalogación de los productos generados durante el proceso de diseño del SI			

Construcción del SI

Estudio de la seguridad requerida en el proceso de construcción del SI	Evaluación de los resultados de pruebas de seguridad	Elaboración del plan de formación de seguridad	Catalogación de los productos generados durante el proceso de construcción del SI		

Construcción del SI		Estudio de la seguridad requerida en el proceso de construcción del SI		Evaluación de los resultados de pruebas de seguridad		Elaboración del plan de formación de seguridad		Catalogación de los productos generados durante el proceso de construcción del SI					
CSI-SEG 1	Estudio de la seguridad requerida en el proceso de construcción del SI	CSI-SEG 1.1	Estudio de la seguridad requerida en el proceso de construcción del SI	CSI-SEG 2.1	Estudio de los resultados de pruebas de seguridad	CSI-SEG 3.1	Elaboración del plan de formación de seguridad	CSI-SEG 4.1	Clasificación y catalogación de los productos generados durante el proceso de construcción del SI				
CSI-SEG 2	Evaluación de los resultados de pruebas de seguridad												
CSI-SEG 3	Elaboración del plan de formación de seguridad												
CSI-SEG 4	Catalogación de los productos generados durante el proceso de construcción del SI												

Implementación y aceptación del sistema		Estudio de la seguridad requerida en el proceso de implantación y aceptación del sistema		Revisión de medidas de seguridad del entorno de operación		Evaluación de resultados de pruebas de seguridad de implantación del sistema		Catalogación de los productos generados durante el proceso de implantación y aceptación del sistema		Revisión de medidas de seguridad en el entorno de producción			
IAS-SEG 1	Estudio de la seguridad requerida en el proceso de implantación y aceptación del sistema	IAS-SEG 1.1	Estudio de la seguridad requerida en el proceso de implantación y aceptación del sistema	IAS-SEG 2.1	Revisión de medidas de seguridad del entorno de operación	IAS-SEG 3.1	Estudio de los resultados de pruebas de seguridad de implantación del sistema	IAS-SEG 4.1	Clasificación y catalogación de los productos generados durante el proceso Implantación y Aceptación del Sistema	DSI-SEG 5.1	Revisión de medidas de seguridad en el entorno de producción		
IAS-SEG 2	Revisión de medidas de seguridad del entorno de operación												
IAS-SEG 3	Evaluación de resultados de pruebas de seguridad de implantación												

Implementación y aceptación del sistema		Estudio de la seguridad requerida en el proceso de implantación y aceptación del sistema		Revisión de medidas de seguridad del entorno de operación		Evaluación de resultados de pruebas de seguridad de implantación del sistema		Catalogación de los productos generados durante el proceso de implantación y aceptación del sistema		Revisión de medidas de seguridad en el entorno de producción			
	del sistema												
IAS-SEG 4	Catalogación de los productos generados durante el proceso de implantación y aceptación del sistema												
IAS-SEG 5	Revisión de medidas de seguridad en el entorno de producción												

Mantenimiento de SI		Estudio de la seguridad requerida en el proceso mantenimiento del SI		Especificación e identificación de las funciones y mecanismos de seguridad		Catalogación de los productos generados durante el proceso de mantenimiento de SI							
MSI-SEG 1	Estudio de la seguridad requerida en el proceso mantenimiento del SI	MSI-SEG 1.1	Estudio de la seguridad requerida en el proceso mantenimiento de SI	MSI-SEG 2.1	Estudio de la petición	MSI-SEG 3.1	Clasificación y catalogación de los productos generados durante el Proceso de Mantenimiento de SI						
MSI-SEG 2	Especificación e identificación de las funciones y mecanismos de seguridad			MSI-SEG 2.2	Análisis de las funciones y mecanismos de seguridad afectados o nuevos								
MSI-SEG 3	Catalogación de los productos generados durante el proceso de mantenimiento de SI												

INTEGRACIÓN DE MARCOS Y ESTÁNDARES PARA ESSENCE SEC

Entrenamiento		Amenazas		Diseño		Verificación	
M-SDL	Capacitación básica de seguridad	S C-EA-1	Identificar y comprender las amenazas	S C-AS-1	Insertar consideraciones para lineamientos proactivos de la seguridad en el proceso de diseño	**Pruebas Caja Negra**	
S G-EO-1	Ofrecer acceso a temas de programación segura e implementación	M-SDL	Modelado de amenazas/Riesgos	S C-AS-2	Dirigir el proceso de diseño hacia servicios seguros conocidos y diseños seguros desde la concepción	M-SDL	Pruebas de caja negra
S G-EO-2	Educar a todo el personal en el ciclo de vida del sw con lineamientos específicos en desarrollo seguro	S I-AV-1	Identificar un punto de contacto para problemas de seguridad	S C-AS-3	Controlar formalmente el proceso de diseño y validar la utilización de componentes de seguridad	B ST-ST-2.1	Integrar pruebas de caja negra a los procesos de QA
S G-EO-3	Hacer obligatorio el entrenamiento integral	**Riesgos**		S V-RD-1	Apoyar en las revisiones de diseño para asegurarse que existan los lineamientos de mitigación para riesgos conocidos	**Pruebas Generales**	
B G-SM-1.3	Educación	M-SDL	Valoración de los riesgos de seguridad y privacidad del proyecto	**Requerimientos de Seguridad**		S V-PS-1	Establecer el proceso para la realización de pruebas basándose en la implementación y los requisitos del software
B G-T-1.1	Proporcionar entrenamiento	B I-MA-1.3	Identificar potenciales atacantes	M-SDL	Establecer los requerimientos de seguridad	S V-PS-2	Realizar pruebas de seguridad durante el desarrollo, pudiendo hacer uso de automatización
B G-T-1.7	Entrenamientos por áreas o específicos	S C-EA-2	Aumentar la precisión de la evaluación y mejorar la granularidad de la comprensión por proyecto.	M-SDL	Establecer requerimientos de diseño	S V-PS-3	Realizar pruebas de seguridad específicas al desarrollo en cuestión para asegurarse que los lineamientos de seguridad están implementados antes de

							la publicación
Entrenamiento		**Riesgos**		**Requerimientos de Seguridad**		**Pruebas Generales**	
B G-T-3.4	Actualizaciones de conocimiento anuales	B I-MA-2.7	Crear foros con todos los involucrados para discutir posibles ataques	S C-RS-1	Considerar explícitamente la seguridad durante el proceso de captura de requisitos	B ST-ST	Asegurar control de calidad compatible con test EDGE / análisis de valores límites.
CSI-SEG 3.1	Elaboración del plan de formación de seguridad	B ST-AA-1.4	Usar un cuestionario para rankear el riesgo de la aplicación	S C-RS-2	Aumentar la granularidad de los requisitos derivada de la lógica de negocio y riesgos conocidos	B ST-ST-1.3	Aplicar test con requerimientos y características de seguridad incluidas
A considerar		S V-RC-3	Revisiones integrales para descubrir riesgos específicos	S C-RS-3	Exigir que se siga el proceso de requisitos de seguridad para todo el ciclo de vida del proyecto y 3ros	M-SDL	Análisis dinámico (Tiempo real)
S I-AV-3	Conducir análisis de causa raíz para incidentes	B ST-CR-1.5	Hacer la revisión de código obligatorio para todos los proyectos	B G-CP-1.2	Identificación de información personal confidencial	B ST-ST-3.5	Realización de test con base en los casos de abuso.
B I-MA-2.1	Crear patrones de ataques y casos de abuso que pueden ser utilizados de acuerdo al análisis	M-SDL	Umbrales de Calidad y límite de errores	DSI-SEG 2.1	Análisis de los Riesgos del Entorno Tecnológico	ASI-SEG 3.1	Actualización del Plan de Pruebas
B ST-AA-1.2	Realizar revisión de diseño para aplicaciones de alto riesgo	B G-CP-2.2	Control de cumplimiento relacionado con los riesgos previstos	DSI-SEG 3.1	Identificación de los requisitos de seguridad del entorno de construcción	DSI-SEG 4.1	Diseño de pruebas de seguridad
Equipo		EVS-SEG 3.1	Elaboración de Recomendaciones de Seguridad	IAS-SEG 2.1	Revisión de medidas de seguridad del entorno de operación	CSI-SEG 2.1	Estudio de los resultados de pruebas de seguridad
EVS-SEG 2.1	Selección del Equipo de Seguridad	EVS-SEG 4.1	Valoración y Evaluación de la Seguridad de las Alternativas de Solución	**Normas y Regulaciones**		IAS-SEG 3.1	Estudio de los resultados de pruebas de seguridad de implantación del sistema
		ASI-SEG 2.1	Estudio de las funciones y mecanismos de seguridad a implementar	B G-CP-2.5	Concientización de las obligaciones regulatorias y de privacidad	NIST	Evaluar la seguridad del sistema

Plan de seguridad		Riesgos		Normas y Regulaciones		Pruebas Generales	
NIST	Iniciar el plan de seguridad del proyecto	DSI-SEG 2.1	Análisis de los Riesgos del Entorno Tecnológico	B G-CP-1.1	Revisión de normas regulatorias	NIST	Pruebas de Conducta (Desarrollo, Funcional y Seguridad)
NIST	Categorizar la información del sistema	NIST	Evaluación del impacto de privacidad	EVS-SEG 3.1	Elaboración de Recomendaciones de Seguridad	**PenTesting**	
Respuestas a incidentes		NIST	Evaluación del riesgo para el sistema	**Superficie de Ataque**		B D-PT-1.1	Uso de testers de penetración externos para encontrar defectos
M-SDL	Plan de respuestas a incidentes	NIST	Evaluación del impacto sobre el negocio	M-SDL	Analizar la posible superficie de ataque	B D-PT-1.3	Uso de test de penetración internos
S I-AV-2	Establecer un proceso consistente de respuesta a incidentes	**Métricas y Apoyos**		M-SDL	Revisión del área de ataque	B D-PT-2.3	Realización periódica de test de penetración a lo largo del desarrollo
M-SDL	Ejecución del plan de respuesta a incidentes	S I-HO-2	Mantener guías formales de seguridad de operaciones	**Herramientas**		**Otras**	
Estandarizaciones		B G-T-1.6	Tener un histórico de las experiencias obtenidas por la organización	M-SDL	Uso de herramientas aprobadas	B I-SR-3.1	Control de riesgos al uso de Open Source
S I-HO-3	Realizar firma de código para componentes de aplicaciones	B I-MA-1.2	Crear un esquema de clasificación de datos e inventario.	M-SDL	Prohibir funciones inseguras	B ST-AA-1.1	Revisión de las funciones de seguridad
B ST-AA-2.2	Estandarizar las descripciones de la arquitectura (incluido el flujo de datos)	B I-SFD-2.1	Construir y publicar características de seguridad.	S I-FA-1	Entender el ambiente operativo de la aplicación y sus componentes	B I-MA-1.5	Reunir y usar la inteligencia de ataque.
B ST-CR-3.5	Uso de estándares de codificación	B I-SFD-1.2	Construir frameworks middleware y bibliotecas comunes para utilizarse en todos los desarrollos.	**Control de Procesos**		M-SDL	Prohibir funciones inseguras
B I-SR-2.6	**Usar estándares de codificación segura**	B G-SM-2.5	Identificación de métricas	B G-CP-2.3	Tener un control de cumplimiento	M-SDL	Revisión final de seguridad
		B	Crear una política	B	Publicación del proceso	M-SDL	Archivo de lanzamiento

		G-CP-1.3		G-SM-1.1	(roles, responsabilidades, plan)		
Arquitectura		**Métricas y Apoyos**		**Control de Procesos**		**Otras**	
B ST-AA-2.1	Definir y usar un análisis de la arquitectura	B ST-CR-1.6	Utilizar los informes centralizados como medio para la obtener métricas e impulsar la capacitación.	S I-HO-1	Habilitar las comunicaciones entre los equipos de desarrollo y los operadores de datos críticos	S V-RC-1	Encontrar oportunamente vulnerabilidades básicas a nivel de código y otros problemas de seguridad
PSI-SEG 2.1	Estudio y Evaluación del riesgo de las Alternativas de Arquitectura Tecnológica	B I-SR-1.1	Crear un estándar de seguridad	PSI-SEG 3.1	Determinación de la Seguridad en el Plan de Acción	S I-FA-2	Administración de parches y actualizaciones de los componentes y monitoreo de la configuración
PSI-SEG 2.2	Revisión de la Evaluación del Riesgo de las Alternativas de Arquitectura Tecnológica	B I-SR-1.2	Crear un portal de ayuda sobre temas de seguridad	NIST	Garantizar el desarrollo del sistema de una forma segura	**Automatización de código**	
NIST	Diseño de la arquitectura de seguridad	B I-SR-2.2	Crear una base de conocimientos a partir de estándares revisados	NIST	Evaluar la seguridad del sistema	B ST-CR-1.4	Utilizar herramientas automatizadas junto con una revisión manual.
		B ST-ST-2.4	Integrar los resultados para obtener métricas que ayuden al proceso de QA	NIST	Monitoreo continuo	S V-RC-2	Automatización de las revisiones de código
		B D-PT-1.2	Alimentar los resultados al sistema de gestión y mitigación de defectos.	NIST	Realizar gestión y control de configuración	M-SDL	Análisis Estático
		S C-EA-3	Comparar controles de compensación a cada amenaza contra otros desarrollos	NIST	Desarrollo de la documentación de seguridad		
				NIST	Seleccionar y documentar los controles de seguridad		