INCORPORACIÓN DE ASPECTOS DE SEGURIDAD EN LOS PROCESOS DE DESARROLLO DE SOFTWARE CON ESSENCE SEC

PRESENTA:
FRANCISCO ARELLANO MÉNDEZ

CO AUTORES:
MA. GUADALUPE E. IBARGÜENGOITIA GONZÁLEZ
HANNA OKTABA
MARIO PIATTINI

Áreas de Interés


¿Como unir las 3
áreas de Interés?

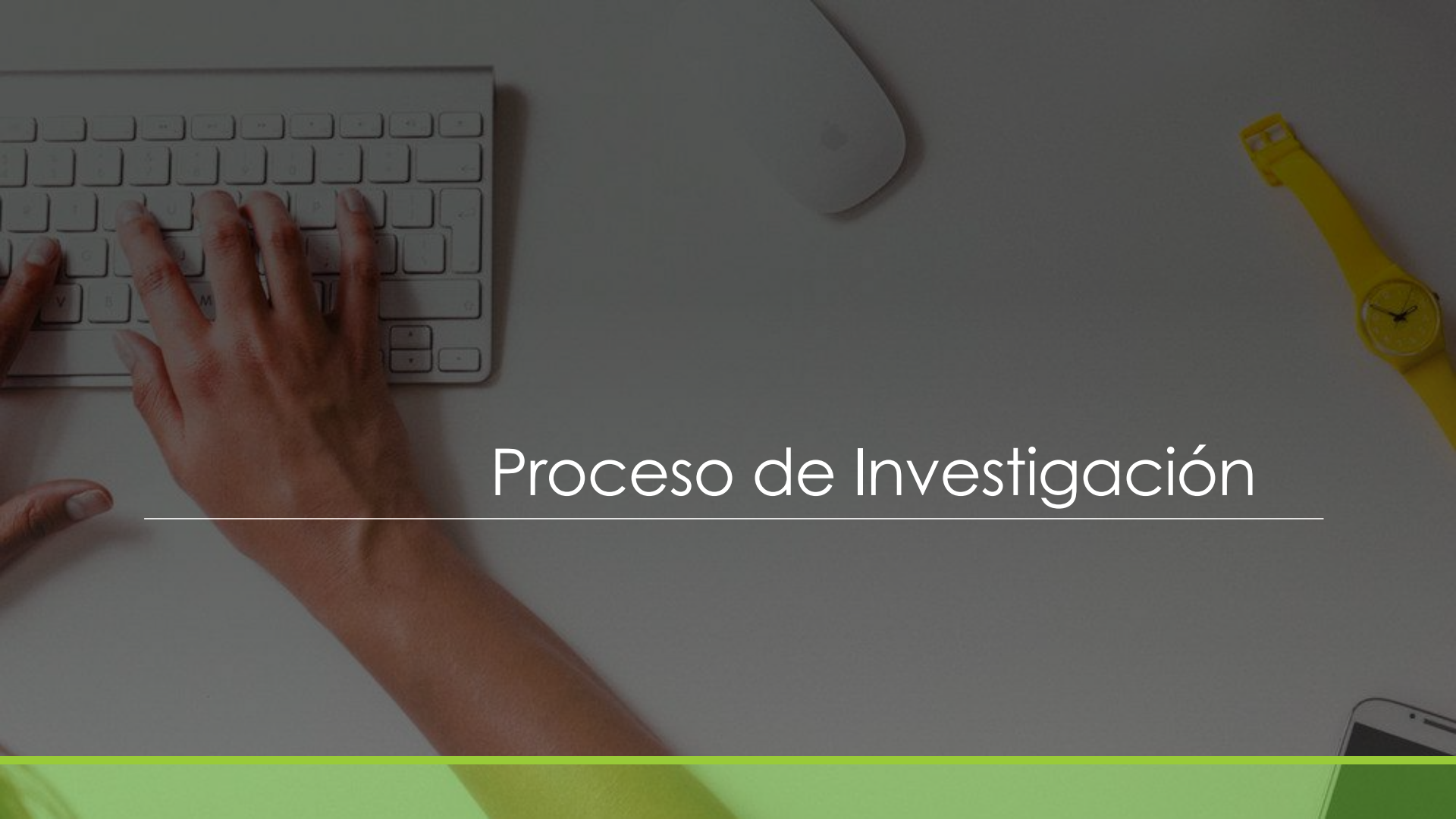
Bajo el Precepto de:

"Seguridad" apunta a una condición ideal, ya que no existe la certeza que se pueden evitar todos los peligros.

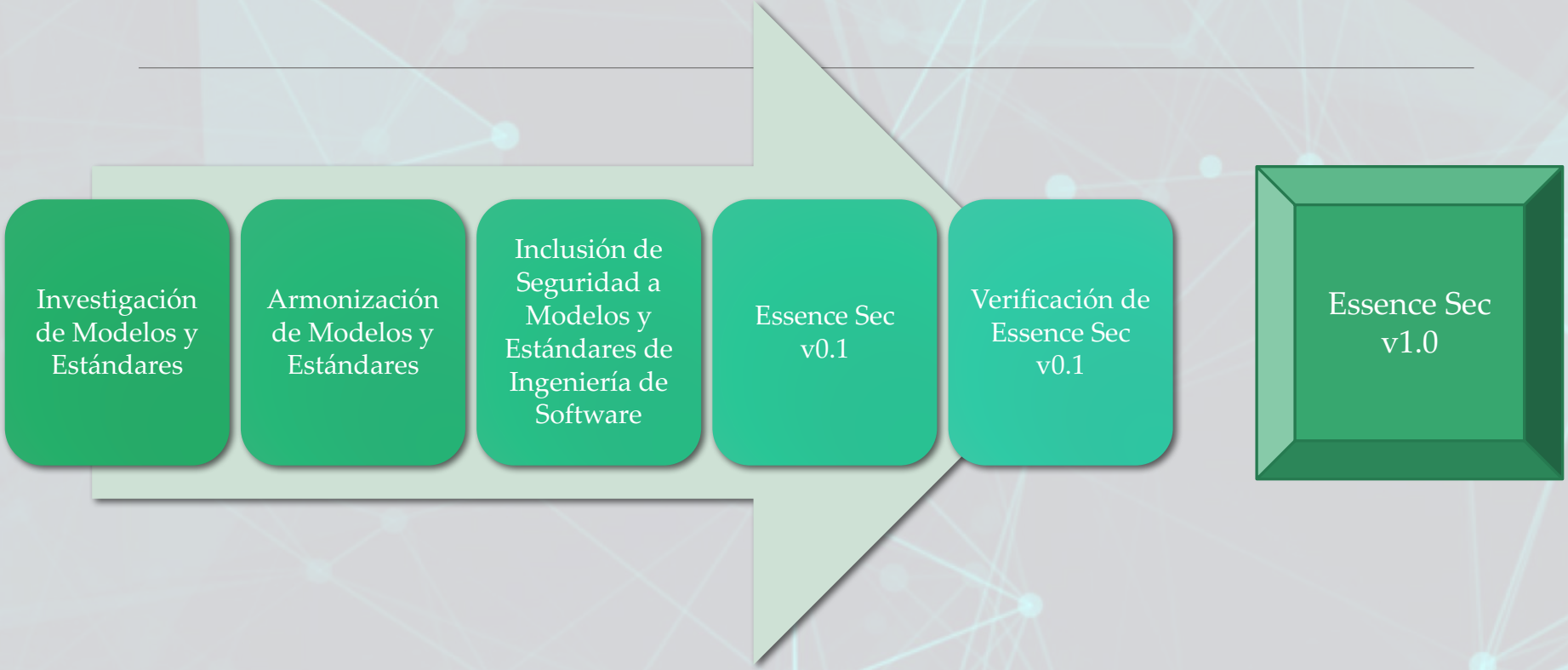
Su propósito es reducir esos riesgos hasta un nivel aceptable

Objetivo

El objetivo general de este trabajo es desarrollar y presentar un modelo de procesos para la mitigación de amenazas y vulnerabilidades de la seguridad informática dentro del desarrollo de software, que proporcione una guía sobre como planificar, gestionar y ejecutar los procesos de desarrollo; manteniendo la integridad del negocio y proporcionando un valor agregado a los productos desarrollados a través de medidas proactivas.



Proceso de Investigación


Investigación de Modelos y Estándares
Armonización de Modelos y Estándares
Inclusión de Seguridad a Modelos y Estándares de Ingeniería de Software
Essence Sec v0.1
Verificación de Essence Sec v0.1
Essence Sec v1.0

Modelos y Estándares de Seguridad en la Ingeniería de Software

ISO 2701	SAMM	BSIMM	Microsoft SDLC
CISQ	Métrica 3	NIST SDLC (800-64)	Common Criteria

Armonización de los Modelos y Estándares

Base de conocimientos

- Igualdades y Diferencias
- Aspectos incluidos y excluidos
- Terminología utilizada
- Aspectos a mejorar

Aspectos de seguridad a incluir

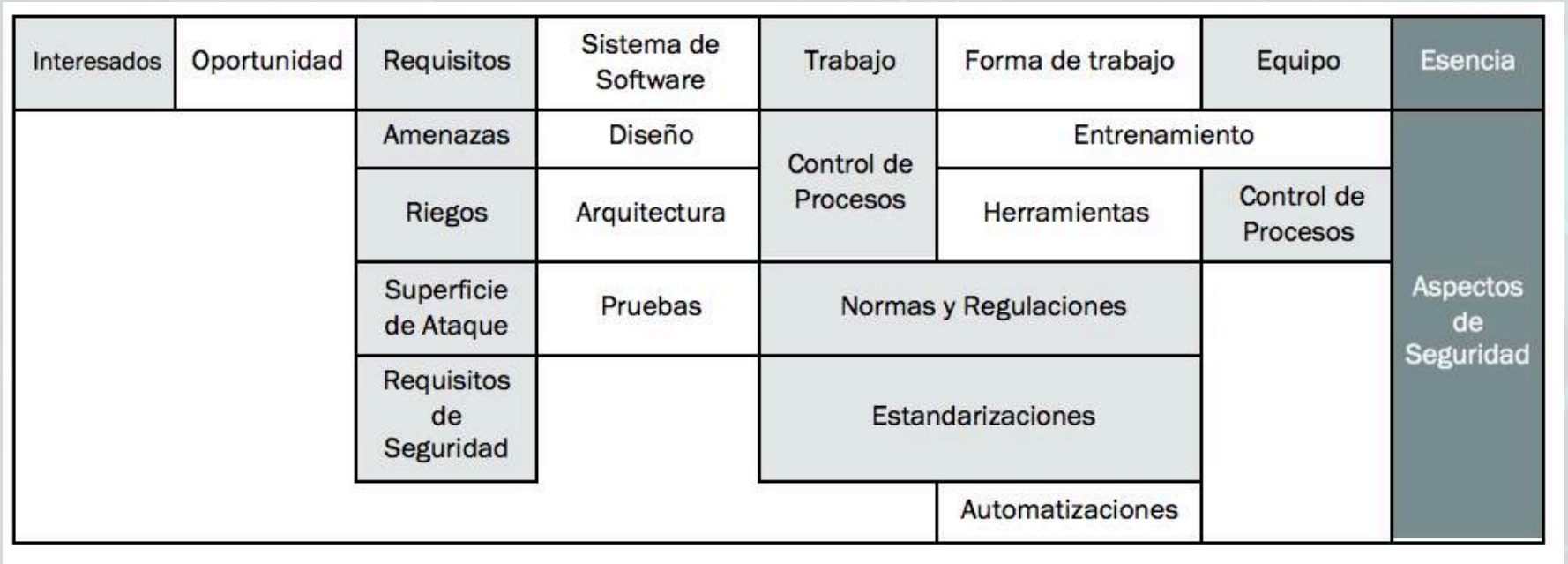
14

- Amenazas
- Riesgos
- Superficie de Ataque
- Requisitos de Seguridad
- Diseño de seguridad
- Arquitectura de seguridad
- Pruebas de seguridad
- Entrenamiento
- Herramientas
- Marcos y Regulaciones
- Estandarización de Procesos
- Automatizaciones
- Control de Procesos
- Métricas

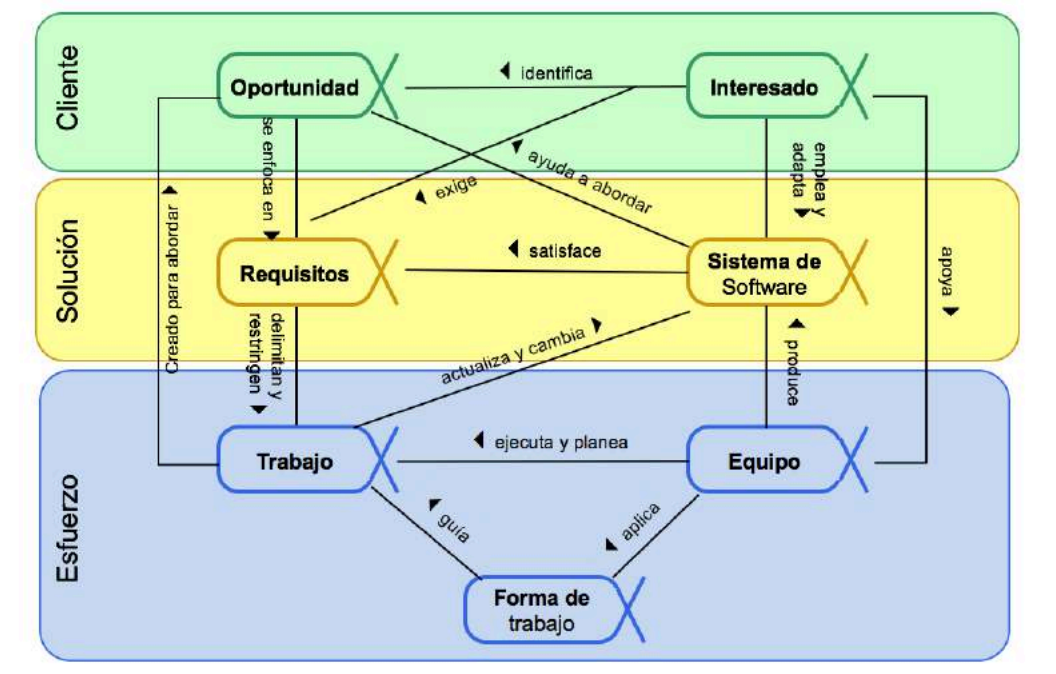

Essence Sec

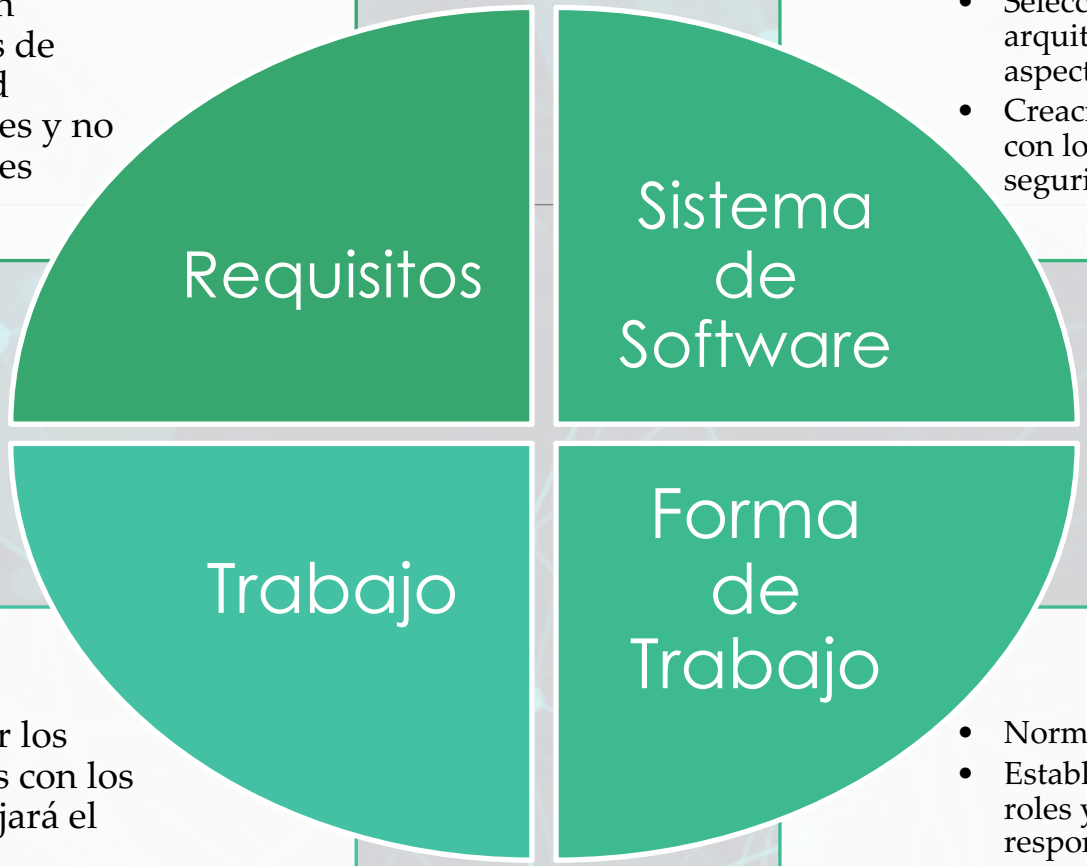
Como se logró

Integración Esencia y los Aspectos de Seguridad



Alfas Seleccionadas





- Obtención requisitos de seguridad funcionales y no funcionales

- Selección del diseño y arquitectura con aspectos de seguridad.
- Creación del Sistema con los lineamientos de seguridad establecidos

- Establecer los principios con los que trabajará el equipo

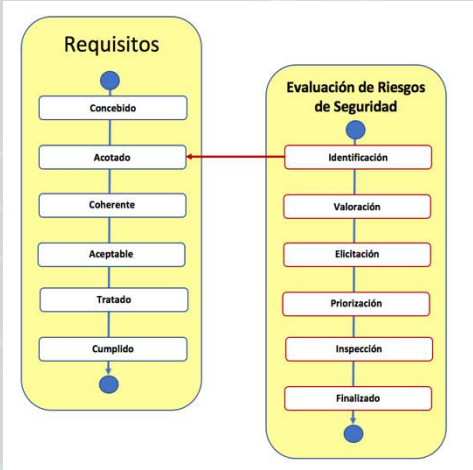
- Normas a considerar
- Establecimiento de roles y responsabilidades

Realizando

Listas de Verificación adicionales

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.	• 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 incorporado los requisitos de seguridad a los requisitos establecidos en el proyecto.

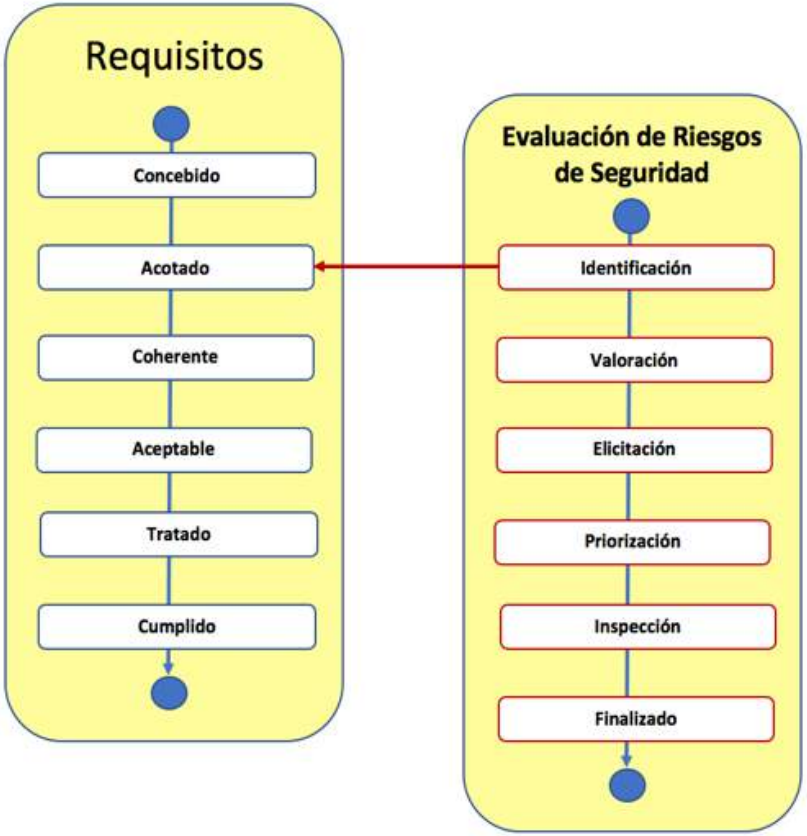
Sub – Alfas complementarias



Prácticas de seguridad

2	Práctica		
Identificación de Activos del Sistema			
Propósito			
Identificar claramente cada activo que tenga el Sistema de Información para accionar una medida de seguridad para su protección.			
Entrada		Resultado	
Productos de trabajo: • Documento: Visión de Seguridad • Documento: Funcionalidad del Sistema		Productos del Trabajo: • Documento: Activos de seguridad	
Criterios de finalización			
Se tienen definidos los activos que se encuentran inmiscuidos en el Sistema de Información que necesitan contar con medidas de seguridad para su protección			
Guía			
Actividad 2.1	Identificación de los activos		
Entrada		Salida	
Productos del Trabajo: • Documento: Visión de Seguridad • Documento: Funcionalidad del Sistema		Productos del Trabajo: • Documento: Activos de Seguridad	
Tareas	Herramientas	Competencias	Medidas
• 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.	• Normas y regulaciones para la seguridad de la información de acuerdo a la ubicación donde se implementará el Sistema de Información.		

Sub – Alfa Evaluación de Riesgos de Seguridad

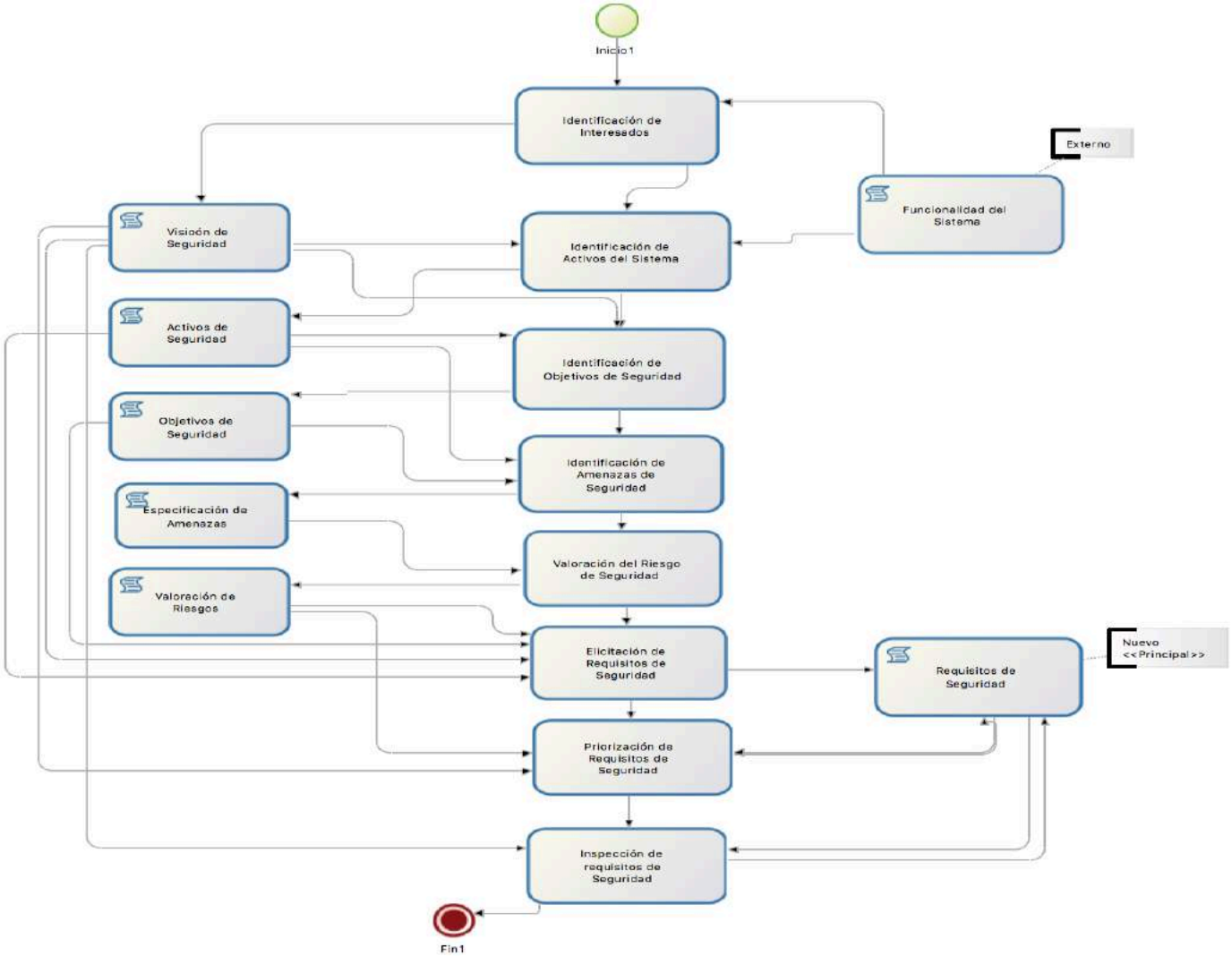


Ejemplo Lista de Verificación

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.

2	Práctica		
Identificación de Activos del Sistema			
Propósito			
Identificar claramente cada activo que tenga el Sistema de Información para accionar una medida de seguridad para su protección.			
Entrada		Resultado	
Productos de trabajo: • Documento: Visión de Seguridad • Documento: Funcionalidad del Sistema		Productos del Trabajo: • Documento: Activos de seguridad	
Criterios de finalización			
Se tienen definidos los activos que se encuentran inmiscuidos en el Sistema de Información que necesitan contar con medidas de seguridad para su protección			
Guía			
Actividad 2.1	Identificación de los activos		
Entrada		Salida	
Productos del Trabajo: • Documento: Visión de Seguridad • Documento: Funcionalidad del Sistema		Productos del Trabajo: • Documento: Activos de Seguridad	
Tareas	Herramientas	Competencias	Medidas
• 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.	• Normas y regulaciones para la seguridad de la información de acuerdo a la ubicación donde se implementará el Sistema de Información.		

Actividades


Inicio1
Identificación de Interesados
Externo
Funcionalidad del Sistema
Visión de Seguridad
Identificación de Activos del Sistema
Activos de Seguridad
Identificación de Objetivos de Seguridad
Objetivos de Seguridad
Identificación de Amenazas de Seguridad
Especificación de Amenazas
Valoración del Riesgo de Seguridad
Valoración de Riesgos
Elicitación de Requisitos de Seguridad
Nuevo
<<Principal>>
Requisitos de Seguridad
Priorización de Requisitos de Seguridad
Inspección de requisitos de Seguridad
Fin1

Integración en la Industria

Tipo de Organización / Proyecto

Complemento de sus procesos

Tamaño de Organización

Caso Práctico

Objetivos 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:

Realización

1ra Entrevista

Presentación de Essence Sec y análisis de terminología

2da Entrevista

Análisis de Essence Sec y sus relaciones con el entorno

3ra Entrevista

Definición de mejoras para Essence Sec

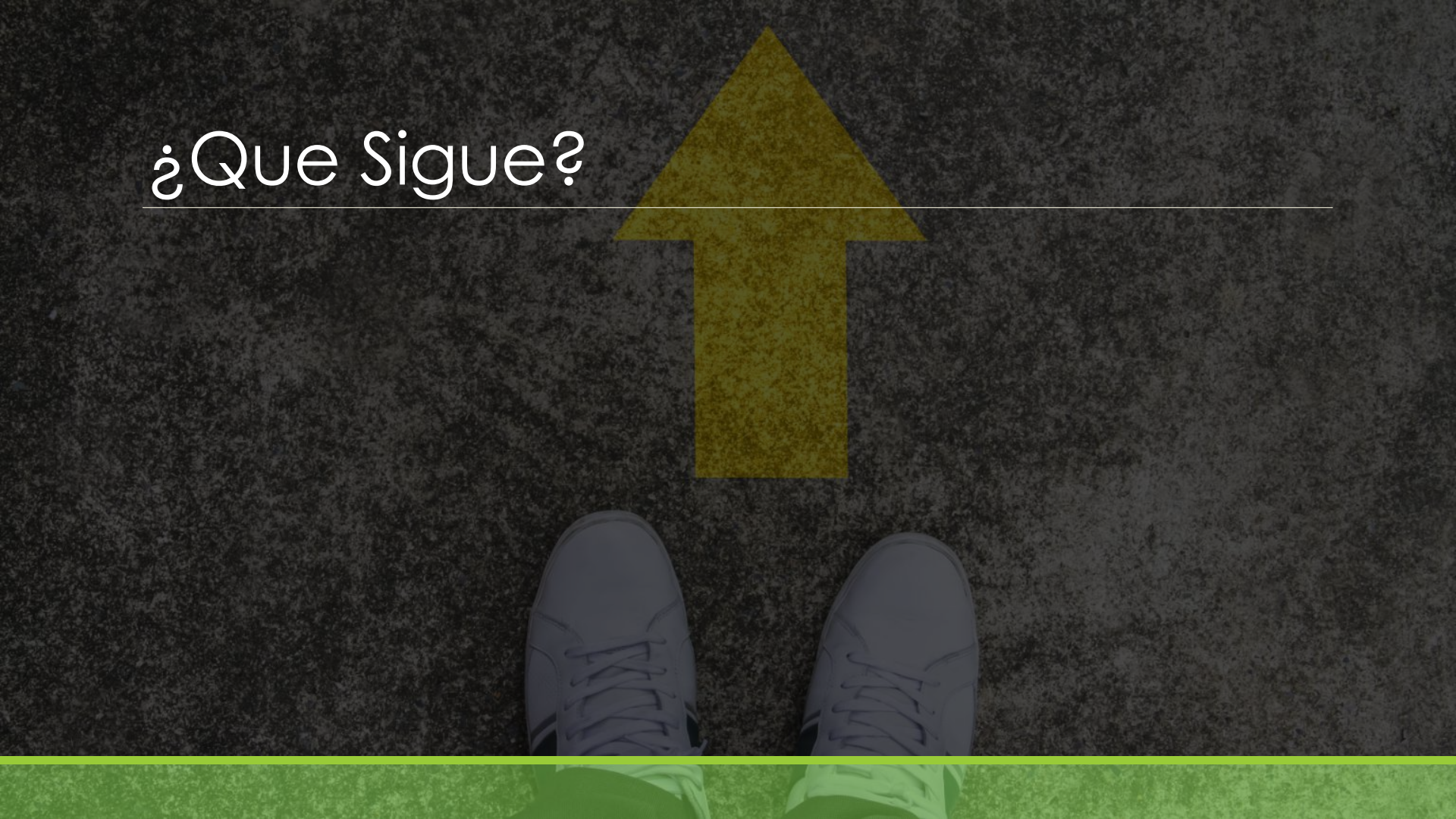
Conclusiones

Objetivo de la Investigación

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.

¿Que Sigue?



Difusión

Octubre 2017

SG SOFTWARE GURU

Posible

CONISOFT 2017

Octubre 2017

CIBSI CONGRESO IBEROAMERICANO DE SEGURIDAD INFORMÁTICA 2017

Noviembre 2017

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

Referencias

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).

Referencias

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

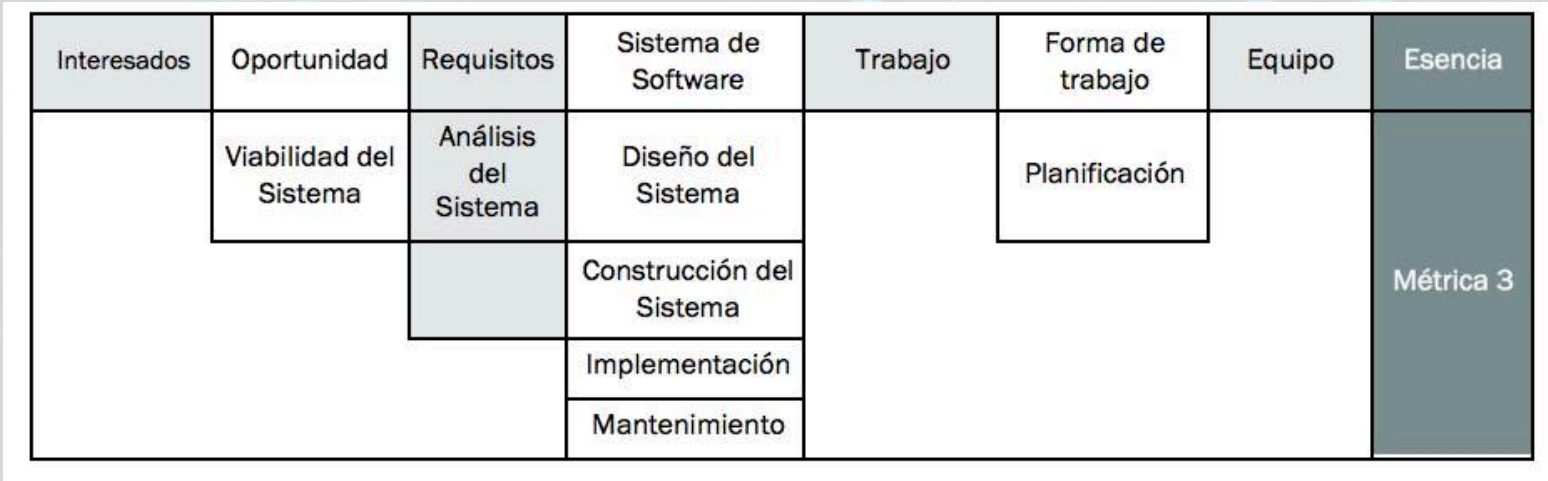
Wood Harper, T. (1985). Research Methods in Information Systems: Using Action Research.

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

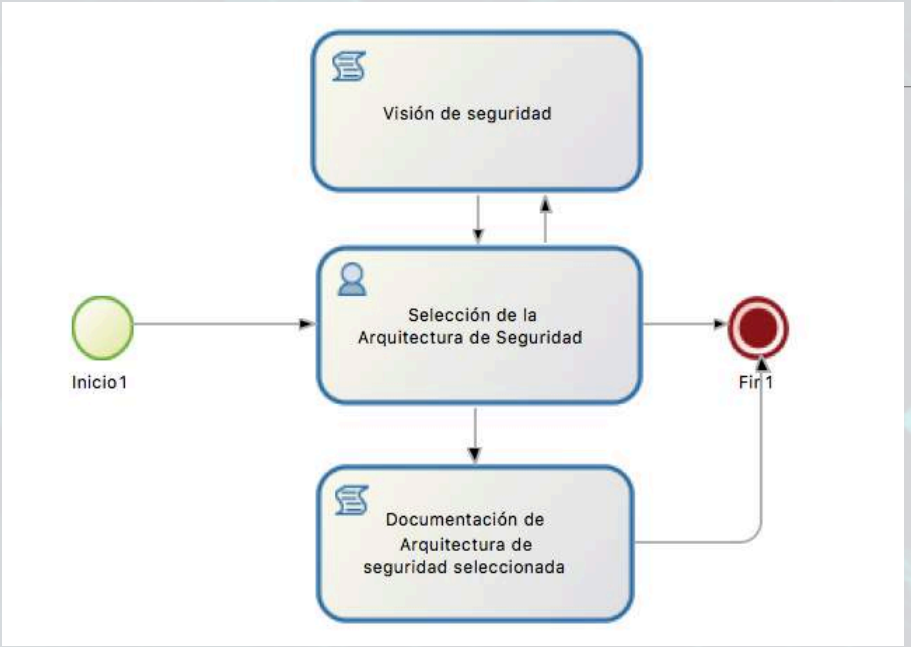
Preguntas

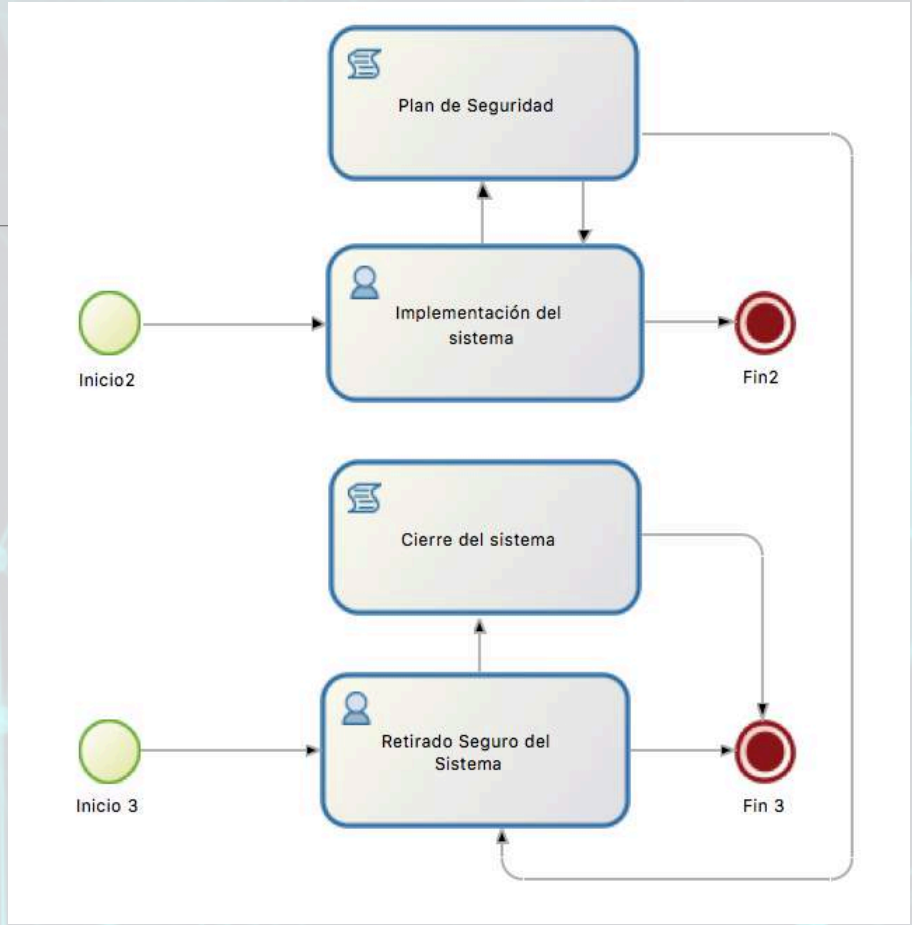

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO
POR MI RAZA HABLARA EL ESPIRITU
THANK YOU
GRACIAS
ARIGATO
SHUKURIA
DANKSCHEEN
BÏYAN
SHUKRIA
TINGKI
YAQHANYELAY
TASHAKKUR ATU
SUKSAMA
EKHMET
GRAZIE
MEHRBANI
BOLZÏN
MERCI
JUSPAXAR
GOZAIMASHITA
EFCHARISTO
KOMAPSUMNIDA
SPASSIBO
SNACHALHUYA
NUHUN
CHALTU
WABEEJA
MAITEKA
YUSPAGARATAM
HUI
GUI
HATUR
EKOJU
SIKOMO
MAKETAI
MINMONCHAR
SPASIBO
DENKAUJA
NENACHALHYA
UNALCHÉESH
MERSI
ATTO
AHHA
DHANYABAAD
PALDIES
LAH
MAAKE
SANCO
MERASTAWHY
GAEJTHO
AGUYJE
FAKAAUE
TAVTAPUCH
MEDAWAGSE
BAIKA
CONISOFT 2017

Comparación Esencia y Métrica 3



Interesados	Oportunidad	Requisitos	Sistema de Software	Trabajo	Forma de trabajo	Equipo	Esencia
	Viabilidad del Sistema	Análisis del Sistema	Diseño del Sistema		Planificación		Métrica 3
			Construcción del Sistema				
			Implementación				
			Mantenimiento				


Visión de seguridad
Selección de la Arquitectura de Seguridad
Documentación de Arquitectura de seguridad seleccionada
Inicio1
Fin 1


Plan de Seguridad
Implementación del sistema
Inicio2
Fin2
Cierre del sistema
Retirado Seguro del Sistema
Inicio 3
Fin 3