Prácticas de seguridad por diseño para la gestión de proyectos TI en PYMEs

Security by Design Practices for IT Projects Management in SMEs

Mercedes de la Cámara, Javier Sáenz-Marcilla

Magdalena Arcilla-Cobián , Jose A. Calvo-Manzano

Resumen — **Seguridad por diseño (SbD) es una filosofía orientada a la gestión de proyectos de desarrollo software seguro. Este artículo presenta el resultado de una investigación, en la que las prácticas de SbD son mapeadas con las prácticas, actividades y objetivos de control propuestos por los principales marcos y estándares que tratan la gestión de proyectos para el desarrollo software. Estos marcos se estructuran en los tres niveles organizativos típicos de las organizaciones: estratégico, táctico y operativo. El resultado de la investigación muestra las principales aportaciones y los vacíos que estos marcos tienen en la gestión de los proyectos para el desarrollo de producto software seguro. Además, en el entorno de las PYMEs, este estudio facilita a los profesionales de TI la aplicación de prácticas, actividades, y objetivos de control de seguridad, integrando distintos marcos y estándares de gobernanza y gestión en los proyectos de desarrollo TI.**

Palabras Clave – Gestión de proyectos; Seguridad por diseño; CMMI-DEV; Mejora de procesos software (SPI); COBIT 5; ISO/IEC 15504; ISO/IEC 27000.

Abstract — **Secure by Design (SBD) is oriented to secure software development project management. This article presents the results of a research where SbD practices are mapped to the practices, activities and control objectives proposed by the major frameworks and standards that deal with the management of software development projects. These frameworks are divided into three organizational levels (strategic, tactical and operational). The results of the research show the main contributions and lacks of these frameworks into managing projects for the development of secure software product. Furthermore, in the environment of SMEs, this study makes it easier for IT professionals implementing practices, activities, and security control objectives, integrating different frameworks and standards of governance and management in IT development projects.**

Keywords - Project management; Security by design; CMMI-DEV; Software Process Improvement (SPI); COBIT 5; ISO/IEC 15504; ISO/IEC 27000.

I. INTRODUCCIÓN

El Ministerio de Industria, Energía y Turismo [1] publica un estudio realizado en 2013, sobre 3.142.928 de empresas de la Unión Europea (UE). Este estudio refleja que las PYMEs representan el 99,9% del tejido empresarial en España y el 99,8% en Europa. Estas empresas generan el 40% del PIB y suponen el 60% del empleo en España y el 66% de empleo en Europa. Según el informe realizado en 2013 por el Observatorio Nacional de las Tecnologías y de la Sociedad de la Información [2], el 99,6% de estas empresas tienen sus sistemas de información conectados por distintos tipos de redes a internet, con el riesgo que este hecho supone. Las operaciones más frecuentes son diferentes tipos de transacciones con bancos y las Administraciones Públicas (AA.PP.), así como el intercambio de documentos propios de las operaciones de negocio.

El informe CHAOS de 2015, realizado sobre 50.000 empresas y publicado en [3], revela que sólo el 29% de los proyectos terminaron con éxito (considerando como éxito estar disponible en tiempo, dentro del presupuesto, y cumpliendo las características y requisitos funcionales del cliente; el 52% finalizó con un presupuesto mucho mayor y/o con fallos en los requisitos; y el 19% fueron cancelados o el producto entregado nunca fue utilizado.

Entre los fallos de los proyectos, están los fallos de seguridad los que preocupan a un porcentaje alto de las empresas por su coste y consecuencias. Kasperski realiza un estudio sobre 5.500 empresas en 26 países [4], donde analiza el coste promedio de los fallos de seguridad y sus principales consecuencias. Así, en este tipo de empresas, un fallo de seguridad supone un coste directo promedio de 38K US$ motivado por: acciones fraudulentas de la propia que plantilla tales como espionaje, o la explotación vulnerabilidades de la red; fallos asociados a terceras partes; malware; *phishing*, fugas de datos, y denegación de servicio (en adelante, DDoS). Además, cada fallo de seguridad supone un coste indirecto

promedio de 8K US$ empleado en la actualización de las capacidades tanto de la infraestructura tecnológica como del personal. Los gastos por necesidad de contratación de otros servicios profesionales (abogados, especialistas, etc.) se elevan a 11K US$, las pérdidas de oportunidades de negocio a 16K US$, siendo la DDoS la consecuencia más cara que asciende a 66K US$.

Ante esta problemática y la constatación de la ausencia de un marco de trabajo que incluya prácticas de seguridad durante la gestión de proyectos de TI aplicable fácilmente en las PYMEs, surgen la filosofía SbD (propuesta por Siemens con el respaldo del SEI en [5]), la propuesta de extensión de las prácticas del estándar ISO/IEC 15504 [6] y el marco GPS-PYME [7]. Así, el objetivo del estudio es presentar un conjunto de prácticas para la gestión de proyectos de desarrollo TI de utilidad para las PYMEs. Estas prácticas son aplicables en distintas funciones de los tres niveles organizativos (estratégico, táctico y operativo) y están basadas e integradas con las que se proponen en los estándares más utilizados en la gestión de proyectos para el desarrollo software seguro. Además, la revisión de estas prácticas sobre distintos marcos y estándares refleja algunos de sus puntos fuertes y debilidades.

Para ello en la sección II se muestra el método de investigación: la sección III realiza una breve descripción de las aportaciones a la gestión de proyectos para el desarrollo seguro que realizan los marcos y estándares más utilizados en la actualidad. La sección IV presenta los resultados del mapeo. Muestra las principales fortalezas y debilidades de los marcos estudiados en relación con la gestión de proyectos para desarrollo seguro. Finalmente, la sección V ofrece las principales conclusiones y perspectivas futuras del trabajo en curso.

II. MÉTODO DE INVESTIGACIÓN

El método de investigación que se propone está basado en la metodología de investigación MSSS (Método de estudio de similitud entre modelos y estándares)", propuesta en [8] y validada en [9]. En el caso que nos ocupa, con el fin de determinar similitudes entre los distintos modelos, se estudia cómo se contempla la seguridad en la gestión de proyectos de desarrollo, en el ámbito de las PYMEs. La metodología se ha resumido en tres etapas: (1) Inicio: se parte de un marco o estándar base que sirva de punto de partida para el estudio y otras soluciones que traten el mismo problema desde distintas perspectivas; (2) Observación: se observan las prácticas presentadas en el marco o estándar base sobre el resto de los marcos, obteniendo como resultado un mapeo prácticas; (3) Análisis de resultados: se analizan los resultados del mapeo y finalmente se propone una nueva solución al problema planteado.

A. Inicio

El estudio utiliza como marco de trabajo base la filosofía de SbD [5]. Sobre la estructura de factores SbD, realizada por los autores de este trabajo en un trabajo anterior, y presentada en [10], se han elegido para su mapeo los marcos más representativos a nivel internacional para cada uno de los tres niveles organizativos (estratégico, táctico y operativo). En el nivel estratégico se contemplan el estándar de gobernanza de TI ISO/IEC 38500 [11], y el marco para gobernanza y control propuesto por COBIT 5 [12]. A nivel táctico, se estudian el estándar de mejora de procesos en desarrollo software CMMI-DEV [13], ISO/IEC 15504-5 [14] e ISO/IEC 12207 [15]. Finalmente, a nivel operativo, se estudian el marco de gestión de proyectos PMBOK [16] y el estándar de seguridad ISO/IEC 27002 [17].

B. Observación

Para la observación se han elegido las prácticas propuestas por SbD. La revisión de cada una de estas prácticas SbD y su correspondiente mapeo sobre los modelos y marcos propuestos se ha realizado siguiendo el método MSSS (adaptándolo al dominio SbD), es decir: para cada práctica, se definen las palabras clave que sirven de búsqueda y revisión en cada uno de los procesos, prácticas, áreas, controles, etc. dependiendo de los marcos y estándares mapeados. El estudio de las coincidencias, entre la práctica SbD y el marco concreto, permite establecer el punto de trazabilidad entre marcos.

C. Análisis de resultados

Una vez establecidos los puntos de trazabilidad, para cada práctica SbD en los marcos elegidos para el estudio, se realiza un análisis de las fortalezas y debilidades que ofrecen en la gestión de proyectos para el desarrollo seguro.

III. DESCRIPCIÓN DE LOS MARCOS

En esta sección se realiza una breve descripción de los marcos estudiados en el trabajo de investigación.

A. Seguridad por Diseño

Este marco es el marco base de estudio. Con el objetivo de mostrar qué prácticas han sido mapeadas, se realiza una descripción más detallada que en el resto de los marcos y estándares mapeados.

SbD propone prácticas organizadas en un marco con cuatro áreas de proceso. En cada área de proceso se presentan un conjunto de metas específicas (Specific Goals, SG) y para cada una de ellas, una serie de prácticas específicas (Specific Pracrtices, SP):

1) OPSD: Organizational Preparedness for Secure Development (Preparación de la Organización para el Desarrollo Seguro). Esta área de proceso prepara a la organización para un desarrollo seguro. Contempla prácticas orientadas a establecer la capacidad organizativa para desarrollar productos seguros a través de: obtener el compromiso y respaldo de la dirección respecto a la seguridad en relación a los objetivos del negocio; estandarizar procesos y otros activos para desarrollo seguro; concienciar y formar para la seguridad de los productos; estandarizar un entorno de desarrollo seguro; y gestionar las vulnerabilidades.

2) SMP: Security Management in Projects (Gestión de la Seguridad en Proyectos). Esta área de proceso describe las prácticas para la gestión de la seguridad, orientadas al producto software durante su desarrollo en la gestión del proyecto. Propone: establecer el plan de proyecto integrado para proyectos de seguridad; planificar y entregar formación

de seguridad; seleccionar proveedores y componentes de terceras partes seguros; e identificar las causas subyacentes en las vulnerabilidades. Además, se proponen tres prácticas específicas encaminadas a la gestión de los riesgos de seguridad del producto software: establecer el plan de gestión de riesgos de seguridad de producto; realizar la evaluación de riesgos de seguridad del producto (software malicioso, defectos, etc.); y planificar cómo mitigar los riesgos de seguridad del producto software.

3) SRTS: Security Requirements and Technical Solution (Requisitos de Seguridad y Solución Técnica de Seguridad). Esta área es propia de ingeniería del software. Está enfocada a definir los requisitos de seguridad y la solución técnica de seguridad del proyecto. Se propone: desarrollar requisitos de seguridad de los clientes, y una arquitectura y diseño seguros; seleccionar las tecnologías apropiadas atendiendo a criterios de seguridad; y estandarizar la configuración de un producto seguro. Además, propone implementar el diseño seguro usando estándares de seguridad para su implementación; e incorporar aspectos relativos a la seguridad en la documentación que soporte el producto.

4) SVV: Security Verification and Validation (Verificación y Validación de Seguridad). Esta última área define prácticas enfocadas a los aspectos de verificación y validación de la seguridad propias de la ingeniería. Se propone: preparar y realizar la verificación y la validación de los requisitos de seguridad.

De estas cuatro áreas de proceso, nos interesan las prácticas que se mapean con las actividades relativas a la gestión segura de proyectos encaminadas a la seguridad del producto de desarrollo y no del proyecto en sí. Por ello, el estudio que se presenta en este artículo se centra en las prácticas específicas de la segunda área de proceso (SMP), que brindan al marco algunas pautas para la gestión segura de proyectos orientadas al producto TI.

B. Marcos y estándares de gobernanza y gestión mapeados

1) ISO/IEC 38500. Describe las prácticas para la gobernanza de TI a través de tres tareas: evaluar; dirigir y monitorizar. En cada una de estas tareas, la norma propone seis principios: responsabilidad; estrategia; adquisición; desempeño; conformidad y comportamiento humano. La norma no incluye directrices específicas en relación con la seguridad del software.

2) COBIT 5. Propone prácticas y controles enfocados en cinco áreas de proceso: evaluar, dirigir y monitorizar (Evaluate, Direct and Monitor, EDM); alinear, planificar y organizar (Align, Plan and Organise, APO); construir, adquirir e implementar (Build, Acquire and Implement, BAI); entregar y soportar servicios (Deliver, Service and Support, DSS); monitorizar, evaluar y valorar los servicios (Monitor, Evaluate and Assess, MEA). Estas áreas describen un total de 37 procesos facilitadores. El trabajo de investigación muestra como se contempla la seguridad durante la gestión de los proyectos de desarrollo desde el punto de vista del producto software. Establece para cada proceso dos tipos de controles: primarios y secundarios. Los controles primarios tienen una relación más estrecha que los seundarios en cuanto a la producción de beneficios, y la optimización de recursos y riesgos.

3) CMMI-DEV. Las áreas de proceso de SbD se definen como una extensión de CMMI-DEV 1.3. Por ello, las prácticas SbD están integradas con las prácticas genéricas y específicas de las áreas de proceso propuestas en CMMI-DEV 1.3. CMMI-DEV v1.3 ofrece 22 áreas de proceso organizadas en cuatro categorías: Gestión de Procesos; Gestión de Proyectos; Ingeniería; y Soporte Técnico.

4) ISO/IEC 15504 – ISO/IEC 12207. El estándar ISO/IEC 15504-5 presenta un modelo de evaluación de los procesos del ciclo de vida del software a través de un conjunto de indicadores de proceso. Aunque recientemente ha sido sustituida por la norma ISO/IEC 33004: 2015, los procesos del ciclo de vida del software, en ambos estándares, hacen referencia a los procesos de la norma ISO/IEC 12207. Este estándar define 43 procesos que se estructuran en 7 categorías: procesos de acuerdos; procesos facilitadores del proyecto a nivel organización; procesos del proyecto; procesos técnicos; procesos de implementación de programas; procesos de soporte de software; y procesos de reutilización de software.

5) PMBOK. Estructura la gestión de proyectos en 10 áreas de conocimiento: gestión de la integración; gestión del alcance; gestión del tiempo; gestión de costes; gestión de la calidad; gestión de recursos humanos; gestión de comunicaciones; gestión de riesgos; gestión de provisión; y gestión de grupos de interés o *stakeholder*. En estas áreas de conocimiento se describen cuarenta y siete procesos, agrupados en 5 categorías o fases para la gestión de proyectos: iniciación, planificación, ejecución, control y cierre de un proyecto.

6) ISO/IEC 27000. La primera parte de la norma, ISO/IEC 27001, ofrece la especificación y descripción de las características de un Sistema de Gestión de Seguridad de la Información (SGSI). La segunda parte, ISO/IEC 27002, proporciona 14 cláusulas orientadas al control de: las políticas de seguridad de la información; la organización de la seguridad de la información; los recursos humanos de seguridad; la gestión de activos; el control de accesoa; las técnicas criptográficas; la seguridad física y del entorno; seguridad en las operaciones; seguridad en las comunicaciones; en la adquisición, desarrollo y mantenimiento de los sistemas; en las relaciones con los proveedores; gestión de incidencias de seguridad de la información; gestión de la continuidad del negocio; y en el cumplimiento de leyes y regulaciones. Estas cláusulas están orientadas a garantizar la confidencialidad, integridad y disponibilidad del sistema de información.

IV. Resultados

Los resultados del mapeo de las prácticas SbD se presentan en los tres niveles organizativos. Las Tablas I a III muestran las metas y prácticas específicas de SbD.

Meta SG 1 Preparar y gestionar las actividades del Proyecto para la Seguridad. Propone: (1) SP 1.1 Establecer el plan integrado del proyecto para proyectos de seguridad. (2) SP 1.2 Planificar y entregar formación de seguridad. (3) SP 1.3 Seleccionar el proveedor y los componentes de terceras partes seguros. (4) SP 1.4 Identificar causas subyacentes de vulnerabilidades.

Meta SG 2 Gestionar los riesgos de seguridad del producto. Propone: (1) SP 2.1 Establecer el plan de gestión de riesgos de seguridad de producto. (2) SP 2.2 Realizar la evaluación de riesgos de seguridad del producto (software malicioso, defectos, etc.). (3) SP 2.3 Planificar la mitigación de riesgos para la seguridad del producto.

Las prácticas se mapean en marcos y estándares en los tres niveles organizativos:

1) Nivel estratégico: los resultados se muestran en la Tabla I.

TABLA I. PRÁCTICAS SBD EN LA GESTIÓN DE PROYECTOS PARA EL DESARROLLO: NIVEL ESTRATÉGICO

SbD	ISO/IEC 38500	COBIT 5 PRIMARIO	COBIT 5 SECUNDARIO
SMP SP 1.1	Dirección	BAI02, BAI07 APO08	BAI03, EDM01, BAI05, BAI06, DSS03, DSS04, DSS05, DSS06,
SMP SP 1.2	Principio 3: Adquisición (Dirección)	APO07	
SMP SP 1.3	Principio 3: Adquisición; Principio 4: Desempeño	APO10	
SMP SP 1.4		APO13, DSS03, DSS05	BAI02
SMP SP 2.1	Principio 2 Estrategia (Evaluación) Principio 3 Adquisición (Evaluación) Principio 4 Desempeño (Evaluación) Principio 6 Comportamiento humano. (Dirección)	APO01, APO02, APO04, APO11, APO12, APO13, BAI01, BAI03, DSS04, EDM03, MEA02	APO01, APO03, APO07, APO11 EDM01, EDM03, DSS02, DSS06
SMP SP 2.2		APO12, BAI02, BAI03	APO13
SMP SP 2.3		APO13, DSS04	

A nivel estratégico, ambos marcos incluyen la necesidad de definir las políticas de seguridad entre las recomendaciones de definición de otras políticas, la mayoría son políticas orientadas a la gestión de riesgos durante los proyectos. Sin embargo, a nivel de gobernanza no se aportan alternativas y técnicas para la definición de políticas de seguridad específicas en cuanto al tratamiento de los riesgos de seguridad del producto. Estas políticas han de transmitirse hacia la empresa y deben formar parte de los procesos implicados en la gestión de los proyectos de desarrollo de software seguro. Tampoco se definen los mecanismos ni planes de comunicación. En cuanto a las directivas de control, COBIT 5 define procesos y actividades encaminados a la gestión de la seguridad en proyectos de desarrollo de TI, tanto a nivel de los procesos de gestión como a nivel de los procesos de desarrollo. Sin embargo, aunque se recomiendan actividades en las que se aborda lo que hay qué hacer, no se especifica el cómo y tampoco se aportan técnicas que ayuden a las PYMEs en esta labor.

2) Nivel táctico: El resultado del mapeo se muestra en la Tabla II.

TABLA II PRÁCTICAS SBD EN LA GESTIÓN DE PROYECTOS PARA EL DESARROLLO: NIVEL TÁCTICO

SbD	CMM-DEV	ISO/IEC 15504 ISO/IEC 12207
SMP SP 1.1	CMMI-DEV-IPM: Gestión Integrada del Proyecto	ENG.7 Integración de Software; ENG.9 Integración de Sistemas
SMP SP 1.2	CMMI-DEV-PP-SP 2.5 Planificar el conocimiento y las habilidades necesarias	RIN.1 Gestión de RRHH
SMP SP 1.3	CMM-DEV-SAM-SP 1.2 Seleccionar a los proveedores, CMMI-DEV-IPM- SP 1.1 Establecer el proceso definido del proyecto	ACQ.2 Selección de proveedores ACQ.3 Contrato de acuerdos, ACQ.4 Monitorización de proveedores
SMP SP 1.4	CMMI-DEV-PP Planificación de Proyecto (SP 1.2 Establecer las estimaciones de los atributos de los productos de trabajo y de las tareas), CMMI-DEV-CAR Análisis Causal y Resolución	SUP.6 Evaluación del producto, SUP.9 Gestión de resolución de problemas
SMP SP 2.1	CMMI-DEV-RSKM Gestión de Riesgos SG 1, SG 2 y SG 3	MAN.5 Gestión de Riesgos
SMP SP 2.2	CMMI-DEV-RD (SP 3.4 Analizar los requisitos para conseguir un equilibrio), CMMI-DEV-RSKM (SP 2.2 Evaluar, clasificar y priorizar los riesgos)	MAN.3 Gestión de proyectos, MAN.5 Gestión de riesgos
SMP SP 2.3	CMMI-DEV-RSKM (SP 3.1 Desarrollar los planes de mitigación de riesgos)	MAN.5 Gestión de riesgos, MAN 6. Medición

Desde la perspectiva de mejora de procesos, CMMI-DEV describe líneas generales de prácticas específicas para definir requisitos de seguridad en el desarrollo, que son complementadas con las prácticas propuestas en el enfoque SbD en la gestión de los proyectos de desarrollo software seguro. Las prácticas SbD aproximan la gestión de proyectos para el desarrollo seguro orientando sus prácticas al producto software y no al proyecto en sí.

Sin embargo, no se aportan técnicas que permitan concretar estas prácticas en las PYMEs. El estándar ISO/IEC 15504 presenta la misma problemática. La extensión propuesta en [6] facilita la gestión de proyectos para desarrollo orientando la seguridad hacia el producto software. Sin embargo, no se ofrecen técnicas y soluciones que indiquen cómo implantarlas.

3) Nivel operativo: El resultado del mapeo se muestra en la Tabla III.

TABLA III. PRÁCTICAS SBD EN LA GESTIÓN DE PROYECTOS PARA EL DESARROLLO: NIVEL OPERATIVO

SbD	PMBOK	ISO 27000
SMP SP 1.1	4.2 Desarrollar el Plan para la Dirección del Proyecto	6.1.5 Seguridad de la información en la gestión de proyectos; 14.2 Seguridad en los procesos de desarrollo y soporte
SMP SP 1.2	9.1 Planificar la Gestión de los Recursos Humanos 9.2 Adquirir el Equipo del Proyecto 9.3 Desarrollar el Equipo del Proyecto	7.Seguridad en RRHH
SMP SP 1.3	12.1 Planificar la Gestión de las Adquisiciones 12.2 Efectuar las Adquisiciones 12.3 Controlar las Adquisiciones 12.4 Cerrar las Adquisiciones	14. Sistema de adquisición, desarrollo y mantenimiento, 15. Relaciones con proveedores
SMP SP 1.4		16. Información de gestión de incidentes de seguridad
SMP SP 2.1	11.1 Planificar la Gestión de los Riesgos 11.2 Identificar los Riesgos	14.2 Seguridad en los procesos de desarrollo y soporte
SMP SP 2.2	11.3 Realizar el Análisis Cualitativo de Riesgos 11.4 Realizar el Análisis Cuantitativo de Riesgos	18.2.3 revisión de cumplimiento técnico
SMP SP 2.3	11.5 Planificar la Respuesta a los Riesgos	12.2 Protección frente al malware, 12.6.1. Gestión de vulnerabilidades técnicas

A nivel operativo, los marcos estudiados se aplican en la gestión de proyectos de diferentes tamaños. Aunque el contexto de este estudio se centra en la seguridad en la gestión de proyectos para el desarrollo de software en las PYMEs, esto no implica que los proyectos abordados sean necesariamente pequeños. Las prácticas propuestas para la gestión de riesgos de PMBOK están orientadas al riesgo del proyecto en sí. Sin embargo, no contempla prácticas orientadas a la seguridad del producto software desarrollado. Los controles que presenta el estándar ISO/IEC 27002 para la implantación de un sistema de gestión de seguridad de la información aconsejan qué controlar en el sistema, pero no se especifica cómo implantarlos y tampoco lo relaciona con la gestión de proyectos de desarrollo.

Por lo tanto, queda patente la necesidad de investigar cómo llevar a cabo los procesos y las actividades necesarias para garantizar que la gestión del proyecto facilite la elaboración de un producto o servicio seguro, y aporte las técnicas y los mecanismos necesarios para ello.

V. CONCLUSIONES

El estudio realizado refleja que aunque aparentemente la mayoría de los marcos tratan el tema de la seguridad en la gestión de proyectos, la mayoría lo enfocan hacia la gestión de riesgos del propio proyecto y no del producto.

Existe un vacío en relación a la seguridad de los productos generados durante la gestión del proyecto de desarrollo, tanto a nivel de planificación como de análisis y gestión de los riesgos.

La mayoría de estas propuestas aportan diversas pautas orientadas al aseguramiento de los proyectos en términos de coste, cumplimiento de períodos y a veces de desempeño del producto, pero no se tiene en cuenta la necesaria seguridad para el buen desempeño del producto.

Las pautas propuestas son orientaciones de qué se debería hacer, pero no orientan sobre cómo podría hacerse y tampoco sobre qué técnicas utilizar relativas a la seguridad en la gestión de proyectos.

Ninguno de los estudios revisados aporta un hilo conductor de seguridad, desde la alta dirección hasta el nivel operativo, en la gestión de proyectos para el desarrollo seguro de TI.

La aplicación de los marcos y estándares en el entorno de las PYMEs es compleja y costosa, incluso en las empresas del sector TIC. En este sentido, se hace necesario para las PYMEs puedan contar con un marco genérico que facilite la gestión de proyectos para desarrollo seguro, orientado al producto y que aporte procesos, técnicas y medidas de evaluación para la validación de mejora de sus procesos de negocio.

AGRADECIMIENTOS

Este trabajo ha sido patrocinado por everis Aerospacial y Defensa y la Universidad Politécnica Madrid a través de la "Cátedra de Mejora de Procesos de Software en el Espacio Iberoamericano".

REFERENCIAS BIBLIOGRÁFICAS

[1] MIET. *Retrato de las PYME 2014.* Madrid: Gobierno de España. Ministerio de Industria,Turismo y Energía, 2014.

[2] ONTSI. *Análisis sectorial de la implantación de las TIC en la PYME española.* Madrid: FUNDETEC, 2014.

[3] Standish Group. *2015 CHAOS Report.* The Standish Group International, Inc.

[4] Kasperski Lab. "Damage control: the cost of security breaches IT security Risk". Specia report series. Kasperski Lab, *2015.*

[5] Siemens AG. "Security by Design with CMMI for Development, Version 1.3. An Application Guide for Improving Processes for Secure Products". Pittsburgh: CMMI Institute, 2013.

[6] Antoni Lluís Mesquida, A. M. "Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension". *Computers & Security. V. 48*, 19-34, 2015.

[7] Cámara, M. GPS-PYMEs: Marco de Gestión de Proyectos para el desarrollo Seguro en PYMEs", Tesis doctoral. UPM. Enero, 2016.

[8] Calvo-Manzano, J.A. J. A. et al., "Process Similarity Study: Case Study on Project Planning Practices Based on CMMI-DEV v1.2."

[9] Gasca, G.P., "Estudio de similitud del proceso de gestión de riesgos en proyectos de outsourcing de software: utilización de un método". Rev. ing. univ. Medellín vol.9 no.17 Medellín July/Dec. 2010.

[10] Camara, M. d., Saenz, F., Calvo-Manzano, J., & Arcilla-Cobian, M. Security by design factors for developing and evaluating secure software. *10th Iberian Conference on* (págs. pp.1-6). 17-20 June, 2015.

[11] ISO/IEC 38500. *ISO/IEC 38500:2008 Corporate governance of information technology.* ISO/IEC, 2008.

[12] ITGI. *COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Rolling Meadows, IL 60008 EE.UU.: ISACA, 2012

[13] SEI. *CMMI® para Desarrollo, Versión 1.3. CMMI-DEV, V1.3. Mejora de los procesos para el desarrollo de mejores productos y servicios.* Pittsburgh: SEI, 2010.

[14] ISO/IEC. *ISO/IEC 15504-5.* Information technology -- Process assessment -- Part 5: An exemplar software life cycle process assessment model. Recuperado el 21 de Febrero de 2016, de http://goo.gl/glujYZ

[15] ISO/IEC. *ISO/IEC 12207:2008 Systems and software engineering – Software life cycle processes.*, 2008

[16] PMI. *A GUIDE TO THE PROJECT MANAGEMENT BODY OF KNOWLEDGE (PMBOK® Guide).* Project Management Institute, 2008.

[17] ISO/IEC. *ISO/IEC 27002: 2013.* Information technology -- Security techniques -- Code of practice for information security controls. Obtenido de ISO/IEC 27002: 2013: Recuperado el 21 de Febrero de 2016 de http://goo.gl/C6tHWN