Factores de seguridad por diseño para el desarrollo y evaluación de software seguro

Security by design factors for developing and evaluating secure software

Mercedes de la Cámara, Fco. Javier Sáenz

Jose Antonio Calvo-Manzano, Magdalena Arcilla

Resumen — **Seguridad por diseño (SbD) es una filosofía orientada a la gestión segura de proyectos de desarrollo software seguro. En este artículo se presenta el resultado de una investigación en la que, partiendo de las prácticas propuestas por SbD, se define una estructura de factores para la gestión segura de proyectos de ingeniería de software. Los factores se estructuran en tres niveles organizativos (estratégico, táctico y operativo) con objeto de facilitar la implantación y evaluación del marco SbD. y han sido mapeados con los marcos y estándares de TI más representativos de los tres niveles organizativos. El resultado muestra las aportaciones y los vacíos de estos marcos para afrontar la seguridad en los proyectos de desarrollo de un producto software seguro.**

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 a project management oriented philosophy to develop secure software. This paper is the result of research based on the practices proposed by SbD. A security factors structure to manage such projects is defined. The factors are structured into three organizational levels (strategic, tactical and operational). The purpose is to facilitate the implementation and evaluation of SbD. The security factors structure for software engineering projects has been mapped with the most representative frameworks and standards and the results are shown.**

Keywords - Project Management; Security by Design; CMMI-Dev; Software Process Improvement (SPI); COBIT5; ISO/IEC 15504; ISO/IEC 27000.

I. INTRODUCCIÓN

El informe CHAOS 2013 [1] realizado sobre una muestra de unos 50.000 proyectos TI, revela que: sólo el 39 % de los proyectos concluyó con éxito en tiempo, dentro de presupuesto y cumpliendo las características y requisitos funcionales requeridos por el cliente; el 43% concluyeron tarde, fuera del presupuesto o con alguna carencia en los requisitos; y el 18 % fueron cancelados o entregados con productos que nunca se llegaron a utilizar. Los desajustes en los requisitos aumentan la vulnerabilidad de los sistemas de información y, con ello, la probabilidad de que se materialicen las amenazas a las que están sujetos.

Para Neumman [2] los fallos del desarrollo software son la raíz de los problemas de seguridad más relevantes y que afectan a los sistemas de información. El Instituto Ponemon, en su informe sobre la seguridad en el desarrollo de aplicaciones [3], analiza la seguridad en el ciclo de vida de los proyectos de desarrollo. En él se describe la intervención de dos tipos de procesos: a) orientados al desarrollo del producto; y b) a la gestión del proyecto. La seguridad del desarrollo de aplicaciones debe orientarse desde ambas perspectivas. Mientras que la perspectiva de proyecto abarca un conjunto de procesos comunes a todos los proyectos, la perspectiva de producto depende de la naturaleza del producto. El trabajo que se presenta está orientado a los procesos de gestión segura en proyectos de desarrollo de software seguro.

En este contexto algunos marcos y estándares, reconocidos internacionalmente, describen buenas prácticas relativas a la gestión de la seguridad en los proyectos de desarrollo de software.

Security by Design (SbD), definido por el Software Engineering Institute (SEI) y la empresa Siemens [4], supone una extensión del marco CMMI-DEV 1.3 [5]. Su aplicación puede realizarse tanto de forma independiente como en combinación con CMMI-DEV o con cualquier otro marco de desarrollo software. Su objetivo es mejorar la calidad del producto software, tratando los requisitos de seguridad de los productos desde las etapas más tempranas del ciclo de vida de desarrollo de software.

Así, partiendo de las prácticas SbD y de las prácticas de seguridad propuestas en los estándares internacionales de gobernanza y gestión aplicables a los proyectos de TI, se propone un conjunto de factores de seguridad, estructurados en

tres niveles organizativos, que podría facilitar la parametrización la seguridad de proyectos de ingeniería del software.

El trabajo presenta la siguiente estructura: en la sección II se muestra el método de trabajo utilizado para la investigación; la sección III presenta los marcos y estándares utilizados para la investigación, se definen los factores de estudio, y se muestra el resultado del análisis cualitativo de los factores relativos al nivel operativo; y en la sección IV se resumen las principales conclusiones y se presentan los trabajos de continuación en curso.

II. MÉTODO DE INVESTIGACIÓN

El estudio que se presenta en este artículo ha sido realizado ha sido realizado en el marco de una investigación sistémica. El enfoque de investigación sistémica se basa en la teoría de la observación. La teoría de la observación trata los sistemas observados, los observadores y los recursos de observación. Cada observación científica representa, por parte del observador de primer orden, la aplicación de algún esquema que le permiten identificar y/o describir información respecto a una realidad [6]. Esta información sirve como línea base para nuevas observaciones. Los resultados de las diferentes observaciones están abiertas a la observación externa de segundo orden. Así, un observador de segundo orden combina distintos puntos de vista y con ello identifica y resalta estructuras y vacíos latentes en las observaciones de primer orden.

En el caso que nos ocupa el objeto observado es - la gestión segura de proyectos de ingeniería de software -. Los sistemas observadores, son los diferentes enfoques que observan, desde las perspectivas estratégica, táctica y operativa, la seguridad del producto software durante la gestión de proyectos en las organizaciones. Los recursos las prácticas que estos enfoques aportan.

En el caso que nos ocupa, se realiza una primera observación de las prácticas SbD. SbD establece cuatro fases para la gestión segura del proyecto que incluye desde la preparación de la organización para abordar los proyectos de ingeniería software hasta la entrega de un producto o servicio seguro. En base a estas prácticas se define un conjunto de factores de seguridad. Se observa el grado de presencia de cada factor en las prácticas propuestas en los marcos y estándares implicados en la gestión de proyectos de ingeniería software. Así, se establece una estructura de factores de seguridad desde cuatro perspectivas encaminadas a asegurar el éxito de estos proyectos en tres niveles:

- Estratégico: factores de seguridad desde la perspectiva orientada a la gobernanza de las TI.
- Táctico: factores de seguridad relativos a la gestión de servicios y la mejora de procesos.
- Operativo: factores de seguridad encaminados a la gestión de proyectos y la gestión de la seguridad a nivel técnico.

Posteriormente, tanto la publicación de este trabajo como su consideración y aplicación en la gestión de proyectos de ingeniería software en PYMES, nos permitirá obtener nuevos resultados en la observación de segundo orden.

III. LAS PRÁCTICAS SBD EN LOS MARCOS Y ESTÁNDARES IMPLICADOS EN LA GESTIÓN DE PROYECTOS DE DESARROLLO SOFTWARE

En esta sección se introduce el marco SbD, se presenta el nivel operativo de la estructura de factores de seguridad definida en base a las prácticas SbD y se muestra el resultado del mapeo de los factores en los principales marcos y estándares de este nivel.

A. Seguridad por diseño (SbD)

El modelo SbD presenta cuatro áreas de proceso con siete metas y veintidós prácticas que sirven de guía para definir las características de seguridad en los procesos de desarrollo software: la primera, OSD, para los aspectos de seguridad relativos a la organización y necesarios para abordar los proyectos de forma segura; la segunda, SMP, relativa a la gestión segura de los proyectos; y dos últimas áreas de proceso para los aspectos de seguridad a nivel operativo en la ingeniería de software.

- OSD. Preparación de la organización para un desarrollo seguro. Las prácticas de esta área están dirigidas a una única meta específica: (SG1) el establecimiento de la capacidad organizativa para desarrollar productos seguros. Estas prácticas están relacionadas con la gobernanza de TI a nivel estratégico.
- SMP. Gestión de proyectos seguros. Las prácticas que se proponen están dirigidas a conseguir dos metas específicas: (SG1), en el nivel táctico, propone la preparación y gestión de las actividades de proyectos de desarrollo software seguro; y (SG2), en el nivel operativo, orientadas a la gestión de los riesgos asociados a la seguridad del producto software La estructura de factores de seguridad que se define en este trabajo está encaminada a detallar y mapear estas dos prácticas específicas de SbD.
- SRTS. Requisitos de seguridad y solución técnica. Mantiene el cumplimiento de dos metas específicas: (SG1) el desarrollo de requisitos de seguridad de los clientes y de una arquitectura y diseño seguros; y (SG2) la implementación del diseño seguro.
- SVV. Verificación y validación de la seguridad. Trata la verificación y validación de la seguridad a través de dos metas específicas: (SG1) realizar la verificación de la seguridad del producto software; y (SG2) llevar a cabo la validación de la seguridad del producto software.

Así, SbD supone una extensión del modelo CMMI-DEV v1.3. Las cuatro áreas de procesos proponen prácticas aplicables en los niveles estratégico, táctico y operativo de la organización Además, su aplicación puede llevarse a cabo de forma independiente o bien de forma integrada con las prácticas genéricas y específicas de las 22 áreas de proceso de CMMI-DEV v1.3. Sin embargo, el marco SbD no concreta

cómo llevar a cabo las prácticas y tampoco describe qué factores son necesarios para su implantación.

En este sentido, los marcos y estándares orientados a la gobernanza y distintos tipos de gestión de TI también aportan prácticas de seguridad que en esta investigación han sido utilizadas para conformar una estructura de factores que facilite la gestión segura de proyectos de ingeniería de software seguro. Esta estructura de factores debe tener las siguientes características: (1) contemplar todas las prácticas SbD y (2) que sean fácilmente integradas con los marcos y estándares que impliquen proyectos de desarrollo software seguro.

Así, en la subsección B, se presentan los marcos y estándares más representativos, estructurados en los tres niveles organizativos definidos; y en la subsección C se presenta el detalle de la estructura de factores y el análisis realizado en el nivel operativo.

B. Marcos y estándares para la gobernanza y gestión de proyectos de desarrollo software seguro

La selección de los marcos y estándares se ha hecho atendiendo a lo extendida que esté su aplicación y a su reconocimiento internacional. Así, en el nivel estratégico, encontramos marcos orientados a la gobernanza de TI. Su objetivo es la evaluación, control y dirección de los activos y recursos de TI. Entre ellos destacan los marcos ISO/IEC 38500 [7], Calder-Moir [8], COSO [9], GRC Capability Model [10], COBIT 5 [11], COBIT QuickStart para PYMES [12] y MAGERIT V3 [13].

En el nivel táctico se han situado las perspectivas de mejora de procesos y de gestión de servicios, ésta última por incluir prácticas para la gestión de proyectos y de la seguridad. Se analizan ISO/IEC 20000 [14], ITIL [15], CMMI-DEV y el estándar internacional ISO/IEC 15504-4 - [16], que describe un modelo de evaluación de los procesos de desarrollo de software definidos en el modelo de referencia ISO/IEC 12207 [17]).

En el nivel operativo se sitúan las perspectivas de gestión de proyectos y gestión de seguridad. Se han analizado los marcos PMBOK [18], PRINCE 2 [19], PSP [20] y TSP [21] Métrica 3 [22], el propio marco SbD [4], las propuestas estatales de seguridad como el ENS [23] o FISMA [24], los estándares ISO/IEC 27000 [25] e ISO/IEC 15408 *Common Criteria* [26], el método de evaluación y gestión de riesgos CRAMM, el modelo de gobernanza de seguridad GASSP (sucesor de GAISP) [27] y el modelo SDL [28].

C. Estructura de factores SbD, y marcos y estándares para la gobernanza y gestión de proyectos de desarrollo software seguro.

La definición de la estructura de factores se ha definido en base a las prácticas propuestas por SbD y los marcos indicados en la subsección B. Se han realizado las siguientes actividades: (1) seleccionar cada una de las prácticas; (2) analizar cada práctica sobre cada marco; (3) preguntar ¿define el marco la práctica o establece mecanismos que permitan su aplicación?; (4) si la respuesta es sí, se definen tantos factores adjuntos a la práctica SbD como aportaciones haga el marco para concretar dicha práctica. Así, tomando como semilla cada práctica SbD, surge el conjunto de factores de seguridad estructurados de acuerdo a los niveles organizativos.

Aunque la investigación llevada a cabo ha realizado el estudio de los factores en los marcos y estándares más representativos, de las cuatro perspectivas en los tres niveles, en este trabajo se presenta el análisis de la presencia de los factores relativos al nivel operativo por tener un vínculo más directo con las metas SG1 y SG2 del área de procesos Gestión de Proyectos Seguros (SMP) del marco SbD.

El análisis de presencia de cada factor pretende: (1) mostrar las aportaciones y carencias de cada marco y estándar en cuanto a la gestión segura de proyectos de ingeniería de software y (2) concretar y completar las prácticas SbD relativas al área de proceso SMP.

Cada factor está identificado por: (1) el carácter F; (2) un código del enfoque del estudio {GB, Gobernanza; GV, Gestión de Servicios; MP, Mejora de Procesos; GP, Gestión de Proyectos; GS, Gestión de Seguridad}; (3) un número secuencial del factor a estudiar; y (4) una breve descripción del factor. Además, el grado de presencia en el marco o estándar se representa mediante un icono:

○ Ausencia del factor en el marco estudiado.

◖ Presencia parcial del factor en el marco estudiado. El marco nombra en algún momento el factor, pero ni lo define ni establece técnicas, métodos o herramientas que permitan su aplicación evaluación y mejora.

● El factor está presente en el marco estudiado de forma completa.

1) Gestion de proyectos: Los objetivos principales de estos marcos son la planificación, el seguimiento y el control de las actividades, los recursos y las personas que participan en los procesos de desarrollo software hasta su finalización, cierre y análisis de las lecciones aprendidas. En este contexto, se han analizado las prácticas SbD en el ámbito de observación de marcos y estándares reconocidos internacionalmente [29] y se definen los factores que se muestran en la Tabla I.

TABLA I. FACTORES DE SEGURIDAD. PERSPECTIVA DE GESTIÓN DE PROYECTOS

F_GP_01 Define factores de seguridad de producto de desarrollo software
F_GP_02 Parametriza las necesidades de seguridad en el proyecto
F_GP_03 Establece objetivos de control de seguridad
F_GP_04 Proporciona mecanismos de control de seguridad
F_GP_05 Proporciona directrices para evaluar la seguridad de la gestión de proyectos de desarrollo de software
F_GP_06 Establece registro de umbrales y valores de seguridad de producto software
F_GP_07 Gestiona la provisión de producto software seguro
F_GP_08 Define una guía de evaluación de seguridad de producto software
F_GP_09 Proporciona guías sobre técnicas de seguridad de producto software en desarrollo

F_GP_10 Gestiona la configuración de activos de seguridad de producto software (PAL)
F_GP_11 Proporciona guías sobre su aplicación en PYMEs
F_GP_12 Establece mecanismos de respaldo y compromiso de la dirección
F_GP_13 Proporciona directrices de competencias y formación en seguridad

Estos factores han sido analizados en cada marco de gestión de proyectos y el resultado se presenta en la Tabla II.

El factor (F_GP_01) revela que, excepto SCRUM, todos los marcos estudiados, incluido SbD, están orientados a procesos.

Los factores F_GP_02 a F_GP_06 se enfocan en el control de la seguridad de los productos software. En este sentido, excepto METRICA 3 y PSP, el resto de los marcos estudiados desde esta perspectiva PMBOK, PRINCE 2, y TSP y SCRUM no contemplan alguna de las prácticas orientadas al control de la seguridad del producto software.

En relación a los factores F_GP_07 a F_GP_09, aunque en las fases de inicio y planificación se establecen umbrales y medidas correctivas para la monitorización y control, éstas no se orientan a la gestión de seguridad sino a la gestión de riesgos del proyecto. En este sentido, se observa en PSP un enfoque claro hacia el producto de desarrollo software. Sin embargo el resto de los marcos no introducen prácticas para la gestión de la provision segura aunque sí introducen técninas y alguna práctica para la evaluación de la seguridad del producto software.

Además, como muestra el análisis del factor F_GP_13, todos los marcos muestran la necesidad de establecer directrices para la definición de perfiles y la formación adecuada. En este sentido, sólo PSP vincula el éxito del proyecto con la definición de las competencias y la formación del personal de desarrollo. Aunque PSP y TSP establecen en la planificación guiones, registros de estado de producto (analizado con los factores F_GP_02, F_GP_03 y F_GP_10) y facilitan una posible re-planificación de las tareas y productos de desarrollo software para PYMEs (factores F_MP_9 y F_MP_11), no concretan parámetros de seguridad. Finalmente, todos los marcos estudiados contemplan la necesidad del respaldo por parte de la dirección (F_GP_12).

TABLA II. FACTORES DE ESTUDIO PARA EL ANÁLISIS DE LAS GUÍAS, ESTÁNDARES Y MARCOS DE GESTION DE PROYECTOS

Factor	PMBOK	PRINCE 2	METRICA 3	PSP	TSP	SCRUM
F_GP_01	◖	◖	◖	◖	◖	○
F_GP_02	◖	◖	◖	◖	○	◖
F_GP_03	○	○	◖	◖	○	○
F_GP_04	◖	◖	◖	◖	○	◖
F_GP_05	○	○	◖	◖	○	◖
F_GP_06	○	○	◖	◖	○	◖
F_GP_07	○	○	◖	○	○	◖
F_GP_08	◖	◖	◖	◖	○	○
F_GP_09	◖	◖	◖	◖	○	○
F_GP_10	○	○	◖	◖	○	○
F_GP_11	○	○	◖	○	○	◖
F_GP_12	◖	◖	◖	◖	◖	◖
F_GP_13	◖	◖	◖	◖	◖	○

2) Gestión de seguridad: esta perspectiva aúna los factores de gestión de seguridad que afectan directamente a los productos de desarrollo software. Por lo tanto, el ámbito de observación en esta perspectiva, como se muestra en la Tabla III, lo forman estándares y marcos de control de seguridad reconocidos a nivel internacional.

TABLA III. FACTORES DE SEGURIDAD. PERSPECTIVA GESTIÓN DE SEGURIDAD

F_GS_01 Política de seguridad de desarrollo de software
F_GS_02 Plan de seguridad del desarrollo de software
F_GS_03 Criterios de evaluación de vulnerabilidades de activos de desarrollo de software
F_GS_04 Criterios de evaluación de seguridad de activos de desarrollo de software
F_GS_05 Criterios de evaluación de riesgos seguridad de desarrollo software
F_GS_06 Declaración de riesgos de seguridad de desarrollo de software
F_GS_07 Declaración de viabilidad de proyecto de desarrollo de software seguro
F_GS_08 Parametrización de seguridad en el desarrollo de software
F_GS_9 Medidas de seguridad desarrollo de software
F_GS_10 Objetivos de control de seguridad de desarrollo de software
F_GS_11 Controles de seguridad desarrollo de software
F_GS_12 Registro de umbrales y valores de seguridad desarrollo de software
F_GS_13 Auditorías de seguridad desarrollo de software
F_GS_14 Alternativas soluciones seguridad desarrollo de software
F_GS_15 Plan de tratamientos de riesgos de seguridad
F_GS_16 Gestión integrada de incidentes de seguridad desarrollo de software
F_GS_17 Gestión de problemas de seguridad desarrollo de software
F_GS_18 Gestión de configuración y activos de seguridad (PAL)
F_GS_19 Gestión de proveedores de producto software seguro

F_GS_20 Gestión de conocimiento de seguridad desarrollo de software
F_GS_21 Informes de seguridad desarrollo de software
F_GS_22 Plan de formación y desarrollo de competencias de seguridad desarrollo de software
F_GS_23 Plan de concienciación seguridad desarrollo de software
F_GS_24 Plan de mejora seguridad desarrollo de software
F_GS_25 Específico para PYMEs

Estos factores de seguridad están estrechamente vinculados con: las vulnerabilidades, los riesgos en cada fase de desarrollo, su monitorización y control a lo largo del ciclo de vida, y los criterios de evaluación de seguridad. La Tabla IV muestra el análisis para: (1) la definición de políticas y planes encaminados a garantizar la seguridad del producto software, (F_GS_01 y F_GS_02); (2) la evaluación de activos de seguridad de desarrollo software, la evaluación de las vulnerabilidades, los riesgos asociados a los productos software como activos seguros (F_GS_03 al F_GS_06); (3) la viabilidad del proyecto, analizada a través del factor F_GS_07; (4) el estudio de los parámetros de seguridad del proyecto, a establecer los objetivos de control, los umbrales de seguridad, los controles, la monitorización, así como las técnicas de medición y registro de la seguridad del producto software (F_GS_08 al F_GS_13); (5) el análisis de las alternativas de solución (F_GS_14 y F_GS_15); (6) la gestión de las incidencias, de las causas raíces, problemas, configuración de activos de seguridad de productos software y la gestión de la provisión de productos de terceros (F_GS_16 al F_GS_19); (7) el análisis de la emisión de informes y la gestión del conocimiento y de las lecciones aprendidas (F_GS_20 y F_GS_21); y (8) la presencia de los planes de formación y concienciación (F_GS_22 y F_GS_23); (9) la presencia de un plan de mejora continua (F_GS_24). El factor F_GS_25 revela que ninguno de los marcos considera específicamente su adaptación a las PYMEs.

TABLA IV. FACTORES DE ESTUDIO PARA EL ANÁLISIS DE LAS GUÍAS, ESTÁNDARES Y MARCOS DE GESTION DE SEGURIDAD

Factor	SbD (SMP)	ISO/IEC 27000	ISO/IEC 15408 CC	CRAMM	FISMA	ENS	GASSP	SDLC
F_GS_01	◖	◖	◖	◖	◖	◖	◖	○
F_GS_02	◖	◖	◖	○	○	○	○	○
F_GS_03	◖	◖	◖	○	○	○	○	◖
F_GS_04	◖	◖	◖	◖	◖	◖	◖	◖
F_GS_05	◖	◖	◖	◖	◖	◖	◖	◖
F_GS_06	◖	◖	◖	◖	◖	◖	◖	◖
F_GS_07	◖	◖	○	○	○	○	○	◖
F_GS_08	◖	○	○	○	○	○	○	◖
F_GS_09	◖	○	◖	○	○	◖	◖	◖
F_GS_10	◖	○	◖	◖	○	◖	◖	◖
F_GS_11	◖	◖	◖	○	○	○	○	◖
F_GS_12	◖	○	○	○	○	○	○	◖
F_GS_13	◖	◖	◖	◖	◖	◖	◖	◖
F_GS_14	◖	◖	◖	○	○	○	○	◖
F_GS_15	◖	◖	◖	◖	◖	◖	◖	◖
F_GS_16	◖	◖	◖	○	○	○	○	◖
F_GS_17	◖	◖	○	○	○	○	○	◖
F_GS_18	◖	○	○	○	○	○	○	◖
F_GS_19	◖	◖	◖	○	○	◖	○	◖
F_GS_20	◖	◖	○	○	○	○	○	◖
F_GS_21	◖	◖	◖	◖	◖	◖	◖	◖
F_GS_22	◖	◖	◖	○	◖	◖	○	◖
F_GS_23	◖	◖	◖	◖	◖	◖	◖	◖
F_GS_24	◖	◖	◖	◖	◖	◖	◖	◖
F_GS_25	○	○	○	○	○	○	○	○

IV. CONCLUSIONES

La causa raíz de la mayoría de los problemas de seguridad de los sistemas de información está en el desarrollo del software implicado. Los fallos de seguridad, además de ocasionar pérdidas, potencian la vulnerabilidad de los sistemas de información y, por lo tanto, tienen una mayor probabilidad de que se materialicen las amenazas a las que está sometido.

La gestión de la seguridad en los proyectos de desarrollo software se debe contemplar desde una doble perspectiva: la gestión de la seguridad del proyecto y la gestión de la seguridad del producto. En este sentido, los marcos y estándares estudiados tratan en profundidad los procesos de gestión encaminados a la seguridad del proyecto. Sin embargo, estos marcos no profundizan en la definición de prácticas enfocadas a la gestión de la seguridad del producto software.

Las prácticas propuestas por SbD se enfocan a la seguridad en el desarrollo software y deben ser observadas desde las perspectivas estratégica, táctica y operativa utilizando marcos y estándares de gobernanza y gestión específicos en cada nivel organizativo. El resultado de esta observación aporta una estructura de factores de seguridad aplicables a nivel operativo en la gestión segura de los proyectos de ingeniería del software.

Se observa que prácticamente la totalidad de los factores son compartidos por los marcos propuestos, estableciéndose así el vínculo de observación deseado. Sin embargo, también se observa que en la mayoría de los casos estos factores, se enuncian pero no están detallados, se enfocan a la seguridad del

proyecto y no del producto, o hacia la gestión del riesgo y no de la seguridad.

Por lo tanto, es necesario definir una base de conocimiento que detalle cada factor las características, métodos y guías de aplicación, indicadores de cumplimiento, métricas, etc, que facilite su implantación en la gestión de la seguridad de proyectos orientada al desarrollo de software seguro.

AGRADECIMIENTOS

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

REFERENCIAS BIBLIOGRÁFICAS

[1] Standish, Goup, «CHAOS 2013. Manifiesto. Think Big, Act Small,» The Standish Group International, 2013.

[2] Neumman, «The Need for a National Cybersecurity Research and Development Agenda,» Inside Risks 220, CACM 53, 2, February 2010, 2010.

[3] Ponemon Institute, «The State of Application Security A Research Study by Ponemon Institute LLC and Security Innovation,» Security Innovation, 2013.

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

[5] SEI, «CMMI® para Desarrollo, Versión 1.3. CMMI-DEV, V1.3. Mejora de los procesos para el desarrollo de mejores productos y servicios,» SEI, Pittsburgh, 2010b.

[6] M. Arnold, «Recursos para la investigación sistémico/constructivista,» Cinta moebio 3, pp. 31-39, 1998.

[7] ISO/IEC 38500, «ISO/IEC 38500:2008 Corporate governance of information technology,» ISO/IEC, 2008.

[8] A. Calder, IT Governance: Implementing Frameworks and Standards for the Corporate Governance of IT, 2008.

9] AICPA, «COSO Enterprise Risk Management -- Integrated Framework,» AICPA, 2004.

[10] S. Mitchell y C. Stern, Modelo de Capacidad GRC, 2013.

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

[12] ISACA, «COBIT QUICKSTART, 2ND EDITION,» ISACA, 2007.

[13] CSAE, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método,» Ministerio de Hacienda y Administraciones Públicas, 2012.

[14] ISO/IEC, «ISO/IEC 20000-1:2011 Information technology — Service management — Part 1: Service management system requirements,» ISO/IEC, 2011.

[15] TSO, An Introductory Overview of ITIL 2011, London: itSMF, 2012.

[16] ISO/IEC, «ISO/IEC 15504-4:2004. Information Technology – Process Assessment – Part 4: Guidance on use for process improvement and process capability determination,» 2004.

[17] ISO/IEC, «ISO/IEC 12207:2008 Systems and software engineering – Software life cycle processes,» 2008.

[18] PMI, Project Management Institute. A guide to the project management body of knowledge (PMBOK guide). 4th Edition, Newton Square: Project Management Institute, 2009.

[19] OGC, Éxito en la gestión de proyectos con PRINCE2, 2009.

[20] W. S. Humphrey, Introduction to the personal software process, SEI Series in Software Engineering, Reading, MA: Addison-Wesley, 1997.

[21] W. S. Humphrey, Introduction to the team software process., SEI Series in Software Engineering, Reading, MA: Addison-Wesley, 2002.

[22] PAe, «Metrica Versión 3,» 2001. [En línea]. Available: http://goo.gl/Q1d8D3.

[23] BOE, «Esquema Nacional de Seguridad,» BOE, 2010.

[24] NIST, «Guide for Assessing the Security Controls in Federal Information Systems and Organizations,» NIST, Gaithersburg, MD 20899-8930, 2010.

[25] ISO/IEC, «ISO/IEC 27000: 2014,» 2014. [En línea]. Available: http://goo.gl/0o7JgU.

[26] ISO/IEC, «ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security —,» 2009. [En línea]. Available: http://standards.iso.org/ittf/licence.html#en.

[27] ISSA, «GAISP. Generally Accepted Information Security Principles. V3,» ISSA, 2004.

[28] Microsoft, «SDL. Security Development Lifecycle,» 2014. [En línea]. Available: http://goo.gl/mhdqF.

[29] CPIICM, «Estudios internacionales sobre el estado actual de la dirección y gestión de proyectos,» CPIICM, Madrid, 2013.

[1]