Método de integración para soportar la armonización de múltiples modelos y estándares

César Pardo[1,2], Félix García[2], Francisco J. Pino[1,2], Mario Piattini[2] y Maria Teresa Baldassarre[3]

[1] Grupo de Investigación IDIS
Facultad de Ingeniería Electrónica y Telecomunicaciones,
Universidad del Cauca, Calle 5 No. 4 - 70.
Popayán, Cauca, Colombia.
{cpardo, fjpino}@unicauca.edu.co

[2] Grupo de Investigación Alarcos
Instituto de Tecnologías y Sistemas de Información - ITSI,
Universidad de Castilla-La Mancha, Paseo de la Universidad 4, Ciudad Real, España
{Felix.Garcia, Mario.Piattini}@uclm.es

[3] Departamento de Informática, Universidad de Bari.
SER&Practices, SPINOFF, Via E. Orabona 4, 70126, Bari, Italy
baldassarre@di.uniba.it

Resumen. Actualmente, el sector empresarial está cada vez más interesado en implementar múltiples modelos y estándares (como marcos de referencia) para mejorar sus procesos con el objetivo de incrementar el nivel de competitividad y garantizar el adecuado control, gestión y rendimiento de las actividades, procesos y procedimientos en distintas áreas y jerarquías organizacionales. Sin embargo, actualmente las organizaciones llevan a cabo la implementación de dos o más marcos de forma separada, sin identificar: (i) sus diferencias y semejanzas, (ii) la forma en que pueden complementarse, (iii) la reducción del costo de implementación, (iv) rápido retorno de la inversión, entre otros. En ese sentido, este artículo presenta un método de integración formado por un conjunto de actividades, tareas, roles y criterios para soportar la integración sistemática de múltiples marcos. Asimismo, se presenta un caso de estudio en el que se aplicó el método definido para la definición de un marco integrado para el gobierno de las Tecnologías y Sistemas de Información (TSI) aplicable al sector bancario. Además, se presenta un extracto del marco integrado obtenido, beneficios y lecciones aprendidas.

Palabras clave: Armonización de múltiples modelos, estándares, marcos de referencia, integración de múltiples modelos y estándares, COBIT, ITIL, RISK IT, VAL IT, ISO 27002, BASEL II.

1 Introducción

La mejora de procesos software se ha convertido en un área fundamental en las organizaciones con el fin de mejorar su desempeño en materia de calidad. En Ingeniería del Software se han definido múltiples modelos y estándares[1] que permiten mejorar distintas necesidades empresariales, por ejemplo: gestión de la calidad como ISO 9001, gestión de la calidad del software como ISO 90003, CMMI e ISO 12207, gestión de la seguridad de la información como la familia de marcos ISO/IEC 27000, gobierno de las Tecnologías de la Información (TI) como ISO 20000, ITIL y COBIT, entre otros.

Aunque el número de marcos de referencia definidos actualmente puede parecer excesivo, la heterogeneidad de marcos permite que las organizaciones puedan disponer de un amplio abanico de "medicinas" para superar distintas "sintomatologías" o necesidades. Por ejemplo, si una organización decide que ITIL no se adapta a sus necesidades de gestión de los servicios de TI, la organización puede elegir un marco de referencia parecido, incluso con mayor detalle como COBIT [1]. Asimismo, las organizaciones pueden implementar más de un marco con el objetivo de mejorar y complementar sus prácticas, por ejemplo, implementar marcos diferentes como CMMI-ACQ e ISO 27002 para mejorar la gestión de la adquisición de productos y servicios y la gestión de la seguridad de la información respectivamente.

Para llevar a cabo la implementación de múltiples marcos se requiere de metodologías específicas que permitan soportar *qué* hacer y *cómo* llevar a cabo la armonización e integración de los elementos de proceso (EP) de múltiples marcos. Sin embargo, los trabajos existentes sobre el tema, abordan especialmente la definición de técnicas de armonización enfocadas a soportar la comparación de modelos específicos, por ejemplo ISO 12207 y CMMI [2]. En cuanto a los métodos y/o técnicas de integración, las propuestas definidas son muy pocas y sólo permiten abordar la integración de marcos específicos con un número máximo de dos marcos, por ejemplo ISO 9001:2000 y CMMI [3]. Esta situación implica que las compañías lleven a cabo la institucionalización de un nuevo marco por separado y sin tener en cuenta: (i) los esfuerzos de mejora previamente realizados, (ii) similitudes y diferencias entre marcos, (iii) rápido retorno de la inversión, entre otros.

Teniendo en cuenta lo anterior y con el objetivo de soportar la armonización de múltiples marcos, en este artículo se describe un método de integración que permite que las compañías puedan llevar a cabo la unión y/o combinación de múltiples marcos y así mejorar distintas áreas de negocio de manera sistemática e integrada. El método definido describe un proceso formado por un conjunto de actividades, tareas, roles y criterios de integración que permiten soportar paso a paso y a un bajo nivel de abstracción la integración de los EP de múltiples marcos de referencia. Este método forma parte de un framework para la armonización de múltiples marcos [4], que incluye: (1) una técnica de homogeneización que permite solucionar las diferencias a nivel de las estructuras de procesos definidas por marcos diferentes [5], (ii) un método

[1] En adelante, con el objetivo de unificar los diferentes términos usados por las diferentes organizaciones y autores para referirse a los modelos, usaremos el término genérico "marco" para hacer referencia a: modelos y estándares.

de comparación que permite identificar las diferencias y similitudes entre marcos [6], un método para analizar el cumplimiento de los marcos con relación a las características y subcaracterísticas de calidad de producto [7], y el método de integración definido en este artículo. El método de integración ha sido aplicado para la definición de un marco integrado para el gobierno de las Tecnologías y Sistemas de Información (TSI) destinado al sector bancario y denominado ITGSM [8]. La definición de este marco se ha llevado a cabo a través de la integración de seis marcos de referencia: COBIT 4.1 [9], BASEL II [10], VAL IT [11], ITIL V.3 [12], RISK IT [13] e ISO 27002 [14].

Aparte de esta introducción, el artículo está organizado como sigue: en la sección 2 se presenta un resumen de los trabajos relacionados. La sección 3 presenta el método de integración describiendo las actividades, tareas, roles y criterios de integración que lo conforman. La sección 4 presenta un resumen de la aplicación del método de integración en la definición de un marco integrado de marcos para soportar el gobierno de las TSI en el sector bancario. Asimismo, se presenta un resumen de la estructura del modelo integrado. Por último, la sección 5 presenta la discusión, lecciones aprendidas, conclusiones y trabajos futuros.

2 Trabajos Relacionados

En base a los resultados obtenidos a partir de una revisión sistemática de la literatura realizada acerca de los esfuerzos y propuestas relacionadas con la armonización de múltiples marcos [15], la Tabla 1 muestra la clasificación de algunos trabajos de acuerdo al conjunto de métodos y técnicas que estos definen, por ejemplo técnicas para abordar las diferencias estructurales, comparación, integración, entre otros. La clasificación organiza los trabajos relacionados en dos grupos: *técnicas* y *métodos* de acuerdo a su nivel de formalismo y detalle. En ese sentido, se tuvo en cuenta: (i) que los métodos indican procedimientos generales y (ii) las técnicas dan soporte a los procedimientos específicos. Es decir, un método es un procedimiento que generalmente se orienta hacia la realización de un propósito específico, mientras que las técnicas dan soporte a las diferentes maneras de aplicar un método.

Tabla 1. Métodos y Técnicas identificadas.

	Trabajos relacionados	Sinónimos encontrados	Método/ Técnica	Referencia
1	Homogeneización	Solución de diferencias estructurales	SI	[5]
1	Comparación	Mapping/Alineación	SI	[6], [16, 17], [18]
2	Integración	Combinación/Fusión/Unificación	NA	[19], [3, 20], [18]
3	Otros estudios: Marcos Integrados/Universales		NA	[21], [22], [23]

NA: No se encontró ninguna evidencia formal.

Del análisis de estos trabajos se observó que aunque es posible encontrar algunas propuestas para soportar la armonización de múltiples marcos, ninguna describe un método, procedimiento o técnica detallada para abordar las tareas de integración a un

bajo nivel de abstracción y que sea aplicable a cualquier tipo de marco independientemente de su enfoque. Con relación a la categoría *otros estudios*, se han podido encontrar estudios que proponen marcos integrados/universales. Sin embargo, estos no describen el enfoque de integración utilizado para soportar la integración de los marcos involucrados.

El aporte de este trabajo es proponer un *método de integración* detallado que permite soportar la integración de múltiples marcos de referencia de procesos siguiendo un enfoque sistemático e independiente del enfoque de aplicación de los marcos que sean integrados. Es decir, que permite apoyar a las organizaciones la integración no solo de las recomendaciones y prácticas de marcos de software, sino también los marcos relacionados con los procesos de gestión, gobierno de las TSI, seguridad, entre otros.

3 Método de Integración

El propósito de este método es guiar paso a paso a la hora de realizar la integración de múltiples marcos. A continuación se describen las actividades y tareas que conforman el método de integración, cuyos roles son los definidos en la técnica de homogeneización y en el método de comparación propuestos en [5, 6]:

- *Diseñar la integración*: esta actividad involucra las tareas: (i) fijar los Elementos de Proceso Sensibles a ser Integrados (EPSI), (ii) fijar el orden de la integración a seguir (basado en las necesidades de la organización o criterio de priorización) y (iii) fijar una plantilla de integración. Los EPSI se establecen a partir de los resultados obtenidos al comparar dos o más marcos y analizar las necesidades de armonización identificadas.
- *Definir/Establecer un criterio para llevar a cabo la integración de los EPSI*: esta actividad involucra la definición y establecimiento de un conjunto de reglas o criterios que faciliten la integración de los EPSI. La sección 3.1 detalla algunos criterios de integración definidos.
- *Llevar a cabo la integración*: esta actividad involucra las tareas: (i) llevar a cabo un análisis profundo de las descripciones que conforman los EPSI, (si es posible, llevar a cabo un análisis sintáctico), (ii) aplicar los criterios de integración y resolver las discrepancias entre los EPSI involucrados (véase sección 3.1), (iii) verificar y validar los resultados. Esta actividad sigue un enfoque iterativo e incremental para facilitar la gestión durante la integración de los EPSI.
- *Analizar los resultados de la integración*: esta actividad involucra la realización de ajustes a la integración de los marcos (si es necesario).
- *Presentar el modelo integrado*.

La Figura 1 presenta los roles, actividades y algunos productos de trabajo definidos en la técnica de integración definida con SPEM 2.0 como estándar de notación.

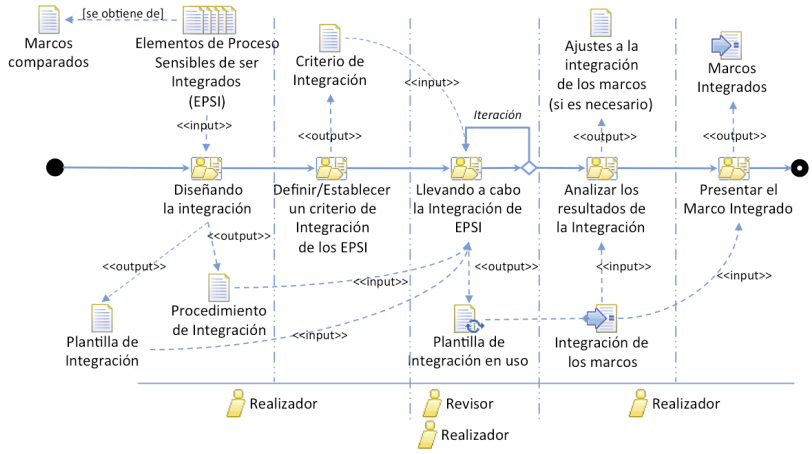

Fig. 1. Diagrama de actividad del método de integración.

3.1 Criterios de integración para soportar la unificación de EPSI

Con el objetivo de facilitar la integración de las descripciones y/o recomendaciones contenidas en las prácticas de los marcos a ser integrados, el método de integración define un conjunto de reglas de integración que permiten decidir que acción realizar en situaciones específicas durante la integración de los EPSI involucradas. La implementación de los criterios predefinidos no es obligatorio, por lo que los usuarios de este método tienen la libertad de establecer sus propios criterios. Asimismo, estos criterios sólo describen recomendaciones para ciertas situaciones y no representan un criterio aplicable en todos los casos. Los criterios de integración definidos son:

a). *Cuando la descripción de un EPSI definido en un marco A está soportado y contenido en la descripción de un EPSI definido en un marco B*:

   i). Cuando el EPSI del marco A ofrece una descripción más detallada que el EPSI del marco B, el EPSI de B podría ser absorbido por el EPSI de A.

   ii). Cuando el EPSI del marco A ofrece una descripción igual (en detalle) que la descripción del EPSI del marco B, el EPSI de B podría ser absorbido por el EPSI de A o viceversa.

   iii). Cuando el EPSI del marco A ofrece una descripción con menos detalle que el EPSI del marco B, el EPSI de A podría ser absorbido por el EPSI de B.

b). *Cuando la descripción de un EPSI definido en un marco A no está contenido dentro de la descripción de un EPSI definido en un marco B:*

   i). Se integra el EPSI del marco A como un nuevo EP de acuerdo a la estructura de procesos del marco B.

Los criterios de integración definidos se basan en el resultado obtenido después de llevar a cabo la comparación de las descripciones de los EP de dos o más marcos. En ese sentido, la comparación de las descripciones se debe realizar teniendo en cuenta la calidad y detalle de las descripciones de los EP involucrados. Una descripción de un EP de un marco A es más completa que la descripción de un EP de B cuando tiene un

mayor alcance, incluye más objetivos y requisitos para llevar a cabo una actividad específica. Por otra parte, el detalle de un EP está caracterizado por su nivel de abstracción, por ejemplo las actividades, tareas, pasos, roles y demás elementos que detallen el EP. En ese sentido, la descripción de un EP de un marco A puede ser más completa que la descripción de un EP de un marco B. Sin embargo, el EP de A no necesariamente llega a ser más detallado que A en todos los casos. Este tipo de situaciones pueden presentarse durante la comparación, en ese sentido, se hace necesario establecer criterios de integración mucho más específicos. Por ejemplo, el criterio (a.iii) podría detallarse aun más con un criterio alterno (a.iii.i) de la siguiente manera: si el EPSI del marco A ofrece una descripción con menos detalle que el EPSI del marco B, *pero la descripción del EPSI de A es mejor que la descripción del EPSI de B*, el realizador podría elegir la descripción del EPSI de A y complementarlo con el detalle del EPSI de B. El *realizador* es libre de establecer más criterios alternos según sea necesario.

Por otra parte, la integración de un EPSI de un marco A con respecto al EPSI de un marco B está influenciado por las necesidades de armonización e integración identificadas. Asimismo, es responsabilidad del *realizador*, establecer un sistema de versiones o control de cambios que permita gestionar la adaptación de las descripciones de los EPSI integrados. La Figura 2 muestra el procedimiento para soportar la integración de los EPSI a partir de los criterios de integración definidos.

En la siguiente sección se presenta la validación del método de integración descrito anteriormente. El método ha sido utilizado para soportar la definición de un marco integrado para el gobierno de las TSI aplicable al sector bancario. Para ello, el método de integración ha soportado la unificación de las mejores prácticas definidas en los marcos: ITIL V3, ISO 27002, BASEL II, RISK IT, VAL IT y COBIT 4.1.

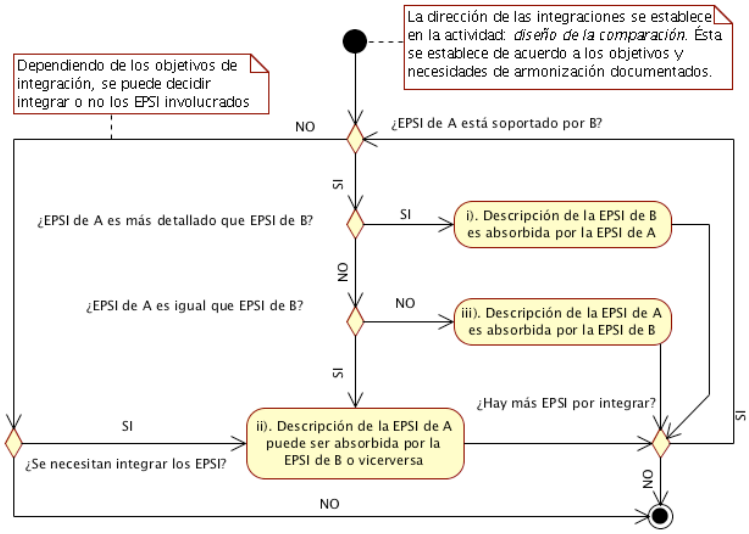

Fig. 2. Procedimiento para soportar la integración de los EPSI.

4 Integrando múltiples marcos para la definición de un marco para el gobierno de las TSI en el sector bancario.

El marco para el gobierno de las TSI o Information Technology Governance Model for Banking – ITGSM (ver [8]) ha sido definido a partir de la ejecución de una estrategia de armonización conformada por la alineación sistemática y estratégica de tres métodos y técnicas, ellas son: una técnica de homogeneización [5], una técnica de comparación [6] y el método de integración presentado previamente. La estrategia de armonización obtenida ha sido definida a partir de la ejecución de un proceso de armonización que permite gestionar la ejecución de las actividades enfocadas a la definición de una estrategia que permita llevar a cabo la armonización de múltiples marcos presentado en [4]. Un trabajo más detallado de la estrategia de armonización utilizado para definir ITGSM se presenta en [24].

Dado que las técnicas de homogeneización y comparación ya han sido presentadas detalladamente en trabajos previos ([5] y [6]) y su aplicación en la definición de ITGSM no ha implicado algún cambio o modificación, en este artículo se profundizará en la aplicación del método de integración. La Figura 3 muestra la relación establecida entre el método de integración y las técnicas de homogeneización y comparación.

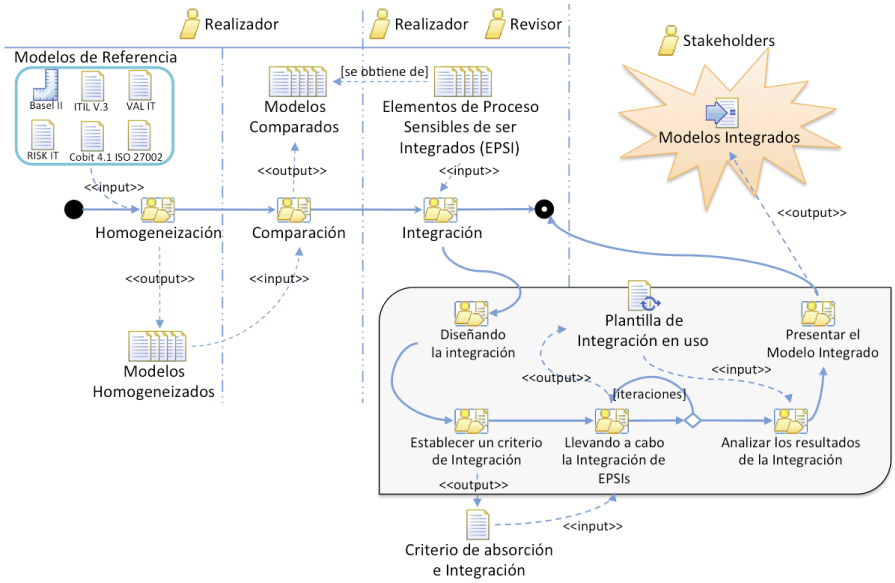

Fig. 3. Relación entre el método de integración y las técnicas de homogeneización y comparación.

4.1 Homogeneización y Comparación

Antes de llevar a cabo la integración de los EPSI de los marcos involucrados, fue necesario conciliar las diferencias encontradas entre sus estructuras de proceso. Esto se llevó a cabo a través de la técnica de homogeneización y estructura común de elementos de proceso (ECEP) descritos en [5]. La homogeneización ha permitido poner en armonía las estructuras de proceso y reducir la complejidad de las comparaciones entre los marcos involucrados.

Después de llevar a cabo la homogeneización de los marcos, el realizador y revisor llevaron a cabo su comparación a través de la técnica de comparación presentada en [6]. Esta técnica permitió identificar los EP relacionados. Con el objetivo de minimizar la complejidad de las comparaciones, el realizador y revisor llevaron a cabo la comparación de los marcos en grupos de dos de la siguiente manera: (i) se compararon los principios de BASEL II y los procesos descritos en COBIT (identificando los principios de BASEL que soportaban el cumplimiento de los procesos de COBIT). Los procesos de COBIT 4.1 que soportaron el cumplimiento de los principios de BASEL II se utilizaron para llevar a cabo las comparaciones con: (ii) VAL IT, (iii) RISK IT, (iv) ISO 27002 e ITIL V3. En la primera comparación se encontraron 44 (procesos) relacionados, los que fueron reforzados a partir de las comparaciones con los marcos siguientes. La definición de ITGSM se basó en la integración del conjunto de resultados obtenido en las comparaciones de los marcos involucrados.

4.2 Diseño de la Integración

A partir de los resultados obtenidos en la comparación, el *realizador* identificó los EP sensibles de ser integrados o EPSI. El grupo de entidades de proceso sensibles de ser integradas está conformado por los elementos de proceso que permiten solucionar las necesidades y objetivos de armonización identificados previamente en el proceso de armonización. Para este caso los EPSI fueron los principios definidos en BASEL II y los EP de COBIT, ISO 27002, ITIL, RISK IT y VAL IT que estuvieran relacionados. Una vez identificados los EPSI, el *realizador* llevó a cabo su integración a través de la aplicación del método de integración definido bajo la supervisión permanente del *revisor*. Con el fin de reducir la complejidad durante la integración de los EPSI, el *realizador* siguió el enfoque iterativo e incremental del método de integración. El enfoque iterativo permitió gestionar la ejecución de los integraciones en grupos de dos marcos hasta terminar con todos los marcos involucrados. El enfoque incremental soportó la integración y evolución de la plantilla de integración, la cual creció con la realización de cada iteración hasta obtener el producto final o marco integrado.

4.3 Realización de la Integración

La integración se llevó a cabo a nivel de los EP comparados (procesos y actividades) de cada marco, y al igual que en la ejecución de las comparaciones, el enfoque iterativo e incremental facilitó la gestión sistemática de los EPSI involucrados. La

Figura 4 resume paso a paso el trabajo realizado durante la ejecución de las iteraciones de integración.

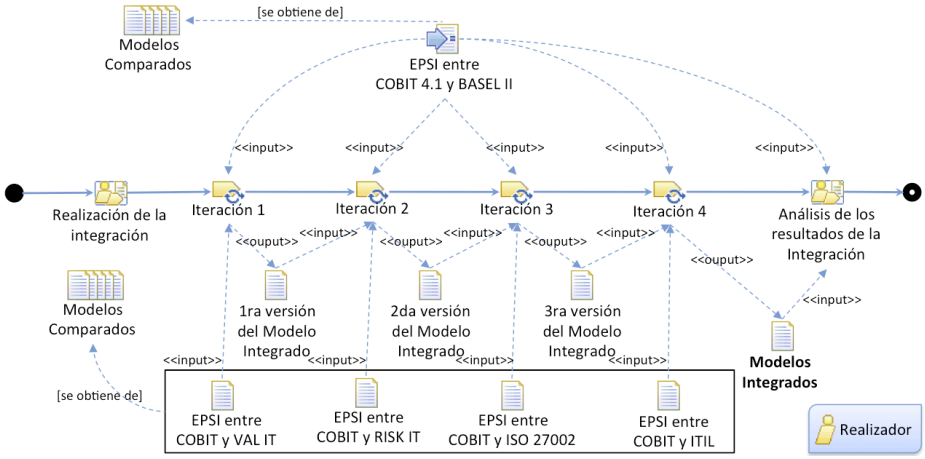

Fig. 4. Trabajo realizado para integrar los EPSI.

Para integrar las descripciones de los EPSI, el *realizador* siguió el conjunto de criterios de integración definidos en la sección 3.1. Los criterios permitieron que el *realizador* conociera la forma de abordar ciertas situaciones originadas durante la integración de los EPSI. La definición de estos criterios fue fundamental para llevar a cabo la integración adecuada de los marcos. Como lección aprendida fue posible notar que el conocimiento previo del realizador en los marcos involucrados y su experiencia en el sector de la supervisión bancaria, ha eliminado la necesidad de capacitación en el uso e implementación de los marcos involucrados.

La Tabla 2 muestra un ejemplo de cómo es aplicado un criterio de integración para soportar la combinación del objetivo de control PO9.1 definido en COBIT 4.1 y el principio de riesgo operativo 1 (PRO1) de BASEL II. Asimismo, la Tabla 2 presenta un ejemplo de la adaptación realizada sobre la descripción de PO9.1 de acuerdo a los requisitos de PRO1.

Como se puede observar en la Tabla 2, PO9.1 soporta el cumplimiento de la descripción de PRO1 definido por BASEL II. En ese sentido, de acuerdo al criterio de integración establecido el método de integración, el elemento de proceso PO9.1 de COBIT podría ser absorbido por el PRO1 de BASEL II. Sin embargo, dado que el objetivo principal de armonización se enfocó hacia la definición de un marco para el gobierno de las TSI aplicable al sector bancario, el *realizador* llevó a cabo la adaptación de las descripciones de los EPSI involucrados. Esto permitió armonizar las diferencias semánticas y definir las prácticas del nuevo marco de acuerdo a los principios definidos por BASEL II.

Tabla 2. Aplicación del criterio de integración al PO9.1 definido en COBIT 4.1 y PRO1 de BASEL II.

BASEL II: Riesgo operativo 1: El Consejo de administración deberá conocer los principales aspectos de los riesgos operativos para el banco y deberá aprobar y revisar periódicamente el marco que utiliza el banco para la gestión de este riesgo.			
Marco	**EPSI**	**Criterio**	**Adaptación**
COBIT	PO9.1: Marco de Trabajo de Administración de Riesgos:	Se cumple el criterio (a-i, ver sección 3.1), por lo tanto el objetivo de control se mantiene. Sin embargo, se realiza una pequeña *adaptación* en su descripción.	*Velar por el establecimiento de un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.*

La Tabla 3 presenta la estructura usada por ITGSM para organizar las descripciones de los procesos y actividades de los marcos que dan soporte a los principios de BASEL II. Asimismo, muestra un extracto de algunos procesos definidos por ITGSM. Un resumen más detallado de ITGSM se presenta en [8].

Tabla 3. Extracto de la Estructura General de ITGSM.

PR B-II	Procesos	**Prácticas que dan soporte al cumplimiento de los principios de BASEL II**				
	ID del Proceso y Descripción	COBIT 4.1	VAL IT	RISK IT	ISO 27002	ITIL V.3
PR1	P2: Conocer, aprobar y velar por el cumplimiento de un marco de trabajo de administración de riesgos. El marco de trabajo documenta un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales.	PO9.1 PO9.2	IM1.2	RG1.5 RG1.7 RG1.8 RG3.3 RG3.4 RE1.1 RR1.3 RR3.4	Cláusulas:4. 1 5.1 13.1 14.1.1	SS9.5
PR2	P4: Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones, incluyendo evaluaciones de Auditoría Interna y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.	ME2.1 ME2.2	-NA-	RG1 RE2 RR1.2 RR1.3	Cláusulas: 5.1 6.1.8 15.2 15.3	-NA-
PR4	P17: El monitoreo efectivo de riesgos se retroalimenta de diferentes fuentes de conocimiento, entre ellas, las que resultan del monitoreo del desempeño de TI. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones o eventos que puedan llegar a materializarse en riesgos.	ME1.2 ME1.3 ME1.4	VG5 PM5 IM9	RE1.5 RR1.2	-NA-	SD3 SD4.2 ST4.5 SO5 CSI9.3

Acrónimos utilizados:
(1) PR B-II= Principios de BASEL II,
(2) COBIT 4.1: PO= Plan and Organize, ME= Monitor and Evaluate, DS= Deliver and Support,
(3) VAL IT: PM= Portfolio Management, IM= Investment Management, VG= Value Governance,
(4) RISK IT: RG= Risk Governance, RE= Risk Evaluation, RR= Risk Response,
(5) ITIL V.3: SD= Service Design, SS= Service Assets, SO= Service Operations, CSI=Continual Service Improvement, ST=Service Transition,
(6) NA= No Aplica.

4.4 Análisis y presentación de resultados

En base a los resultados obtenidos y con el objetivo de aumentar la fiabilidad de las integraciones, el revisor realizó un análisis de las iteraciones realizadas, para posteriormente presentar el marco obtenido a los *stakeholders* o partes interesadas.

Como resultado de la ejecución del método de integración se obtuvo un marco unificado para el gobierno de las TI y la banca llamado ITGSM. ITGSM cumple con los principios de riesgo operacional establecidos por BASEL II y las prácticas de diferentes marcos para dar soporte a un conjunto de características como: (i) Gestión de la inversión - VAL IT, (ii) Gestión de Riesgos de TI – RISK TI, (iii) Gestión de la seguridad de la información - ISO 27002 y soporte a la (iv) Gestión del ciclo de vida de los servicios- ITIL V3.

Actualmente, ITGSM define una estructura de 44 procesos orientados hacia la banca. Sin embargo, la versión 1.0 de ITGSM describe en detalle las descripciones, propósito general, objetivos específicos y actividades de 22 procesos, los 22 procesos restantes están actualmente en proceso de definición. La Tabla 3 presenta una vista general de la estructura y algunos procesos de ITGSM. Un resumen detallado de ITGSM se presenta en [8].

La Tabla 4 presenta un extracto del proceso 2 de ITGSM presentado en [8], este proceso describe las prácticas sugeridas para apoyar *la gestión de riesgos de TI como parte de la conciencia y las responsabilidades de la junta directiva en una organización*. El proceso está organizado de la siguiente manera: título del proceso, el principio de Basilea II que ITGSM cumple, objetivo general, objetivos específicos y prácticas de los marcos integrados que soportan el cumplimiento del principio. Para facilitar la trazabilidad de los EP utilizados para definir cada actividad, ITGSM referencia el nombre del EP integrado.

5 Discusión y Conclusiones

En este artículo se presentó un método para soportar la integración de múltiples marcos. El método de integración presentado describe un proceso que detalla un conjunto de actividades, tareas y roles para soportar paso a paso la integración de múltiples marcos. Asimismo, define los criterios de integración necesarios para abordar la integración de los EP sensibles de ser integrados. El método de integración ha sido aplicado en un caso de estudio para la definición de un marco unificado llamado ITGSM, el cual integra y armoniza a un bajo nivel de abstracción las mejores prácticas descritas en seis marcos de referencia: BASEL II, COBIT 4.1, VAL IT, RISK IT, ISO 27002 e ITIL V.3. El método de integración presentado en este artículo ha mostrado ser extremadamente útil para las organizaciones y consultores que planeen llevar a cabo la armonización e integración de múltiples marcos.

Además de los beneficios obtenidos gracias al proceso sistemático definido por el método de integración, el enfoque iterativo incremental utilizado como procedimiento para gestionar la actividad relacionada con la integración de los EPSI trajo algunos beneficios como:

(i). *Reducción de la complejidad originada al integrar múltiples marcos* mediante la definición y establecimiento de iteraciones que permitieron gestionar de forma ágil y adecuada la integración de los EPSI.

(ii). *La supervisión constante* del *revisor* permitió verificar y validar la fiabilidad de los resultados y la aplicación del método de integración.

(iii). La plantilla de gestión de las iteraciones de integración facilitó la *trazabilidad* de cada iteración de integración.

(iv). *La gestión enfocada y dirigida por los objetivos de armonización* permitió obtener resultados alineados con las necesidades identificadas.

Tabla 4. Extracto del Proceso 2 definido en ITGSM presentado en [8].

Proceso 2: Gestión de riesgos de las TSI como parte de la conciencia y responsabilidades de la Junta Directiva			
Que responde al principio 1 de riesgo operativo - BASEL II: El Consejo de administración deberá conocer los principales aspectos de los riesgos operativos para el banco y deberá aprobar y revisar periódicamente el marco que utiliza el banco para la gestión de este riesgo.			
Objetivo General: Apoyar la evaluación y administración de los riesgos de las TSI buscando la aprobación por parte del Consejo de Administración de un marco de gestión de riesgos adecuado.			
Objetivo Específico: Conocer, aprobar y velar por el cumplimiento de un marco de trabajo de administración de riesgos de las TSI aplicable a toda la organización. El marco de trabajo documenta un nivel común y acordado de riesgos de las TSI, sus estrategias de mitigación y definición de umbrales aceptables de riesgo.			
	Actividades		**Referencia**
Actividades orientadas al Gobierno de las TSI (COBIT)			
2.1	Marco de trabajo de administración de riesgos aprobado	Velar por el establecimiento de un marco de trabajo de administración de riesgos de TI que esté alineado al marco de trabajo de administración de riesgos de la organización.	PO9.1
2.2	Establecimiento del contexto de riesgos	Establecer el contexto en el cual el marco de trabajo de evaluación de riesgos se debe aplicar.	PO9.2
Actividades orientadas a gestionar la inversión de TI (VAL IT)			
2.3	Desarrollar un programa inicial de conceptos de negocio	Solicitar el desarrollo de un programa inicial de conceptos de casos de negocio para describir los resultados esperados de las inversiones realizadas, las asunciones claves que deben ser consideradas y los riesgos que deben ser identificados, impactos potenciales y las estrategias de mitigación.	IM1.2
Actividades orientadas a la gestión de riesgos específicos de TI (RISK IT)			
2.4	Aprobar la tolerancia a riesgos de TI.	La Gerencia debe aprobar los niveles de tolerancia a los riesgos relacionados con las TSI, de acuerdo a los umbrales de aceptación de riesgo empresariales.	RG1.5
2.5	Promover una cultura de conciencia de los riesgos de TI.	Fomentar la creación y promoción efectiva de una cultura de responsabilidad de los riesgos relacionados con TI, esto requiere de comunicación, organización y estructuras adecuadas para su realización.	RG1.7
Actividades orientadas a la gestión de la seguridad de la información (ISO 27002)			
2.12	Evaluación de los riesgos de seguridad.	Promover evaluaciones de riesgo a la seguridad, que identifiquen, cuantifiquen y prioricen los riesgos en comparación con el criterio de aceptación del riesgo y los objetivos relevantes para le organización.	4.1
2.13	Promover y aprobar la política de seguridad de la información.	Aprobar la política de seguridad de la información a nivel organizacional y promover su aplicación, en concordancia con los objetivos del negocio y las leyes y regulaciones aplicables.	5.1
Actividades orientadas a administrar el ciclo de vida del servicio (ITIL V3)			
2.16	Considerar y promover la administración de riesgos en la entrega y soporte de servicios TI.	Solicitar que se considere dentro de la gestión del ciclo de vida del servicio la gestión de los riesgos relacionados con la soporte y la entrega de los servicios de TI.	SS9.5
Acrónimos utilizados: (1) COBIT 4.1: PO= Plan and Organize, ME= Monitor and Evaluate, DS= Deliver and Support, (2) RISK IT: RG= Risk Governance, (3) ITIL V.3: SS= Service Assets.			

En base a la aplicación del método de integración hemos identificado algunas lecciones aprendidas que podrían tenerse en cuenta para mejorar el método en futuras aplicaciones: (i) establecer un sistema de versiones que permita gestionar el control de cambios durante la adaptación de las descripciones de los EPSI integrados y (ii) detallar los criterios de integración adicionando nuevos estados alternos.

Actualmente, estamos trabajando en la definición de una *estrategia de armonización generalizada* (EAGA) conformada por las técnicas y método de integración definido. Este trabajo permitirá tanto a organizaciones como consultores, disponer de una estrategia genérica adaptable de acuerdo a sus necesidades de armonización y capaz de soportar desde la solución de las diferencias estructurales de múltiples marcos, hasta la comparación e integración de sus prácticas.

Como trabajo futuro, esperamos aplicar nuevamente el método de integración para el lanzamiento de la segunda versión de ITGSM. Con esta versión se espera definir los 22 procesos restantes que permitirán dar apoyo al cumplimiento de los principios 7, 8, 9 y 10 de BASEL II (que no se han tratado en la primera versión). Los resultados obtenidos se utilizarán para fortalecer los procesos definidos en ITGSM y confirmar la eficacia del método propuesto. Asimismo, esperamos poder aplicar el método a otros casos de estudio con el objetivo de validar su generalidad y adaptación de acuerdo a distintas necesidades de armonización.

Agradecimientos. Este trabajo ha sido financiado por los proyectos: ARMONÍAS (JCCM de España, PII2I09-0223-7948) y PEGASO/MAGO (MICINN y FEDER de España, TIN2009-13718-C02-01). Francisco J. Pino agradece a la Universidad del Cauca donde trabaja como profesor asociado.

Referencias

1. Oud, E.J.: The Value to IT of Using International Standards. Information Systems Control Journal. 3, (2005)
2. Pino, F.J., Baldassarre, M.T., Piattini, M., Visaggio, G., Caivano, D.: Mapping Software Acquisition Practices from ISO 12207 and CMMI: In: Maciaszek, L.A., González-Pérez, C., Jablonski, S. (eds.): Evaluation of Novel Approaches to Software Engineering, Vol. 69. Springer Berlin Heidelberg (2010) 234--247
3. Yoo, C., Yoon, J., Lee, B., Lee, C., Lee, J., Hyun, S., Wu, C.: A unified model for the implementation of both ISO 9001:2000 and CMMI by ISO-certified organizations. Journal of Systems and Software. 79, 954--961 (2006)
4. Pardo, C., Pino, F.J., García, F., Piattini, M., Baldassarre, M.T.: A Process for Driving the Harmonization of Models. In: The 11th International Conference on Product Focused Software Development and Process Improvement (PROFES 2010). Second Proceeding: Short Papers, Doctoral Symposium and Workshops, pp. 51--54. Markku Oivo, M.A.B., Matias Vierimaa, Limerick (2010)
5. Pardo, C., Pino, F., García, F., Piattini, M.: Homogenization of Models to Support multi-model processes in Improvement Environments. In: 4th International Conference on Software and Data Technologies ICSOFT'09, pp. 151--156. Sofía (2009)
6. Pino, F., Balssarre, M.T., Piattini, M., Visaggio, G.: Harmonizing maturity levels from CMMI-DEV and ISO/IEC 15504. Journal of Software Maintenance and Evolution: Research and Practice. 22, 279--296 (2010)

7. Pardo, C., Pino, F.J., García, F., Piattini, M.: Analizando el apoyo de marcos SPI a las características de calidad del producto ISO 25010. Revista Española de Innovación, Calidad e Ingeniería del Software (REICIS). (Edición especial XI Jornadas de Innovación y Calidad del Software, JICS). 5, 6--16 (2009)
8. Lemus, S.M., Pino, F.J., Piattini, M.: Towards a Model for Information Technology Governance applicable to the Banking Sector. In: V International Congress on IT Governance and Service Management (ITGSM 2010), pp. 1--6. Alcalá de Henares (2010)
9. ITGI: COBIT 4.1: Framework, control objectives, management guidelines and maturity models. IT Governance Institute, EEUU (2007)
10. BIS: International Convergence of Capital Measurement and Capital Standards - Basel II. Bank for International Settlements. (2004). Available on http://www.bis.org
11. ITGI: VAL IT Framework 2.0. IT Governance Institute, EEUU (2008)
12. ITIL: Information Technology Infrastructure Library V3. (2010). Available on http://www.itil-officialsite.com/
13. ITGI: Risk IT: Framework for Management of IT Related Business Risks. IT Governance Institute. (2009). Available on http://www.isaca.org/
14. ISO: Information technology -security techniques- code of practice for information security management - ISO 27002:2005. International Organization for Standardization. (2005). Available on http://www.iso.org/
15. Pardo, C., Pino, F.J., García, F., Piattini, M., Baldassarre, M.T.: Trends in Harmonization of Multiple Reference Models: Evaluation of Novel Approaches to Software Engineering, LNCS. Springer-Verlag, (Special edition best papers ENASE 2010, extended and updated paper) (2011) In press
16. Mutafelija, B., Stromber, H.: Architecting Standard Processes with SWEBOK and CMMI. Systems and Software Consortium. In: SEPG 2006 Conference, pp. 38. Nashville (2006)
17. Mutafelija, B., Stromber, H.: ISO 9001:2000 - CMMI V1.1 Mappings. Technical report, Software Engineering Institute (2003)
18. Biffl, S., Winkler, D., Höhn, R., Wetzel, H.: Software process improvement in Europe: potential of the new V-modell XT and research issues. Software Process: Improvement and Practice. 11, 229--238 (2006)
19. Jalote, P.: CMM in Practice: Processes for Executing Software Projects at Infosys, Vol. 1. Addison-Wesley Professional, Massachusetts (1999)
20. Yoo, C., Yoon, J., Lee, B., Lee, C., Lee, J., Hyun, S., Wu, C.: An integrated model of ISO 9001:2000 and CMMI for ISO registered organizations. In: Proceedings - Asia-Pacific Software Engineering Conference (APSEC), pp. 150--157. Busan (2004)
21. Lin, L.-C., Li, T.-S., Kiang, J.P.: A continual improvement framework with integration of CMMI and six-sigma model for auto industry. Quality and Reliability Engineering International. 25, 551--569 (2009)
22. CITIL: CMMI+ITIL. (2010). Available on http://www.wibas.de/publikationen/referenzmodelle/was_ist_cmmi/index_de.html
23. Ibrahim, L., Pyster, A.: A Single Model for Process Improvement. IT Professional. 6, 43–49 (2004)
24. Pardo, C., Pino, F.J., García, F., Piattini, M., Baldassarre, M.T., Lemus, S.: Homogenization, Comparison and Integration: A Harmonizing Strategy for the Unification of Multiple-Models in the Banking Sector: In: Visaggio, G., Caivano, D., Oivo, M., Baldassarre, M.T. (eds.): The 12th International Conference on Product Focused Software Development and Process Improvement (PROFES 2011). Vol. 6759. Springer, Heidelberg, 59--72. Bari (2011)