Estudio Aplicación del Modelo de Madurez Capacidad de Ingeniería en Seguridad de los Sistemas (SSE-CMM) por áreas de Proyecto y Organización

José Antonio Calvo-Manzano, Tomás San Feliu, Ariel Serrano
Departamento de Lenguajes y Sistemas Informáticos e Ingeniería del Software
Facultad de Informática, Universidad Politécnica de Madrid

En este artículo se describen los resultados de un estudio de investigación sobre la aplicación del modelo SSE-CMM, realizado a los estudiantes de la II Edición del Master en Auditoría y Seguridad Informática organizado por la ALI y la Facultad de Informática de la UPM. Este trabajo se centró en determinar qué prácticas del modelo son más utilizadas y qué prácticas requieren de una mayor atención o son poco conocidas por parte del grupo de profesionales interesados en la seguridad y que cursaron el master durante el año 2003.

1. Introducción

La creciente expansión de las redes de datos, la interconexión de los sistemas y las aplicaciones, y el uso cada vez más extendido de Internet como medio de intercambio de información ha desencadenado el papel central que tiene la seguridad en los sistemas de información. Cada vez más se requiere de productos, servicios y sistemas para mantener y proteger la información, y es un hecho que cada vez más clientes y proveedores están interesados en mejorar sus esquemas de seguridad. El enfoque de sistema seguro ha pasado de ser exclusivo de organismos gubernamentales, a virtualmente ser indispensable para todas las aplicaciones y sistemas basados en ordenador. Es en este marco donde surge la Ingeniería de la Seguridad, que al ser una disciplina en desarrollo aún no existe consenso por parte de la comunidad informática que la defina como tal. Sin embargo es posible establecer los objetivos primordiales que ésta persigue [1] (Tabla 1).

Aunque el campo de Ingeniería de la Seguridad tiene varios principios bien aceptados, hasta hace poco carecía de un marco global para su evaluación. Es aquí donde el *Systems Security Engineering Capability Maturity Model* (SSE-CMM) [1] surge como una herramienta para evaluar y mejorar la capacidad de una organización a la hora de implementar los principios y objetivos de la Ingeniería de la Seguridad.

Según establece el propio SSE-CMM, su aplicación se centra en cuatro grupos primarios: 1) En los profesionales interesados o responsables de la Ingeniería de la Seguridad den-

- Obtener una comprensión de los riesgos asociados a la seguridad.
- Establecer un sistema equilibrado de necesidades de seguridad de acuerdo con los riesgos identificados.
- Transformar las necesidades de seguridad en directrices que estén integradas en las actividades de un proyecto, en las descripciones de una configuración o en la operación del sistema.
- Establecer confianza en la corrección y eficacia de los mecanismos de seguridad.
- Determinar niveles aceptables en el impacto de la operación del sistema debido a las vulnerabilidades de seguridad (riesgos aceptables).
- Integrar los esfuerzos de todas las disciplinas y especialidades de la ingeniería para una comprensión combinada de seguridad.

Tabla 1. Objetivos de la Ingeniería de la Seguridad.

tro de su organización. 2) En los desarrolladores del proceso. 3) En los encargados de evaluar los procesos de Ingeniería de la Seguridad dentro de una organización. 4) En los gerentes del área de Ingeniería de la Seguridad.

Con el propósito de evaluar el estado actual de Ingeniería de la Seguridad y tomando como referencia el SSE-CMM, este trabajo de investigación realizó un estudio a un grupo de estudiantes de la II Edición del Master en Auditoría y Seguridad Informática organizado en forma conjunta por la ALI (Asociación de Doctores Licenciados e Ingenieros en Informática) y la Facultad de Informática de la Universidad Politécnica de Madrid. Si bien es cierto que esta investigación cubre en parte los cuatro grupos primarios a los cuales va dirigido el SSE-CMM, se enfoca sobretodo al grupo uno, "Profesionales interesados o responsables de Ingeniería de la Seguridad". Los participantes del master provienen de diversas organizaciones públicas y privadas de España, pero a su vez comparten el interés común en mejorar los mecanismos de seguridad de los sistemas dentro de sus propias empresas.

Usando el SSE-CMM como modelo de referencia, los objetivos de esta investigación son: primero, determinar aquellas prácticas que son utilizadas por la mayoría de los participantes y que están bien documentadas. Segundo, determinar qué prácticas requieren de una mayor atención o son poco conocidas por los participantes del estudio. Y por último, dar las conclusiones generales y las lecciones aprendidas de la aplicación del modelo por parte de los profesionales de Ingeniería de la Seguridad que participaron en el master.

1.1 ¿Qué es el SSE-CMM?

El *Modelo de Madurez de la Capacidad de Ingeniería de la Seguridad de Sistemas* (SSE-CMM) es una herramienta para evaluar y ayudar a mejorar las prácticas y métodos de seguridad de una organización. El modelo establece un marco de referencia para medir y mejorar las prácticas relativas a la seguridad dentro del contexto de la Ingeniería del Software [2]. El SSE-CMM fue diseñado tomando como base la estructura y las prácticas del SE-CMM [3] e interpretando aquellas prácticas que cubren las necesidades de la disciplina en especialidad de Ingeniería de la Seguridad.

El SSE-CMM puede utilizarse como una herramienta para guiar a las organizaciones en la evaluación de sus prácticas de Ingeniería de la Seguridad, pero también se puede utilizar como un mecanismo estándar para que los clientes evalúen la capacidad en la Ingeniería de la Seguridad de un proveedor. El modelo es una métrica estándar para las prácticas de ingeniería de la seguridad y cubre:

- El ciclo de vida completo, incluyendo las actividades de desarrollo, operación y mantenimiento.
- Todas las actividades de la organización, incluyendo las actividades de gestión, de organización y de ingeniería.
- Las interacciones con otras disciplinas como sistemas, software, hardware, factores humanos, pruebas, gestión de sistemas, operación y mantenimiento.
- Las interacciones con otras organizaciones, incluyendo adquisición, gestión de sistemas, certificación, acreditación y evaluación.

1.2 Breve Historia del SSE-CMM

La iniciativa SSE-CMM comenzó en abril de 1993 como una necesidad de contar con un modelo de capacidad para Ingeniería de la Seguridad, en sus inicios fue patrocinado por la Agencia Nacional de Seguridad de los EE.UU. *(NSA-National Security Agency)*, y en la actualidad también lo patrocinan la Oficina del Secretario de Defensa de los EE.UU. y el Centro de Investigación de la Seguridad para las Telecomunicaciones de Canadá *(CST-Centre de la sécurité des télécommunications)*. La primera versión del modelo se publicó en octubre de 1996 y el método de evaluación en abril de 1997, pero desde 1999 el organismo encargado del desarrollo y promoción del modelo es la Asociación Internacional de la Ingeniería de la Seguridad de los Sistemas *(ISSEA-International Systems Security Engineering Association)*, quién publicó la última versión (3.0) del modelo en junio del 2003. El SSE-CMM se ha desarrollado gracias a la colaboración de grupos de compañías con antecedentes de éxito en la construcción de sistemas seguros.

2. Descripción de la arquitectura del SSE-CMM

El SSE-CMM divide la Ingeniería de la Seguridad en tres áreas básicas: Riesgo, Ingeniería y Aseguramiento. Aunque estas áreas son dependientes unas de otras, es posible considerarlas de forma separada. En el nivel más simple, el proceso de Riesgo identifica y da prioridad a los peligros inherentes al producto o sistema desarrollado. El proceso de Ingeniería trabaja con las otras disciplinas de ingeniería para determinar e implementar soluciones a los problemas presentados por los peligros. Finalmente, el proceso de Aseguramiento establece la confianza en las soluciones de seguridad y transmite dicha confianza a los clientes [4].

La arquitectura del SSE-CMM está diseñada para permitir la determinación de la madurez del proceso de Ingeniería de la Seguridad de la organización. El objetivo de la arquitectura es separar claramente las características básicas del proceso de Ingeniería de la Seguridad de las características de gestión e institucionalización. Para asegurar esta separación, el modelo tiene dos dimensiones: Dominio y Capacidad. La dimensión del dominio consiste simplemente en todas las prácticas que de forma colectiva definen la Ingeniería de la Seguridad, estas prácticas se denominan Prácticas Base y están clasificadas por áreas de proceso. La dimen-

Áreas de Proceso de Ingeniería de la Seguridad	Áreas de Proceso del Proyecto y la Organización
PA01 – Gestionar Controles de Seguridad	PA12 – Asegurar la calidad
PA02 – Determinar el Impacto de la Seguridad	PA13 – Gestión de Configuración
PA03 – Determinar el Riesgo de la Seguridad	PA14 – Gestionar el Riesgo del Proyecto
PA04 – Determinar la Amenaza	PA15 – Supervisar y Controlar el Esfuerzo Técnico
PA05 – Determinar la Vulnerabilidad	PA16 – Planificar el Esfuerzo Técnico
PA06 – Construir Argumentos de Aseguramiento	PA17 – Definir el proceso de Ingeniería de Sistemas
PA07 – Seguridad Coordinada	PA18 – Mejorar los procesos de Ingeniería de Sistemas
PA08 – Supervisar la postura de Seguridad	PA19 – Gestionar la Evolución de la Línea de Producto
PA09 – Proporcionar Entradas de Seguridad	PA20 – Gestionar el Entorno de Soporte de Ing. Sistemas
PA10 – Especificar las Necesidades de Seguridad	PA21 – Proporcionar Habilidades y Conocimientos
PA11 – Verificar y Validar la Seguridad	PA22 – Coordinar con los Proveedores

Tabla 2. Áreas de Proceso de la Dimensión de Dominio.

sión de la capacidad representa las prácticas que indican la capacidad de gestión y de institucionalización del proceso, las cuales se denominan Prácticas Genéricas, ya que se aplican en todos los dominios o áreas de proceso. Ambas prácticas juntas, base y genéricas, proporcionan una forma de verificar la capacidad de una organización para realizar una actividad en particular.

2.1 Prácticas Base

Como ya se mencionó, el SSE-CMM consta de dos dimensiones y, una de ellas, la *Dimensión del Dominio*, está organizada en dos grupos divididos por su función: Áreas de Proceso de Ingeniería de la Seguridad (Tabla 2) y Áreas de Proceso del Proyecto y la Organización. Estas últimas se enfocan en la mejora del proyecto y en la capacidad que tiene la organización (Tabla 2). Las 22 áreas de proceso en las que se clasifica la dimensión del dominio contienen 129 prácticas base. De éstas, 61 prácticas están organizadas en 11 áreas de proceso que cubren todas las áreas de Ingeniería de la Seguridad. Las 68 prácticas base restantes organizadas en 11 áreas de proceso cubren las áreas del Proyecto y la Organización.

Cabe señalar que este trabajo de investigación no abarcó las áreas de proceso de Ingeniería de la Seguridad, debido a que se obtuvo poca información a causa de la dificultad por parte de los encuestados para contestar a estas

NIVEL 1	Realizado Informalmente	CC1.1	Las Prácticas Base son Realizadas
NIVEL 2	Planificado y seguido	CC2.1	Planificación de la Ejecución
		CC2.2	Ejecución Disciplinada
		CC2.3	Verificar la Ejecución
		CC2.4	Dar Seguimiento a la Ejecución
NIVEL 3	Bien Definido	CC3.1	Definición de un Proceso Estándar
		CC3.2	Ejecutar el Proceso Definido
		CC3.3	Coordinar las Prácticas de Seguridad
NIVEL 4	Controlado Cuantitativamente	CC4.1	Establecimiento de Objetivos Medibles de Calidad
		CC4.2	Gestionar de forma Objetiva la Ejecución
NIVEL 5	Mejorando Continuamente	CC5.1	Mejorar la Capacidad de la Organización
		CC5.2	Mejorar la Eficacia del Proceso

Tabla 3. Niveles de Capacidad y Características Comunes.

Característica Común 2.1 – Planificación de la Ejecución
GP 2.1.1 – Asignar recursos
GP 2.1.2 – Asignar responsabilidades
GP 2.1.3 – Documentar el proceso
GP 2.1.4 – Proporcionar herramientas
GP 2.1.5 – Asegurar el entrenamiento
GP 2.1.6 – Planificar el proceso
Característica Común 2.2 – Ejecución Disciplinada
GP 2.2.1 – Utilizar planes, estándares y procedimientos
GP 2.2.2 – Gestión de configuración
Característica Común 2.3 – Verificar la Ejecución
GP 2.3.1 – Verificar el cumplimiento del proceso
GP 2.3.2 – Auditar los productos de trabajo
Característica Común 2.4 – Dar Seguimiento a la Ejecución
GP 2.4.1 – Dar seguimiento, utilizando métricas
GP 2.4.2 – Tomar acciones correctivas

Tabla 4. Prácticas Genéricas del Nivel 2 de Capacidad.

preguntas. Esta situación la encontró también Hefner [2, 5] en sus investigaciones sobre la validación del modelo SSE-CMM realizadas a un grupo de empresas durante el año 1996, en donde los profesionales evaluados tuvieron algunas dificultades con la terminología y la interpretación de las prácticas de Ingeniería de la Seguridad para su entorno de trabajo.

2.2 Prácticas Genéricas

Las prácticas genéricas pertenecen a la *Dimensión de la Capacidad* y son utilizadas en la valoración del proceso para determinar su nivel de capacidad. Las prácticas genéricas se agrupan de acuerdo a sus características comunes y los distintos Niveles de Capacidad (Tabla 3).

El SSE-CMM tiene 29 prácticas genéricas agrupadas en 12 características comunes que determinan la institucionalización del proceso en cuanto al nivel de capacidad alcanzado. El presente trabajo de investigación sólo abarca la única práctica genérica del Nivel 1 de Capacidad y las 12 prácticas genéricas correspondientes al Nivel 2 de Capacidad (Tabla 4).

Contestando a todas las cuestiones que surgen de la combinación de todas las prácticas base con todas las prácticas genéricas es posible tener una visión de la capacidad de Ingeniería de la Seguridad de una determinada organización.

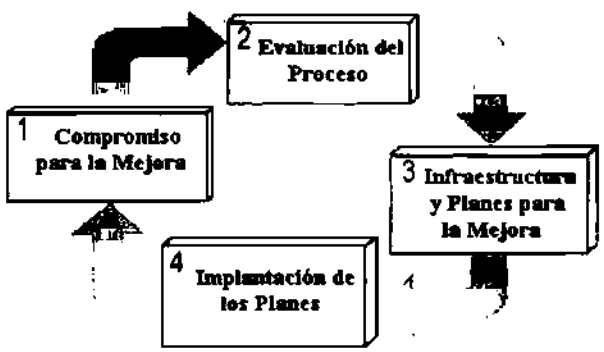

Figura 1. Modelo Genérico de ISPI para la Mejora del Proceso de Software.

3. Análisis de los Datos

3.1 Utilizando el SSE-CMM para evaluar la mejora del proceso

El SSE-CMM puede utilizarse como una herramienta para mejorar el proceso de Ingeniería de la Seguridad de una organización y recomienda a todo el que quiera comenzar un esfuerzo serio de mejora del proceso utilizar algún enfoque como el IDEAL [6] o el desarrollado por el ISPI [7] (Figura 1).

3.2 Método de Evaluación del SSE-CMM

El método desarrollado por la ISSED para evaluar la capacidad del proceso de Ingeniería de la Seguridad en una organización, "*The SSE-CMM Appraisal Method (SSAM)*" [8], se divide en cuatro fases: Planificación, Preparación, Ejecución e Informe de Resultados. La fase de preparación incluye las actividades de capacitación sobre el modelo y el método de evaluación, así como la recogida de datos mediante el uso de instrumentos como cuestionarios y/o entrevistas. A pesar de sus ventajas, este método utiliza para la fase de preparación un cuestionario muy simple que no permite libertad en los tipos de respuesta. Sin embargo el propio SSE-CMM indica que no es necesario utilizar SSAM en particular para la evaluación de la capacidad del proceso.

Por lo anterior y para poder determinar con mayor precisión el nivel de cobertura que tiene el SSE-CMM entre los profesionales en el Master en Auditoría y Seguridad Informática y, en algunos casos, responsables de la seguridad de sus organizaciones, decidimos utilizar como método de evaluación el desarrollado por el grupo de investigación SOMEPRO constituido por profesores de la Universidad Politécnica de Madrid, la Universidad Carlos III de Madrid y la Universidad Nacional de Educación a Distancia [9] [10].

Antes de iniciar el proceso de evaluación se proporcionó entrenamiento a los alumnos del Master sobre el método de evaluación y el SSE-CMM. Este conocimiento es esencial para que los encuestados entiendan la terminología y los conceptos básicos del modelo, así como la forma de rellenar el cuestionario.

	% de ocurrencia			
	100 – 75	75 - 25	25 - >0	0
Documentada	Siempre	Usualmente	Rara Vez	Nunca
No Documentada	Usualmente	Algunas veces	Rara Vez	Nunca

Tabla 5. Tipos de respuestas a cada pregunta del cuestionario.

A la vez que se proporcionaba el entrenamiento, cada alumno iba rellenando el cuestionario por área de proceso tras acabar su correspondiente formación. El cuestionario se ha desarrollado sobre la base de 68 preguntas que corresponden una a una con las prácticas base de las Áreas de Proceso del Proyecto y la Organización (PA12 a la PA22) (Tabla 2). También para cada área de proceso se aplicaron 29 preguntas que correspondientes una a una con todas las prácticas genéricas de los Niveles 1 al 5 de Madurez. Sin embargo para el análisis de los datos sólo se incluyó la práctica genérica del Nivel 1 y las 12 prácticas genéricas del Nivel 2 de Capacidad (Tabla 4).

El cuestionario se basó en respuestas cerradas con el fin de facilitar su análisis e interpretación a la hora de determinar la cobertura del proceso para cada práctica y en general para el área de proceso. Para cada pregunta hay cinco posibles respuestas: Siempre, Usualmente, Algunas Veces, Rara Vez, Nunca (Tabla 5). Éstas determinan el nivel de cobertura para cada práctica.

Para cada pregunta que corresponde con una práctica (base o genérica) se calcula la media ponderada de las respuestas válidas de todos los encuestados y se establece que aquellas prácticas cuya media sea menor al 75% no están suficientemente implantadas en la organización y se considerarán como un **Aspecto a Mejorar**. Sólo aquellas prácticas cuya media sea mayor o igual al 75% se considerarán como **Puntos Fuertes** siempre y cuando la Desviación Típica de las respuestas sea pequeña (menor o igual a 1). En caso contrario quiere decir que existen fuertes discrepancias y, por lo tanto, se deberá explorar en mayor profundidad a través de entrevistas.

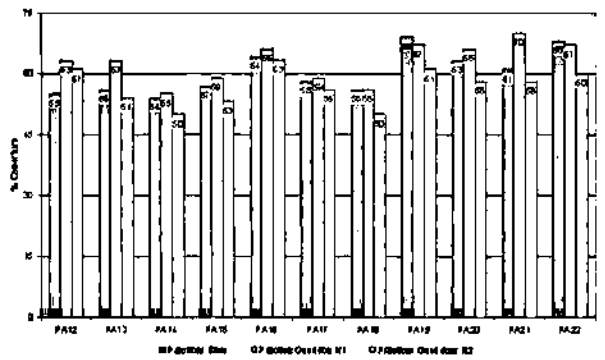

Figura 2. Nivel de Cobertura de las Prácticas Base y las Práctica Genéricas de Nivel 1 y 2.

3.3 Cobertura de las Áreas de Proceso del Proyecto y la Organización

Como primer resultado de la encuesta encontramos que ningún Área de Proceso (PA) del Proyecto y la Organización alcanzan el mínimo del 75% de cobertura para ser consideradas como institucionalizadas. Sin embargo dos PA's tienen una cobertura de casi el 70%, PA19 Gestionar la Evolución de la Línea de Producto, y PA22 Coordinar con los Proveedores (Figura 2).

3.3.1 Cobertura de las Áreas de Proceso con el Nivel 1 de Capacidad

Otro punto a considerar dentro del análisis es comparar en la Figura 2 el valor de cobertura de las dos primeras barras del gráfico para cada PA, las primeras corresponden a la cobertura de las prácticas base y las segundas corresponden a la cobertura de la única práctica genérica "*CC–1.1 Realizar las Prácticas Base*" del Nivel 1 de Capacidad. El porcentaje de cobertura de la práctica base debe ser similar con el respectivo porcentaje de cobertura del N1 de capacidad.

En todas las prácticas encontramos una diferencia marginal entre 0 y 3 puntos porcentuales salvo en PA12, PA13 y PA21 con diferencias de 8, 7 y 9 puntos porcentuales respectivamente. Estas diferencias obedecen a discrepancias entre las respuestas de las prácticas genéricas y la respectiva práctica base. Para estos casos será necesario profundizar con entrevistas adicionales para consolidar la información obtenida.

3.3.2 Cobertura de las Áreas de Proceso con el Nivel 2 de Capacidad

En la misma Figura 2 el valor de cobertura de las terceras barras del gráfico para cada PA, corresponden a la cobertura global de todas las prácticas genéricas del Nivel 2 de Capacidad. Encontramos que ningún área de proceso alcanza el valor requerido del 75% para que sea considerada como institucionalizada, sin embargo para todas las PA's la cobertura supera el 50%. Esto hace suponer que los encuestados tienen conocimiento y realizan algunas prácticas de institucionalización pero solo algunas veces documentan este esfuerzo.

3.3.3 Cobertura de las Prácticas Base por cada Área de Proceso

Cada área de proceso tiene un número variable de prácticas base. La Figura 3 muestra el total de prácticas base por cada PA. Por otro lado, el análisis de este gráfico muestra que la mayor parte de las prácticas se encuentra entre un 50 y 75% de cobertura, cuatro prácticas son mayores o iguales al 75% y solo una práctica está por debajo del 50% de cobertura.

Para considerar a las cuatro prácticas que tienen una cobertura del proceso mayor o igual al 75% como Puntos Fuertes es necesario revisar si el valor de la media obtenida tiene una desviación típica menor o igual a 1. Las cuatro prácticas son:

- En PA16, la práctica "*BP.16.04–Determinar el proceso técnico a utilizar en el proyecto*" obtuvo una media de cobertura del 76% con una desviación típica de 0,7
- En PA19, la práctica "*BP.19.01–Definir los tipos de productos a ofrecer*" obtuvo una media de cobertura del 79% con una desviación típica de 0,8.
- En PA22, la práctica "*BP.22.01–Identificar los componentes o servicios del sistema necesitados que deben ser proporcionados por otras organizaciones*" obtuvo una media de cobertura del 75% con una desviación típica de 0,9.
- En PA22 la práctica "*BP.22.02–Identificar los suministradores que han mostrado experiencia en las áreas identificadas*" se obtuvo una media de cobertura del 76% con una desviación típica de 0,8.

Por otro lado la práctica que se considera como más débil es en PA12 "*BP.12.03–Medir la calidad el proceso de ingeniería de sistemas utilizado por el proyecto*" con un valor de cobertura de tan solo el 47%. Todas las demás prácticas están entre un 50% y un 75% de cobertura.

3.3.4 Cobertura de las Prácticas Genéricas del Nivel 2 de Capacidad

La Figura 4 muestra el comportamiento que tienen las respuestas de las prácticas genéricas contra cada PA. La práctica genérica que alcanza el máximo nivel de cobertura es "*2.1.1–Asignar recursos*" con hasta 80% de cobertura para PA16. La práctica "*2.1.2–Asignar responsabilidades*" obtuvo el mejor valor medio.

La misma Figura 4 muestra que la práctica genérica que tiene menor cobertura es la "*2.1.5–Asegurar el entrenamiento*" en donde para la mayor parte de las PA su valor de cobertura estuvo por debajo del 55%.

Por otro lado los valores más altos de cobertura fueron para el área de proceso "*PA16–Planificar el esfuerzo técnico*" donde todas las prácticas genéricas superaron el 50% de cobertura.

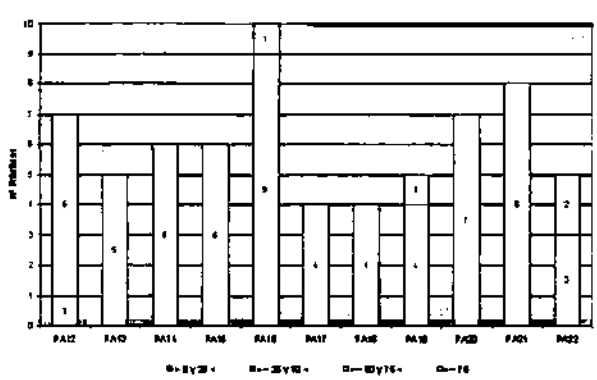

Figura 3. Nivel de Cobertura de las Prácticas Base.
Por cada Área de Proceso del Proyecto y la Organización.

4. Conclusiones

El análisis de resultados de la investigación realizada al grupo de profesionales participantes en el Master en Auditoría y Seguridad Informática indica que para las 68 prácticas base de las áreas de proceso del Proyecto y de la Organización el nivel de cobertura fue en promedio del 60%, es decir, las actividades de Ingeniería de la Seguridad relacionadas con la mejora del proyecto se llevan a cabo en más de la mitad de las veces aunque probablemente en su mayor parte no están documentadas.

Las tres Áreas de Proceso (PA) con una mayor cobertura, cercana al 70% son: "*PA16–Planificar el Esfuerzo Técnico*", "*PA19–Gestionar la Evolución de la Línea de Producto*" y "PA22–Coordinar con los Proveedores".

En el análisis en detalle de las prácticas que componen estas PA, se encontró que la práctica base con mayor cobertura, *BP.19.01*, con casi un 80% de cobertura, pertenece al área de proceso *PA19*. El objetivo de esta práctica es definir las líneas de producto que soporten la visión estratégica de la organización. Algunos ejemplos de líneas de productos de la seguridad son: prácticas de gestión de configuración, selección del personal para el desarrollo de código seguro y la obtención de una certificación de productos seguros. Le siguen las prácticas *BP.22.01* y *BP.22.02*, con un 75% y 76% de cobertura respectivamente, que pertenecen al área de proceso *PA22* y su objetivo es contar con mecanismos para seleccionar y contratar a los proveedores de seguridad más adecuados. Por último, la práctica base *BP.16.04*, con un 76% de cobertura, pertenece al área de proceso *PA16* y su objetivo es seleccionar y establecer un modelo de Ciclo de Vida acorde con las características del proyecto y de la organización.

De estos resultados se obtienen tres conclusiones con respecto a las prácticas más utilizadas por el grupo de profesionales de la Ingeniería de la Seguridad y son que:

1. Se tienen bien definidos los procesos internos para la gestión de la línea de producto.

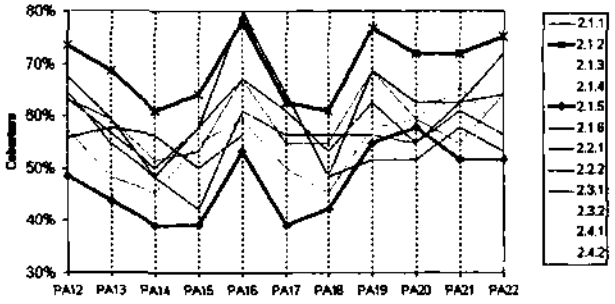

Figura 4. Prácticas Genéricas para cada Área de Proceso.

2. Se tienen procesos definidos y documentados para la supervisión los proveedores de Ingeniería de la Seguridad.

3. Se conocen y se tienen bien definidos el proceso de selección del ciclo de vida a utilizar en los proyectos.

Por último, el punto con menos cobertura aunque sin embargo casi alcanza el 50% de cobertura, *BP.12.03*, se refiere a la práctica para medir la calidad del proceso de la Ingeniería de la Seguridad, lo que indica una posible deficiencia en cuestiones de calidad con respecto a todas las demás prácticas. El resultado de esta última práctica confirma el hecho de que la medición de calidad es *una de las últimas prácticas que* se implementan.

Con respecto a las prácticas genéricas del Nivel 2 de Capacidad, para poder considerar como institucionalizada a un área de proceso es necesario que todas sus respectivas prácticas base superen el 75% de cobertura. En el estudio ningún área de proceso cumple estas condiciones de institucionalización.

Todos los resultados obtenidos en el estudio, reflejan un grado intermedio en la aplicación de las áreas de proceso del Proyecto y la Organización en las actividades y procesos de la Ingeniería de la Seguridad.

También se encontraron tres casos donde las prácticas se ejecutan y documentan en la mayor parte de los proyectos pero sin llegar al 100%.

Por último, es importante recalcar que aunque existe comprensión e interés por la Ingeniería de la Seguridad, por parte del grupo sujeto del estudio, la mayor parte de las prácticas requiere de un esfuerzo importante sobre todo en la documentación de los procesos y en la institucionalización de los mismos en toda organización de tal forma que se puedan considerar como definidos y repetibles.

Referencias

[1] Project Team Members, "Systems Security Engineering Capability Maturity Model® SSE-CMM®, Version 3.0", The International Systems Security Engineering Association (ISSEA), June 15, 2003, http://www.sse-cmm.org/model/ssecmmv2final.pdf

[2] R. Hefner, "*Lessons Learned with the Systems Security Engineering Capability Maturity Model*", *presented at 19th International Conference* on Software Engineering, Boston, Massachusetts, USA, 1997, pp 566 - 567.

[3] Bate, Roger, et al., "A Systems Engineering Capability Maturity Model®, Version 1.1", CMU/SEI-95-MM-003, Software Engineering Institute, Carnegie Mellon University, November 1995, http://www.sei.cmu.edu/pub/documents/95.reports/pdf/mm003.95.pdf

[4] J. A. Calvo-Manzano, T. San-Feliu, and J. M. De-las-Heras, "Ingeniería de la Seguridad: Modelo de Madurez de la Capacidad de Ingeniería de la Seguridad de los Sistemas SSE-CMM", Base Informática, Junio 2002, pp. 26 - 29.

[5] R. Hefner, "A process standard for system security engineering: development experiences and pilot results", presented at Third IEEE International Software Engineering Standards Symposium and Forum, (ISESS '97), 'Emerging International Standards', Walnut Creek, CA USA, 1997, pp 217 - 221.

[6] McFeeley, Robert, "IDEAL: A User's Guide for Software Process Improvement", CMU/SEI-96-HB-001, http://www.sei.cmu.edu/pub/documents/96.reports/pdf/hb001.96.pdf

[7] J. A. Calvo-Manzano, G. Cuevas, T. San-Feliu, A. De-Amescua, L. García, and M. Pérez, "Experiences in the Application of Software Process Improvement in SMES", Software Quality Journal, vol. 10, 2002, pp. 261 - 273.

[8] Project Team Members, "The SSE-CMM Appraisal Method (SSAM), Version 2.0", The International Systems Security Engineering Association (ISSEA), April 16, 1999, http://www.sse-cmm.org/org/SSAM.pdf

[9] J. A. Calvo-Manzano, J. Cervera, and T. San-Feliu, "Software process improvement: MESOPYME model", Journal of Computing and Information Technology, vol. 43, 1997, pp. 159 - 165.

[10] G. Cuevas, A. de Amescua, J.A. Cerrada, T. San Feliu, J.A. Calvo-Manzano, M. Arcilla, M. Cordero, Gestión del Proceso Software, Madrid: Centro de Estudios Ramón Areces, 2002, pp. 415 - 429.