La Ingeniería de Seguridad como ayuda al desarrollo de los SGSI

Una de las mayores dificultades a las que se enfrentan las organizaciones que desean desarrollar un proyecto de SGSI (Sistema de Gestión de Seguridad de la Información) bajo la norma ISO/IEC 27001 es el análisis, diseño e implantación del Proceso Global de Seguridad teniendo en cuenta las necesidades de seguridad definidas en sus propias estrategias de negocio. Los procesos de seguridad dentro del Proceso Global de Seguridad son tratados de forma detallada por la norma ISO/IEC 21827:2002 Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM). En este artículo se muestra cómo la aplicación del modelo SSE-CMM en los proyectos de SGSI puede convertirse en una herramienta de gran ayuda para el éxito del proyecto. Para ello se presenta un modelo de referencia que facilita la utilización del citado modelo.


José Antonio Calvo-Manzano / Ana de las Heras

La Ingeniería de la Seguridad como ayuda al desarrollo del Proyecto de SGSI

Es conocido por cualquier organización que se plantea llevar a cabo un proyecto de SGSI y desea además que una vez implantado pueda ser certificado, que el estándar mundial más utilizado es el propuesto por la norma ISO/IEC 27001, cuyos controles se basan en la última actualización de ISO/IEC 17799:2005. Sobre cómo afrontar y planificar el proyecto de SGSI bajo ISO/IEC 27001 se dispone de abundante documentación, más aún si se tiene en cuenta que esta norma puede considerarse como la última revisión de la norma BS 7799:2002 Parte 2 de la que ya había en el mundo alrededor de 2.000 SGSI certificados.

Pero en un proyecto de SGSI nunca se debe olvidar que hay que enfrentarse, en primer término, al análisis, diseño e implantación del "Proceso de Seguridad" para la organización en la que se ha de implantar, teniendo en cuenta las necesidades de seguridad definidas en su estrategia de negocio. Y es evidente que el éxito de cualquier proyecto de SGSI está íntimamente relacionado con el éxito en el diseño e implantación del Proceso Global de Seguridad. Siendo así, sería adecuado que se tuviera en cuenta, además de las normas ISO/IEC 27001 e ISO/IEC 17799, otras normas específicas disponibles para este propósito como es SSE-CMM (norma ISO/IEC 21827:2002 Information Technology – Systems Security Engineering – Capability Maturity Model). SSE-CMM es una de las normas más utilizadas internacionalmente en relación con la definición e implantación de los procesos de seguridad ya que define con profundidad y precisión los procesos que deben tenerse en cuenta en cualquier organización que desea implantar un "Proceso Global de Seguridad".

Puesto que un proyecto de SGSI también es un proyecto de Ingeniería de Seguridad, SSE-CMM es de gran ayuda para el éxito del mismo. Esta ayuda será todavía más importante cuanto mayor sean las exigencias de seguridad; por ejemplo: alcanzar niveles concretos de capacidad, cumplimiento de leyes y normas de seguridad específicas, certificaciones contra otras normas, etc.

¿Qué es la Ingeniería de la Seguridad en los Sistemas T.I.?

En INFOSEC-99 se define como: "*El esfuerzo para alcanzar y mantener la seguridad óptima y supervivencia de un sistema en todo su ciclo de vida*".

• ***Seguridad:*** *la condición resultante de establecer y mantener medidas de protección que aseguran un estado de inviolabilidad ante actos o influencias hostiles.*

• ***Supervivencia:*** *la propiedad de un sistema, subsistema, equipo, proceso o procedimiento que aporta un grado definido de aseguramiento de la entidad, que deberá continuar funcionando durante y después de una perturbación natural o realizada por el hombre. Para una aplicación dada, la supervivencia deberá ser caracterizada especificando: el rango de condiciones bajo las que la entidad sobrevivirá, el nivel mínimo aceptable de funcionalidad después de la perturbación y el tiempo máximo aceptable en el que la entidad puede no funcionar o dejar de dar el servicio.*

• ***Sistema:***

– Un conjunto organizado de recursos y procedimientos combinados y regulados por la interacción o interdependencia para llevar a cabo un conjunto de funciones específicas.

– Un conjunto de personas, equipos y métodos organizados para cumplir un conjunto específico de funciones.

En relación con la seguridad, SSE-CMM va más lejos y desarrolla un Modelo de Madurez de la Capacidad de Ingeniería de la Seguridad de los Sistemas, en el que se describen las características esenciales del proceso global de ingeniería de la seguridad de una organización. Este proceso debe existir para asegurar una buena ingeniería de la seguridad. SSE-CMM no prescribe un proceso o secuencia particular, pero indica las prácticas observadas en la industria. 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.

• La organización completa, incluyendo las actividades de gestión, organizativas e ingeniería.

• Interacciones con otras disciplinas como sistemas, software, hardware, factores humanos e ingeniería de pruebas; gestión de sistemas, operación y mantenimiento.

• Interacciones con otras organizaciones, incluyendo adquisición, gestión de sistemas, certificación, acreditación y evaluación.

Alcance del SSE-CMM

Trata las actividades de ingeniería de la seguridad que cubren el ciclo vida completo del sistema seguro, incluyendo la definición del concepto, el análisis de los requisitos, el diseño y el desarrollo. También se aplica a todos los tipos y tamaños de organizaciones de ingeniería de la seguridad, como por ejemplo comerciales, gubernamentales y académicas.

Promociona la integración con otras disciplinas, tomando la seguridad como incluida en todas las disciplinas de ingeniería (sistemas, software, hardware y factores humanos), y definiendo los componentes del modelo para tratar tales problemas.

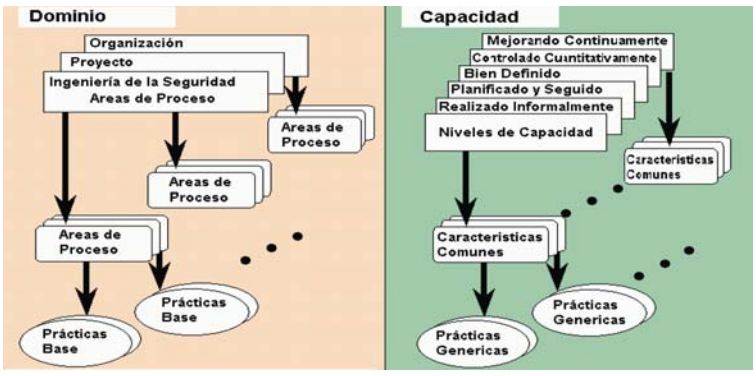

Figura 1. Arquitectura del modelo SSE-CMM, norma ISO/IEC 21827:2002.

Utilización del SSE-CMM

El modelo SSE-CMM y el método para aplicar el modelo suelen utilizarse como:

• Herramienta usada por las organizaciones para evaluar sus prácticas de ingeniería de la seguridad y definir las mejoras a ellas.

• Base para las organizaciones que evalúan la ingeniería de la seguridad (por ejemplo, certificadores de sistemas o evaluadores de productos), con objeto de establecer confianzas organizativas basadas en la capacidad.

• Mecanismo estándar para que los clientes evalúen en un proveedor su capacidad de ingeniería de la seguridad.

Las evaluaciones pueden utilizarse en la aplicación del modelo para la automejora y/o en la selección de los suministradores.

SSE-CMM (norma ISO/IEC 21827) es en la actualidad poco conocida en nuestro país, aunque es muy utilizada en países como EE.UU., Canadá, Australia, Alemania, Austria, Japón, India, etc. para diseñar e implantar los procesos de seguridad, medir su capacidad y establecer planes de mejora en las áreas de proceso de interés para la organización.

SSE-CMM tiene dos dimensiones, "dominio" y "capacidad". En la **Figura 1** se representa su arquitectura.

La dimensión del dominio: comprende las prácticas que de forma colectiva definen la ingeniería de la seguridad. A estas prácticas se las denomina "prácticas base". SSE-CMM contiene alrededor de 60 prácticas base de seguridad, organizadas en 11 áreas de proceso que cubren todas las áreas principales de la ingeniería de la seguridad. Estas prácticas base se establecieron a partir de un amplio rango de materiales, prácticas y experiencias existentes y representan la mejor practica existente de la comunidad de ingeniería de la seguridad. Cada área de proceso tiene un conjunto de objetivos que representan el estado esperado de una organización que está realizando de forma satisfactoria el área de proceso.

La dimensión de la capacidad: comprende las prácticas que indican capacidad de gestión y de institucionalización del proceso. Se denominan "prácticas genéricas", ya que se aplican en un amplio rango de dominios. Estas prácticas genéricas representan las actividades que deberían realizarse como parte de hacer las prácticas base. Las prácticas genéricas se agrupan en áreas lógicas denominadas "Características Comunes", que están organizadas en "Niveles de Capacidad", los cuales representan el aumento de la capacidad de la organización. Cada uno de estos niveles se pueden caracterizar por las frases:

• **Nivel 1** Realizado informalmente: *"tiene que hacerlo antes de poder gestionarlo".*

• **Nivel 2** Planificado y seguido: *"comprender lo que está ocurriendo en el proyecto antes de definir los procesos de toda la organización".*

• **Nivel 3** Bien definido: *"utilice lo mejor de lo que ha aprendido a partir de sus proyectos para crear los procesos de toda la organización".*

• **Nivel 4** Controlado cuantitativamente: *"no puede medirlo hasta que no sepa lo que es"* y *"la gestión con medida sólo* es *significativa cuando mide las cosas correctas".*

• **Nivel 5** Mejorando continuamente: *"una cultura de mejora continua requiere una base de sólida práctica de gestión, procesos definidos* y *objetivos medibles".*

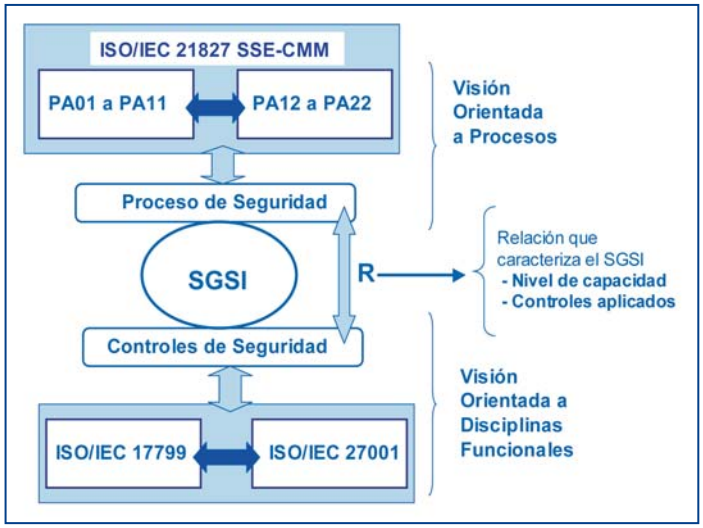

Figura 2. Integración de ISO/IEC 27001 y SSE-CMM en el modelo de Referencia.

A diferencia de las prácticas base, las prácticas genéricas están ordenadas de acuerdo a la madurez. Poniendo las prácticas base y las prácticas genéricas juntas se proporciona una forma de verificar la capacidad de una organización para realizar una actividad particular.

Por las limitaciones de extensión del artículo no se entra en detalles de SSE-CMM; los interesados en ampliar información pueden visitar la dirección de ISSEA (International Systems Security Engineering Association): **http://www.issea.org/**

Visión funcional y de procesos en un proyecto de SGSI

En un proyecto de SGSI estas dos visiones están permanentemente presentes y seguirán estando presentes después de que el SGSI esté implantado.

Cuando se examina en detalle la ISO/IEC 27001, se puede apreciar que los dos aspectos más fuertes que ofrece son la descripción detallada de los controles y el método PDCA (Plan-Do-Check-Act) para aplicarlos, dejando total libertad en los criterios para establecer el proceso global de seguridad y elegir el método para analizar, evaluar y gestionar los riesgos. En un proyecto de SGSI, esta libertad también puede convertirse en una deficiencia, pues en cierta forma *"está ligando estos proyectos a la propia experiencia de diseño de procesos de seguridad de los ejecutores del mismo"*. Lo contrario sucede cuando se examina en detalle SSE-CMM (ISO/IEC 21827): se puede apreciar que los dos aspectos mas importantes que ofrece son la descripción de todas las áreas de proceso (en total 22), que hay que considerar para analizar, diseñar e implantar el proceso de seguridad y los controles más adecuados en el proceso de seguridad, dejando total libertad para elegir los que se consideren más adecuados a la organización.

Así, la primera pregunta que puede hacerse un jefe de proyecto de un SGSI sería: *¿por qué no utilizar en su desarrollo ambas normas y aprovechar para su éxito las ventajas y complementariedad que ofrecen?* Esta pregunta es la que se hicieron, hace cuatro años, los Ingenieros de los países mencionados y su respuesta fue clara*: ¡utilicemos ambas!* No es casual que sea en estos países en los que en la actualidad se concentra el mayor número de SGSI certificados. Entonces, *¿cómo se pueden utilizar e integrar ambas normas en un proyecto de SGSI?* La respuesta no es sencilla, pues lo primero que se *necesita es un modelo de referencia sencillo que integre ambas visiones Funcionales o Procesos, y que además sea válido para cualquier organización*. Una vez conseguido este modelo, el paso siguiente es situar dentro del mismo tanto los controles de ISO/IEC 27001 como las áreas de proceso de SSE-CMM (ISO/IEC 21827).

¿Cómo se ha realizado el modelo de referencia para proyectos de SGSI?

Por limitaciones de espacio, se explica de forma resumida según el esquema de la **Figura 2.**

a) Visión orientada a disciplinas funcionales (ver Tabla): en el modelo se diferencian las seis disciplinas funcionales: Seguridad Fundamental; Seguridad Ambiental y en Infraestructuras; Seguridad en los Sistemas; Seguridad en Comunicaciones y Redes; Seguridad Física; Seguridad de las Personas.

b) Visión orientada a procesos (ver **Tabla**): en el modelo se han identificado ocho subprocesos de seguridad: Gestión Estratégica de la Seguridad; Cumplimiento Legal y de Estándares Aplicables; Identificación, Clasificación y Evaluación de Activos; Análisis y Evaluación de Riesgos de Seguridad; Tratamiento y Gestión de Riesgos de Seguridad; Gestión de la Seguridad Operacional; Seguridad en las Operaciones: Condiciones normales; Seguridad en las Operaciones: Condiciones anormales.

c) El concepto de "Seguridad Fundamental": es muy importante ¿Por qué? Si se examina la tabla se puede ver que incluye un conjunto de controles y subprocesos definidos en ambas normas SSE-CMM (ISO/IEC 21827) y 27001 que son imprescindibles para que el proceso de seguridad realmente exista, mas allá de la mejora de su capacidad, de las necesidades específicas de seguridad en áreas concretas del negocio. Los controles y subprocesos indicados en este nivel

Distribución de controles ISO/IEC 27001 y áreas de proceso SSE-CMM (ISO/IEC 21827) en el modelo de referencia del SGSI.

PROCESOS DESEGURIDAD EN LAS ORGANIZACIONES		1. Gestión Estratégica de la Seguridad	2. Cumplimiento Legal y Estándares Aplicables	3. Identificación, Clasificación y Evaluación de Activos	4. Análisis y Evaluación de Riesgos de Seguridad	5. Tratamiento y Gestión de Riesgos de Seguridad	6. Gestión de la Seguridad Operacional	7. Seguridad en Operaciones: Condiciones Normales	8. Seguridad en Operaciones: Condiciones Anormales
DISCIPLINAS FUNCIONALES	Seguridad Fundamental	**A5 (completo) A6.1 (1,2,3,7) A11.1** PA06 PA07 PA09 PA10 PA11	**A15.1 A6.1.5 A6.2.3 A8.1.1.3 A10.8.2** PA10 PA11	**A7 (completo)** PA02 PA10	**A.6.2.1 A14.1.2** PA02 PA03 PA04 PA05	**A6.1.8 A6.2.2** PA03	**A9.1 A10 (1,2,3) A11.2 A11.6** PA01 PA07 PA08 PA11	**A6.1 (4,6,7) A10 (4,5,6) A10 (7,8,9)** PA07 PA09 PA10	**A13 (completo) A14 (completo)** PA06 PA10
	Ambiental y en Infraestructuras	PA06 PA07 PA09 PA10 PA11 PA02	PA10 PA11 y PA02	PA02 PA10 y PA09	PA02 PA03 PA04 PA05 PA09	PA03 y PA09 PA10	**A9.2** PA01 PA07 PA08 PA11	PA07 PA09 PA10	PA06 PA10 y PA07 PA09
	Seguridad en los Sistemas	**A12.1** PA06 PA07 PA09 PA10 PA11	**A15.2 A15.3** PA10 PA11	PA02 PA10	PA02 PA03 PA04 PA05	**A12.2 A12.3** PA03	**A11.5 A11.7 A12.4 A12.5** PA01 PA07 PA08 PA11	**A12.6** PA07 PA09 PA10	PA06 PA10
	Seguridad en Comunicaciones y Redes	PA06 PA07 PA09 PA10 PA11 y PA01 PA08	PA10 PA11 y PA02	PA02 PA10	PA02 PA03 PA04 PA05	PA03	**A11.4** PA01 PA07 PA08 PA11 PA09 PA10	**A10.10** PA07 PA09 PA10	PA06 PA10 y PA07 PA10
	Seguridad Física	PA06 PA07 PA09 PA10 PA11	PA10 PA11	**A9 (completo)** PA02 PA10	PA02 PA03 PA04 PA05	PA03	PA01 PA07 PA08 PA11	**A6.2 (1,2)** PA07 PA09 PA10	PA06 PA10
	Seguridad de las Personas	PA06 PA07 PA09 PA10 PA11	PA10 PA11	PA02 PA10	**A8.1** PA02 PA03 PA04 PA05	**A8.2** PA03	**A11.3** PA01 PA07 PA08 PA11	**A8.3** PA07 PA09 PA10	PA06 PA10

*Comentarios: **A.x.y.z expresan los controles establecidos en ISO/IEC 27001. PAnn expresan las Áreas de Proceso de Seguridad en SSE-CMM (ISO/IEC 21827)**

son también comunes para el resto de áreas funcionales. (En la Tabla se indica con ▼).

Este modelo en el que se integran ambas visiones de la seguridad, se deriva de la base de conocimientos TPKB, Theoretical and Practical Knowledge Base que desde 2004 está desarrollando ISSPCS (International Systems Security Professional Certification Scheme), que colabora con ISSEA, (International Systems Security Engineering Association).

Ventajas de utilizar la visión integrada Funcional o Procesos en proyectos de SGSI

• **Seguridad fundamental.** En una organización que todavía no tenga definido el Proceso Global de Seguridad, la primera etapa debería ser definirle teniendo en cuenta los subprocesos de seguridad y controles que se proponen en el modelo de referencia.

• **Proyectos de SGSI en ámbitos sectoriales.** En organizaciones encuadradas en sectores específicos como podrían ser: Desarrollo de Software, Hospitales, Banca, Ayuntamientos, etc. con procesos de negocio muy especializados: *"Podrían realizarse proyectos de SGSI concretos con el fin de profundizar en las aportaciones de SSE-CMM (ISO/IEC 21827) en estos sectores".* Su conocimiento es de gran importancia, tanto para conocer mejor las necesidades de seguridad planteadas en estos sectores, como las dificultades propias del sector a tener en cuenta en los proyectos de SGSI a llevar a cabo, *facilitando la creación de patrones para el desarrollo de soluciones de seguridad sectoriales.*

• **Nivel de capacidad.** En un proyecto de SGSI debería de plantearse que el Proceso Global de Seguridad diseñado e implantado pueda ser evaluado con un nivel 3 de capacidad "Bien definido": un SGSI en cuya evaluación se obtuviera un Nivel 1 "Realizado Informalmente" tendría deficiencias importantes. *El modelo de referencia facilita la consecución del nivel que se desee alcanzar.*

• **Ámbito legislativo (*) (leyes y reglamentos).** Puesto que tanto las leyes como sus reglamentos tienen en cuenta procesos de seguridad de la información: *"Podrían realizarse proyectos que tuvieran como objetivos revisar las leyes bajo la visión de procesos de seguridad y descubrir las aportaciones que esta norma puede hacer para: entender, mejorar y aplicar las mismas".*

No se puede aplicar SSE-CMM (ISO/IEC 21827) si no se conoce. La Facultad de Informática de la Universidad Politécnica de Madrid (UPM), puede contribuir a que las organizaciones interesadas conozcan la norma y pueda ser de uso común en los Proyectos de SGSI, como ya lo es en los países mencionados. ■

José Antonio Calvo-Manzano Villalón
Dpto. LSSI
UNIVERSIDAD POLITÉCNICA DE MADRID
jacalvo@fi.uom.es

Ana de las Heras Muñoz
Ingeniero en Informática (UPM)
BSI Lead Auditor ISO/IEC 27001
TELEFÓNICA INGENIERÍA Y SEGURIDAD
Ana.delasherasmunoz@telefonica.es

REFERENCIAS

[ISO], ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements **http://www.iso.org**

[SSE-CMM, 2003], SSE-CMM Project, Systems Security Engineering Capability Maturity Model Description Document, Version 3.0, Jun 15, 2003. **http://www.sse-cmm.org**

[BS 7799-2:2002, 2002], Information security management systems Specification with guidance for use. BSI publications, 2002. **http://www.bsi-global.com**

[ISSEA] International Systems Security Engineering Association. **http://www.issea.org**

International Register of ISMS Certificates **http://www.iso27001certificates.com/**