ISO/IEC 21827
Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

Ignacio Ballesteros González
w140062
05448027V

21 de junio de 2017

A causa del interés de clientes y proveedores en crear un marco que proporcione herramientas de mejora en las aplicaciones y principios de la ingeniería de la seguridad, *ISO*[1] e *IEC*[2] se desarrolla el estándar *SSE-CMM*®.

1. Introducción

q

El estándar *SSE-CMM*® busca crear una herramienta para las organizaciones de ingeniería de la seguridad que sirva para medir sus- prácticas, definir mejoras, establecer un indicador de confianza en la organización y evaluar la capacidad en seguridad de un proveedor.

Los fines de *SSE-CMM*® es proporcionar un marco en el que los productos y procesos desarrollados tengan la capacidad de ser continuados y reproducibles. Además de buscar la eficiencia y seguridad de los mismos. La *SSE-CMM*® no pretende sustituir los procesos de las organizaciones, sino que estos se enmarquen en ella.

La realización de *SSE-CMM*® ha contado con la participación de más de 50 organizaciones y con grupos de trabajo pequeños, medianos y grandes; además de contar con una evaluación y comentarios de críticos independientes.

2. Arquitectura Modelo

La *SSE-CMM*® divide la ingeniería de seguridad en tres areas principales: riesgo, ingeniería y garantía. Estas areas no son independientes entre sí.

Riesgo Combinación de amenazas, vulnerabilidades e impacto.

[1] International Organization for Standarization
[2] International Electrotechnical Commision

Ingeniería Proceso de creación de soluciones enmarcadas en un marco de restricciones y requisitos.

Garantía Grado de confianza que satisface según *NIST94a*.

2.1. Modelo básico

La *SSE-CMM*® tiene dos dimensiones, *dominio* y *capacidad*. El *dominio* se compone de todas las prácticas que colectivamente definen la ingeniería de la seguridad. La *capacidad* representa prácticas de los modelos de gestión.

Estas dos dimensiones se distribuyen en un modelo matricial que permite ubicar la capacidad técnica de ingeniería de la seguridad de una organización.

La *SSE-CMM*® enumera una serie de prácticas y procesos que se relacionan con el *ciclo de vida* de un proceso.

2.2. Prácticas básicas

La *SSE-CMM*® enumera y describe las prácticas básicas que hay en un proceso de seguridad. Sin embargo, no especifica que toda organización deba poseer o evaluar todas ellas, ya que puede que tenga una sola o una mezcla de varias.

La *SSE-CMM*® menciona 11 prácticas básicas, ampliadas posteriormente en un anexo.

Administración de controles de seguridad Asegurarse de que se cumplen los procesos de control de seguridad. Se contempla la asignación de responsabilidades, la eduación en seguridad y la responsabilidad de revisar el cumplimiento de los requisitos.

Evaluación del impacto Identificación de posibles impactos que puede ocasionar los riesgos, ya sea de manera tangible (financión) o intagible (reputación). Se realizan listas de prioridades, evaluaciones y métricas de impactos. Incluye la identificación y monitorización de los mismos.

Evaluación de los riesgos Identifica, analiza y evalúa los riesgos en seguridad en los que se pueda ver envualta la organización. Se selecciona un método de evaluación, evalúa el nivel de exposición y su certeza[3]. Incluye también la priorización de riesgos y su monitorización.

Evaluación de las amenazas Identifica las amenazas en la seguridad, sus propiedades y caracteristicas. Incluye la identificación de amenazas naturales, humanas, métricas, capacidad de respuesta y la probabilidad de suceder. También la monitorización y sus características.

[3]Métrica de que realmente ocurra.

Evaluación de vulnerabilidades Se identifican las vulnerabilidades a las que se enfrente la organzación, eligiendo unos métodos, técnicas y criterios para caracterizarlas. Recolecta la información relacionada con las vulnerabilidades y monitoriza sus cambios.

Construcción de un argumento de aseguración Proceso para convencer al cliente de la seguridad propia. Se identifican los objetivos, las medidas de control y monitorización. Recoge evidencias y realiza análisis sobre ellas. Con ello se contruye el argumento acerca de la propia seguridad.

Coordinación de la seguridad Se asegura de que todas las partes son conscientes y están involucradas en las actividades de ingeniería de la seguridad. Define la coordinación, sus mecanismos y facilitación de los mismos.

Monitorización de la postura en la seguridad Se asegura de que todos los fallos son identificados y comunicados.

Proporcionar información en seguridad Proporciona a arquitectos, diseñadores, implementadores y/o usuarios la información que necesitan.

Especificación de las necesidades de seguridad Indentifica y relaciona las necesidades acerca del sistema. Define las bases en seguridad para satisfacer los requisitos legales, políticos y organizativos.

Verificación y validación de la seguridad Se asegura del cumplimiento de los compromisos adquiridos.

La *SSE-CMM*® define además otros procesos organizativos en anexos, continuación de los aquí descritos.