Seguridad y Calidad en Aplicaciones Web

Unidad N° 6: Normas

Referente de Cátedra: Walter R. Ureta
Plantel Docente: Pablo Pomar, Walter R. Ureta

CMM

El Modelo de Madurez de Capacidades o CMM (Capability Maturity Model), es un modelo de evaluación de los procesos de una organización, predecesor de CMMI. Fue desarrollado inicialmente para los procesos relativos al desarrollo e implementación de software por la Universidad Carnegie-Mellon para el SEI (Software Engineering Institute).

CMMi

Los modelos CMMI® (Capability Maturity Model® Integration) son colecciones de buenas prácticas que ayudan a las organizaciones a mejorar sus procesos. Estos modelos son desarrollados por equipos de producto con miembros procedentes de la industria, del gobierno y del Software Engineering Institute (SEI).

SSE-CMM

El System Security Engineering Capability Maturity Model o Modelo de Madurez de Capacidades en la Ingeniería de Seguridad de Sistemas es un modelo derivado del CMM y que describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de sistemas.

Nació a partir de 1993 bajo los auspicios de la Agencia Nacional de Seguridad (NSA) de los E.U.A., con la participación de numerosas compañías de los sectores de tecnologías de la información, seguridad y defensa

ISO/IEC 21827:2008 Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

CMM-Niveles

Capability Level 1 – Performed Informally
Capability Level 2 – Planned and Tracked
Capability Level 3 – Well Defined
Capability Level 4 – Quantitatively Controlled
Capability Level 5 – Continuously Improving

CMM-SECURITY BASE PRACTICES

PA01 – Administer Security Controls
PA02 – Assess Impact
PA03 – Assess Security Risk
PA04 – Assess Threat
PA05 – Assess Vulnerability
PA06 – Build Assurance Argument
PA07 – Coordinate Security
PA08 – Monitor Security Posture
PA09 – Provide Security Input
PA10 – Specify Security Needs
PA11 – Verify and Validate Security

CMM-PROJECT AND ORGANIZATIONAL BASE PRACTICES

PA12 – Ensure Quality
PA13 – Manage Configurations
PA14 – Manage Project Risk
PA15 – Monitor and Control Technical Effort
PA16 – Plan Technical Effort
PA17 – Define Organization's Systems Engineering Process
PA18 – Improve Organization's Systems Engineering Processes
PA19 – Manage Product Line Evolution
PA20 – Manage Systems Engineering Support Environment
PA21 – Provide Ongoing Skills and Knowledge
PA22 – Coordinate with Suppliers

SSE-CMM-Dimensiones

	PA01 – Administer Security Controls	PA02 – Assess Impact	PA03 – Assess Security Risk	PA04 – Assess Threat	PA05 – Assess Vulnerability	PA06 – Build Assurance Argument	PA07 – Coordinate Security	PA08 – Monitor Security Posture	PA09 – Provide Security Input	PA10 – Specify Security Needs	PA11 – Verify and Validate Security	PA12 – Ensure Quality	PA13 – Manage Configuration	PA14 – Manage Project Risk	PA15 – Monitor and Control Technical Effort	PA16 – Plan Technical Effort	PA17 – Define Org. Systems Eng. Process	PA18 – Improve Org. Systems Eng. Process	PA19 – Manage Product Line Evolution	PA20 – Manage Systems Eng. Support Env.	PA21 – Provide Ongoing Skills and Knldge	PA22 – Coordinate with Suppliers
5.2 Improving Proc. Effectiveness																						
5.1 Improving Org. Capability																						
4.2 Objectively Managing Perf.																						
4.1 Establish Meas. Quality Goals																						
3.3 Coordinate Practices																						
3.2 Perform the Defined Process																						
3.1 Defining a Standard Process																						
2.4 Tracking Performance																						
2.3 Verifying Performance																						
2.2 Disciplined Performance																						
2.1 Planned Performance																						
1.1 Base Practices Are Performed																						
Common Features																						
Process Areas																						
	Security Engineering Process Areas											**Project and Organizational Process Areas**										

SAMM - Software Assurance Maturity Model

El modelo de madurez para el aseguramiento de software es un marco de trabajo abierto para ayudar a las organizaciones a formular e implementar una estrategia de seguridad para Software que sea adecuada a las necesidades específicas que está enfrentado la organización.

OWASP
The Open Web Application Security Project

SAMM - Software Assurance Maturity Model

Las bases de este modelo están construidas alrededor de las funciones de negocio relacionadas al desarrollo de Software, se incluyen una serie de prácticas relacionadas a cada función.

SAMM - Software Assurance Maturity Model

Niveles de Madurez

Cada una de las prácticas de seguridad tiene tres niveles de madurez bien definidos y un nivel inicial (cero) implícito. Los detalles de cada nivel difieren entre las prácticas pero generalmente representan:

0 Punto de inicio implícito, las actividades en la practica no se han realizado.

1 Entendimiento inicial y provisión ad hoc de la práctica de seguridad.

2 Incremento en la eficiencia y/o efectividad de la práctica de seguridad.

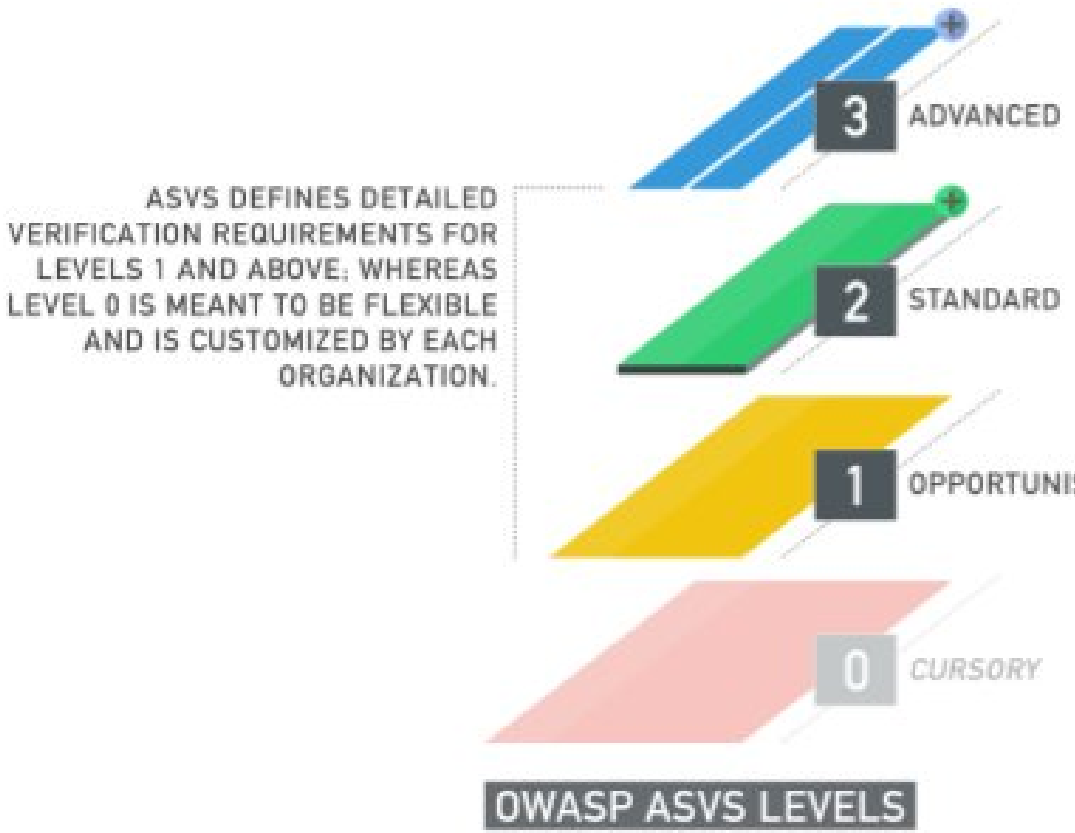
3 Dominio amplio de la práctica de seguridad.

ASVS – Application Security Verification Standard

El objetivo principal del ***Application Security Verification Standard (ASVS)*** del OWASP es normalizar el rango de cobertura y el nivel de rigurosidad disponible en el mercado cuando se realiza la verificación de seguridad de aplicaciones web.

Este estándar podrá ser utilizado tanto por los consumidores como por los proveedores del servicio o la herramienta.

ASVS – Application Security Verification Standard



Nivel 3 es para las aplicaciones más críticas - aplicaciones que realizan transacciones de alto valor, contienen datos médicos sensibles, o cualquier aplicación que requiere el más alto nivel de confianza.

Nivel 2 es para aplicaciones que contienen datos confidenciales, que requiere protección y es el nivel recomendado para la mayoría de las aplicaciones.

Nivel 1 es para bajos niveles de garantía, y es completamente comprobable con pentesting.

Indica que la aplicación solo a pasado algún tipo de verificación definida por la organización.

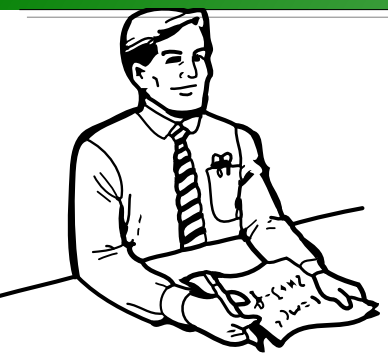
ASVS – Application Security Verification Standard

	Applicability	Building			Building, Configuration, Deployment Assurance and Verification			Assurance and Verification	
Level 1	All apps		Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Penetration Testing	DAST
Level 2	All apps	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
Level 3	High Assurance	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST

Legend	Acceptable	Suitable

ASVS – Áreas de Requerimientos de Seguridad

V1 - Arquitectura, Diseño y Modelado de Amenazas
V2 - Autenticación
V3 - Gestión de sesiones
V4 - Control de Acceso
V5 - Validación, Desinfección y Codificación
V6 - Criptografía almacenada
V7 - Manejo y Registro de Errores
V8 - Protección de Datos
V9 - Comunicación
V10 - Código Malicioso
V11 - Lógica de Negocio
V12 - Archivos y Recursos
V13 - API y Servicios Web
V14 - Configuración



Normativa de Ciberseguridad De la República Argentina

Leyes

- Ley 26.388 de Delito informático
- Ley 25.326 de Protección de Datos Personales
- Decreto Reglamentario N° 1558/2001
- Ley 25.506 de Firma Digital
- Decreto Reglamentario N° 2628/2002
- Ley 26.904 de Grooming

https://www.argentina.gob.ar/jefatura/innovacion-publica/direccion-nacional-ciberseguridad/normativa

Normas

- **GDPR**, o *"Reglamento General de Protección de Datos"* define la protección del tratamiento y circulación de los datos de personas fisicas pertenecientes a la Union Europea. *[2016:2018]*
- **CCPA**, *"California Consumner Privacy Act"* define el control que los consumidores de California tienen sobre la información personal recolectada comercialmente. Extendiéndose sobre el derecho al conocimiento, borrado, cancelación de permiso de distribucion/venta, discriminación por uso de datos, etc. *[2018]*
- **HIPAA**, o *"Health Insurance Portability and Accountability Act",* es la ley federal de los Estados Unidos que define los estándares para la protección de la información sensible relativa a la salud de un paciente. *[1996]*

Normas

- **PCI DSS**, *"Payment Card Industry Data Security Standard"*, es un estándar de seguridad de la información definido y mantenido por el *"Payment Card Industry Security Standards Council"* para organizaciones que manejan información de tarjetas de crédito El mismo establece revisiones de cumplimiento anuales o trimestrales con diferentes métodos en función del volumen de operaciones manejadas, como:
  - SAQ, Self-Assessment Questionnaire
  - QSA, Qualified Security Assessor (Externo) con *"AOC, Attestation on Compliance"*
  - ISA, Internal Security Assessorcon con "ROC, Report on Compliance"

Normas

- **A4609** Comunicación del BCRA que define los requisitos mínimos de gestión, implementación, y control de los riesgos relacionados con tecnología informática, sistemas de información y recursos asociados para las entidades financieras.
- **ISO 9001** en el alcance sobre el software y sobre los procesos productivos de la organización. No siempre sobre el desarrollo, puede ser en la identificación de requisitos, en el propio desarrollo y por ejemplo en la entrega y mantenimiento.
- **ISO/IEC 9003** Ingeniería del software. Guía de aplicación de la ISO 9001:2000 al software (NO es CERTIFICABLE. Es una norma de buenas prácticas para definir con más detalle los conceptos de software sobre los procesos de la organización).
- **ISO/IEC 12207** *Information Technology / Software Life Cycle Processes*, es el estándar para los procesos de ciclo de vida del software de la organización. Es la base para ISO 15504-SPICE.

Normas

- **ISO/IEC 15504** (conocida como SPICE - *Software Process Improvement And Assurance Standards Capability Determination*). Un conjunto de 7 normas para establecer y mejorar la capacidad y madurez de los procesos de las organizaciones, proporcionando los principios requeridos para realizar una **evaluación de la calidad de los procesos.** La definición de los procesos se realiza sobre ISO/IEC 12207. La familia de normas 15504 espera que la nueva **ISO 29110** sea publicada para crear definitivamente el esquema internacional de certificación, que actualmente está creado con procesos de calidad en las entidades de certificación (realizando evaluaciones externas sobre I**SO/IEC 15504-2** e **ISO/IEC TR 15504-7:2008**.

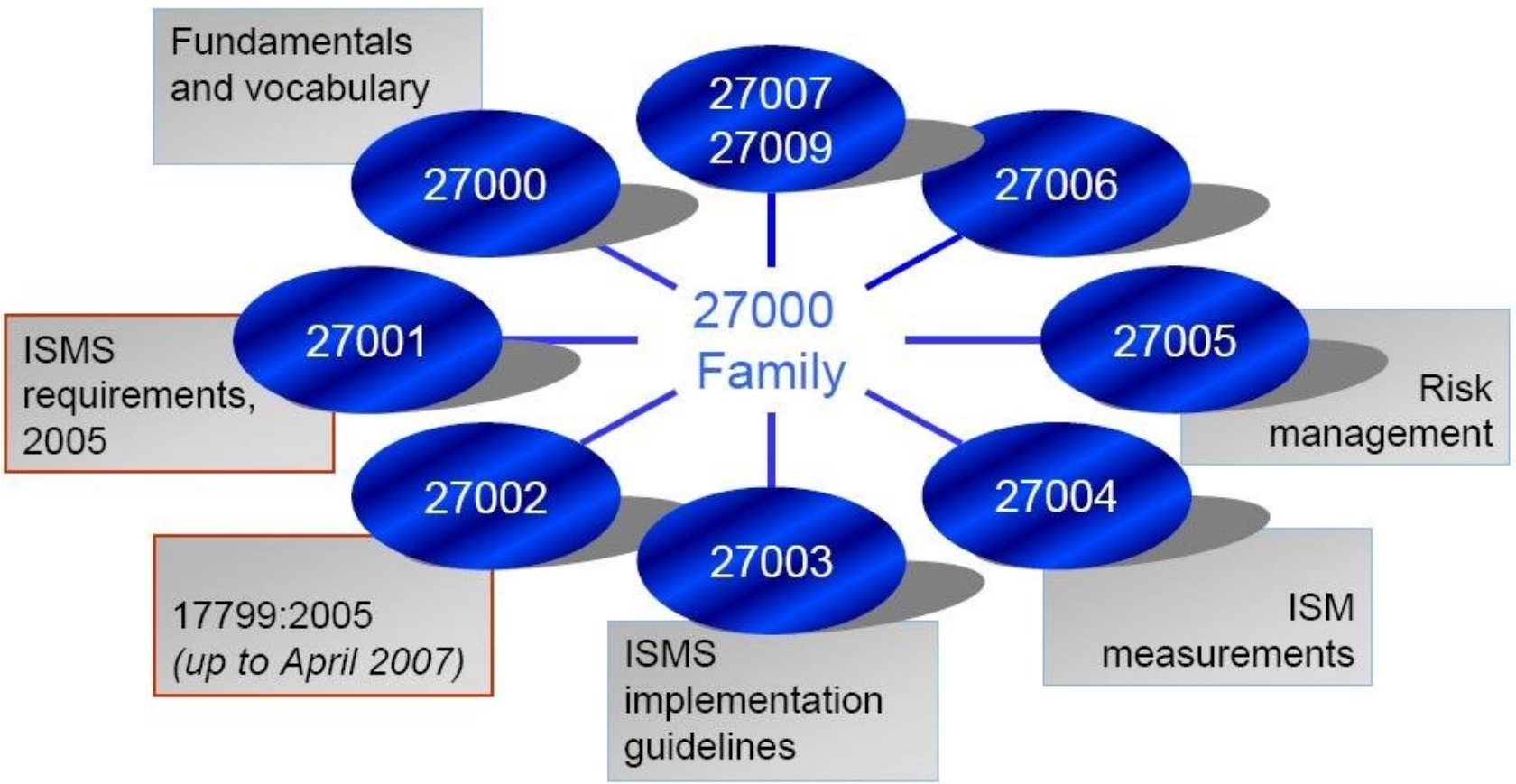
- **ISO/IEC 9126.** Desarrolladas entre 1991 y 2001. *Software engineering – Product quality* consta de 4 partes. La serie de normas ISO/IEC 9126 define las características de calidad del **producto de software** (parte 1), las métricas internas y externas (partes 2 y 3), y la calidad en uso, que explica cómo la calidad del producto está sujeta a las condiciones particulares de uso (parte 4).

Normas

- **ISO/IEC 14598.** Desarrolladas entre 1999 y 2001. *Software product evaluation,* **Evaluación del producto de software**, la familia consta de 6 partes. Directamente relacionada con ISO 9126.
- **ISO 25000.** La familia de normas 25000 establecen un modelo de calidad para el **producto software** además de definir la evaluación de la calidad del producto. Tiene 5 partes publicadas. Pretenden sustituir a ISO 9126 e ISO 14598 ya que desde 2001 no se publicaron nuevas versiones.
- **SCRUM**. No es una **norma**, es un método sencillo y práctico para empezar a practicar calidad. Fabricar y gestionar el desarrollo en tres fases fundamentales: una breve fase de planificación, en la cual se realizan las labores básicas de una planificación breve: visión general del proyecto (estimación muy general, viabilidad del sistema) y construcción del Backlog. por un lado y por otro el desarrollo de la arquitectura al detalle; otra de desarrollo, en la cual tienen lugar los famosos Sprints, y otra final de entrega y balance de los éxitos y fracasos logrados

Normas

- **ISO/IEC 27000:** es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.



Referencias

ISO/IEC 21827:2008 . Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)
https://www.iso.org/standard/44716.html
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

OWASP SAMM
https://owaspsamm.org
https://owasp.org/www-project-samm

OWASP ASVS
https://owasp.org/www-project-application-security-verification-standard
https://github.com/OWASP/ASVS

ISO/IEC 27000:2018 . Information technology — Security techniques — Information security management systems — Overview and vocabulary
https://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

Referencias

General Data Protection Regulation (GDPR)

https://gdpr.eu/tag/gdpr
https://gdprinfo.eu/es
https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679

California Consumer Privacy Act (CCPA)

https://www.oag.ca.gov/privacy/ccpa

Health Insurance Portability and Accountability Act (HIPAA)

https://www.hhs.gov/hipaa/index.html

Payment Card Industry (PCI)

https://www.pcisecuritystandards.org