UNIDAD 6 – NORMAS

CMM

(Capability Maturity Model) Modelo de madurez de capacidades. Modelo de evaluación de los procesos de una organización. Es la madurez que presenta una empresa que desarrolla software.

CMMi

(Capability Maturity Model Integration) colecciones de buenas practicas que ayudan a las organizaciones a mejorar sus procesos.

SSE-CMM

(System Security Engineering - Capability Maturity Model) modelo derivado del CMM que describe las características esenciales de los procesos que deben existir en una organización para asegurar una buena seguridad de sistemas.

Niveles de CMM

1. **Capability Level 1 – Performed Informally** (Nivel abstracto, todos lo hacen)
2. **Capability Level 2 – Planned and Tracked** (presentan fechas estimadas del producto)
3. **Capability Level 3 – Well Defined** (compara con productos anteriores para calcular un estimativo de tiempo, además, conlleva una certificación del trabajo a realizar y documenta todos los procesos)
4. **Capability Level 4 – Quantitatively Controlled** (ademas de lo que se hace en el nivel 3, implementa matrices sobre cada desaerrollo)
5. **Capability Level 5 – Continuously Improving** (busca mejorar las matrices continuamente)

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**

Estas primeras 11 demuestran las áreas de procesos

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**

SAMM – Software Assurance Maturity Model
Modelo de madurez para la seguridad del software. Desarrollado por la OWASP y sirve como una guía para ayudar a las organizaciones a evaluar, mejorar y medir la seguridad en el ciclo de vida del desarrollo de software.
Las bases de este modelo están construidas alrededor de las funciones de negocio relacionadas al desarrollo de software. Se dividen en 5 partes:

- Gobierno
- Diseño
- Implementación
- Verificación
- Operaciones

Niveles de Madurez
Las practicas de seguridad tienen tres niveles de madurez bien definidos y un nivel inicial implícito.

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 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 puede ser utilizado por los consumidores como también por los proveedores.

Niveles

- **Nivel 0:** Indica que la app solo ha pasado algún tipo de verificación definida por la organización.
- **Nivel 1:** Bajos niveles de garantía, y es completamente comprobable con pentesting.
- **Nivel 2:** App que contienen datos confidenciales, que requiere protección. Nivel recomendado para todas las apps.
- **Nivel 3:** App que realizan transacciones de alto valor, datos médicos sensibles, etc. Las que poseen un alto nivel de confianza.

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

- Ley 26.388 de Delito Informatico
- 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

Normas

- **GDPR:** define la protección del tratamiento y circulación de los datos de personas físicas pertenecientes a la Union Europea.
- **CCPA:** define el control que los consumidores de California tienen sobre la información personal recolectada comercialmente.
- **HIPAA:** Ley federal de los EEUU que define los estándares para la protección de la información sensible con relación a la salud.
- **PCI DSS:** Estándar de seguridad de la información definido para organizaciones que manejan información de tarjeas de crédito.
- **A4609:** Define los requisitos mínimos de gestión, implementación y control de los riesgos relacionados con la tecnología informática asociados para las entidades financieras (BCRA).
- **ISO 9001:** Alcance sobre el software y sobre los procesos productivos de la organización.
- **ISO/IEC 9003:** Guía de aplicación de la ISO 9001:2000.
- **ISO/IEC 12207:** Estándar para los procesos de ciclo de vida del software de la organización.
- **ISO/IEC 15504:** Conjunto de 7 normas para establecer y mejorar la capacidad y madurez de los procesos de las organizaciones.
- **ISO/IEC 9126:** Define las características de calidad del producto de software, las métricas internas y externas y la calidad de uso.

- **ISO/IEC 14598:** Evaluación del producto de software.
- **ISO 25000:** Establecen un modelo de calidad para el producto de software además de definir la evaluación de la calidad del producto.
- **SCRUM:** Método sencillo y practico para empezar a practicar calidad.
- **ISO/IEC 27000:** Conjunto de estándares que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, publica o privada.
- **ISO/IEC 21827:2008**
- **OWASP SAMM**
- **OWASP ASVS**
- **ISO/IEC 27000:2018**