

SEG 118 – Desarrollo Seguro basado en OWASP

Ing. Carlos Carreño

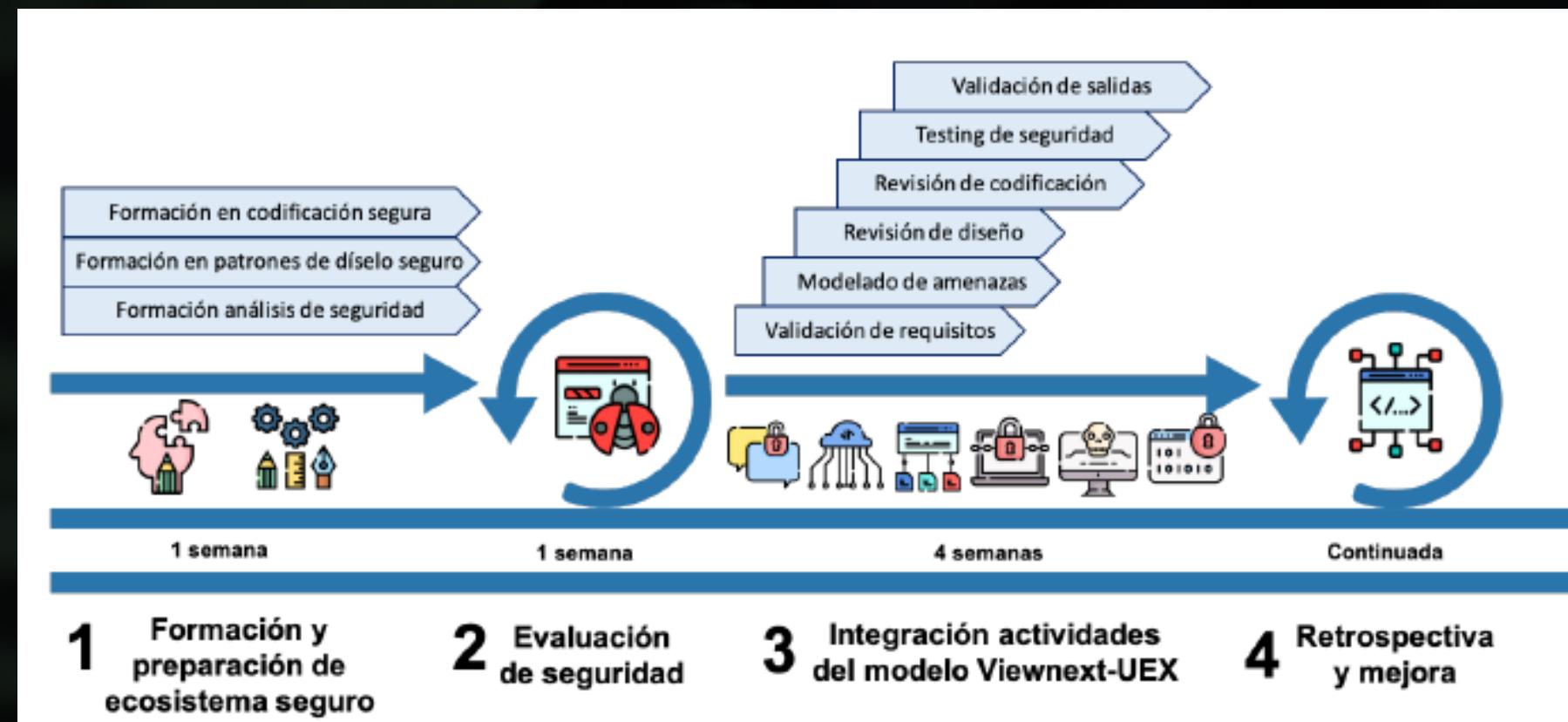
Nov, 2021

MODULO 7: IMPLEMENTACIÓN SEGURA DE APLICACIONES

- Diseño de implementación segura.
- Hardening de software de base.
- Seguridad en el proceso de implementación.
- Administración de la implementación.

Diseño de implementación segura

- Fase de implantación e implementación segura de software



Hardening de software de base

- Hardening (palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema



Proceso de hardening

- Entre las actividades propias de un proceso de hardening se pueden contar las siguientes:
 - ✓ **Configuraciones necesarias para protegerse de posibles ataques físicos o de hardware de la máquina.**
 - ✓ **Instalación segura del sistema operativo**
 - ✓ **Activación y/o configuración adecuada de servicios de actualizaciones automáticas**
 - ✓ **Instalación, configuración y mantención de programas de seguridad**
 - ✓ **Configuración de la política local del sistema**
 - ✓ **Configuración de opciones de seguridad generales**
 - ✓ **Restricciones de software**
 - ✓ **Activación de auditorías de sistema**

... continua

- ✓ Configuración de servicios de sistema
- ✓ Configuración de los protocolos de Red
- ✓ Configuración adecuada de permisos de seguridad en archivos y carpetas del sistema
- ✓ Configuración de opciones de seguridad de los distintos programas
- ✓ Configuración de acceso remoto.
- ✓ Configuración adecuada de cuentas de usuario
- ✓ Cifrado de archivos o unidades según las necesidades del sistema
- ✓ Realizar y programar un sistema de respaldos frecuente a los archivos y al estado de sistema

Seguridad en el proceso de implementación

- Herramientas de seguridad en el proceso de implementación del software

Objetivo	Fase de ejecución	Actividad de seguridad del Modelo Viewnext-UEx	Herramientas
Integración continua	Todo SDLC		Jenkins IBM Cloud Gitlab
Modelado de amenazas	Requisitos Diseño	Validación de requisitos Modelado de amenazas Revisión de diseño	Microsoft IriusRisk
Análisis estático del código fuente			SonarQube PMD Kiuwan Checkmarx FindBugs
Pruebas unitarias de seguridad	Codificación	Revisión de desarrollo	Junit xUnit.net SoapUI
Pruebas de integración de seguridad			Arquillian SoapUI
Test de penetración	Pruebas	Testing de seguridad	AppScan BurpSuite OWASP ZAP Hdiv modSecurity

Administración de la implementación

- Métricas de evaluación de seguridad del software

Tipo de vulnerabilidad	Categoría interna	Criticidad	
Validación de entradas	Arquitectura Desarrollo	Informativa	[0]
Gestión de sesiones		Baja	[0.1-3.9]
Política de control de acceso		Media	[4.0-6.9]
Autorización		Alta	[7.0-8.9]
Sistemas y arquitectura		Crítica	[9-10]
Gestión de errores			
Configuración			
Protección de datos			
Etc.			

Administración de la implementación

- Métricas para medir la ejecución del proyecto de software

Unidad	Fase	Actividades modelo Viewnext-UEx
Horas	Gestión	Estrategia y orientación Validación de salidas
	Análisis y diseño	Definición de riesgos Validación de requisitos Modelado de amenazas Revisión del diseño
	Codificación	Revisión del desarrollo
	Pruebas	Testing de seguridad
	Evaluación	
	Resolución de fallos de seguridad	
	Desarrollo total del módulo	

Referencias

- [https://dehesa.unex.es/bitstream/10662/12316/1/TDUEX 2021 Sancho Nunez.pdf](https://dehesa.unex.es/bitstream/10662/12316/1/TDUEX_2021_Sancho_Nunez.pdf)
- <https://blog.smartekh.com/que-es-hardening>