

# EXCELENCIA PROYECTOS PRIMARIOS



JUNTA DE EXTREMADURA



Financiado por  
la Unión Europea  
NextGenerationEU



*"En cada búsqueda apasionada  
cuenta más la persecución que el  
objeto perseguido"*

**—El Tao del Jeet Kune Do” (1975), Bruce Lee**

# ¿Centro de excelencia?



- **2 centros en Extremadura**
- **45+21 centros en toda España (solo 3 ciber)**
- **Financiación = instalaciones + equipamiento**
- **Formación para el profesorado**
- **Actividades para el alumnado**
- **Prestigio**
- **Trabajo extra por y para el alumnado**



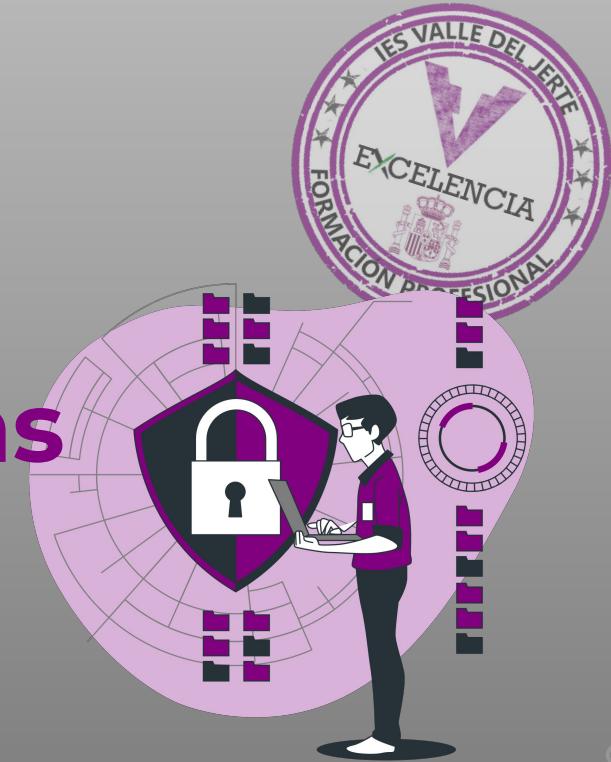
# Proyecto Primario 3



## Introducción de los Principios de Ciberseguridad en los Currículos de FP de la familia de Informática y Comunicaciones



# Herramientas de análisis estático de código y herramientas de escaneo de vulnerabilidades





# ¿Qué es la seguridad en las aplicaciones informáticas?



# ¿En qué fase del desarrollo software tenemos que introducirla?



Perdón que entonces esta va antes...

¿Cuántas fases tenemos dentro del desarrollo software?



# ¿La calidad de mi código influye en la seguridad de mi aplicación?

pero entonces...

¿cómo puedo medir la calidad del código que estoy escribiendo?



¿De dónde provienen las principales amenazas o vulnerabilidades relacionadas con las responsabilidades de los Técnicos de Operación?





**...esta también está antes entonces:**

**¿qué es una debilidad y a que elementos afecta? ¿y una vulnerabilidad?**



... y para terminar, al grano:

¿cómo puedo ver si mis  
equipos, aplicaciones y  
sistemas son vulnerables?

# Contenidos

**01** Seguridad en el ciclos  
de desarrollo Software

**03** Mitigación y/o  
corrección de  
vulnerabilidades

**02** Principales amenazas  
de seguridad

**04** Conclusiones

## 01. Seguridad en el ciclos de desarrollo Software

### ¿Qué es el SDLC?

El SDLC es el ciclo de vida de desarrollo software

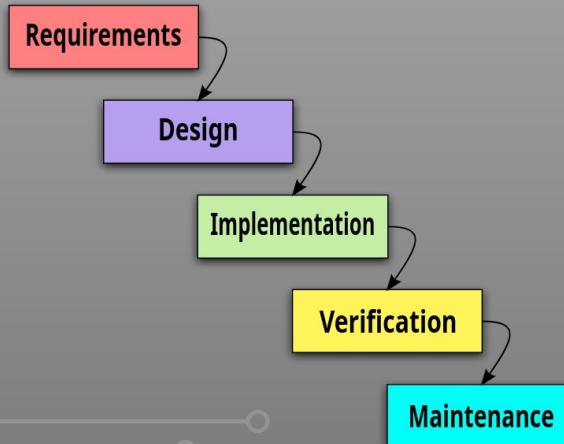
### Fases del SDLC

- Planificación
- Análisis
- Diseño
- Implementación
- Pruebas
- Integración
- Mantenimiento

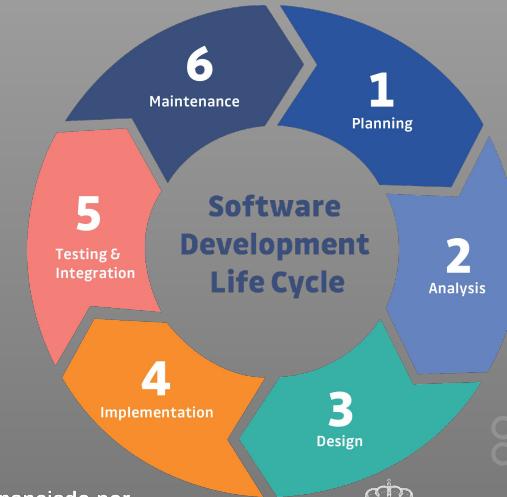
## 01. Seguridad en el ciclos de desarrollo Software

¿Cómo se desarrollan estas fases?

- Módelo Clásico o en cascada



- Modelos circular, en espiral y ágil



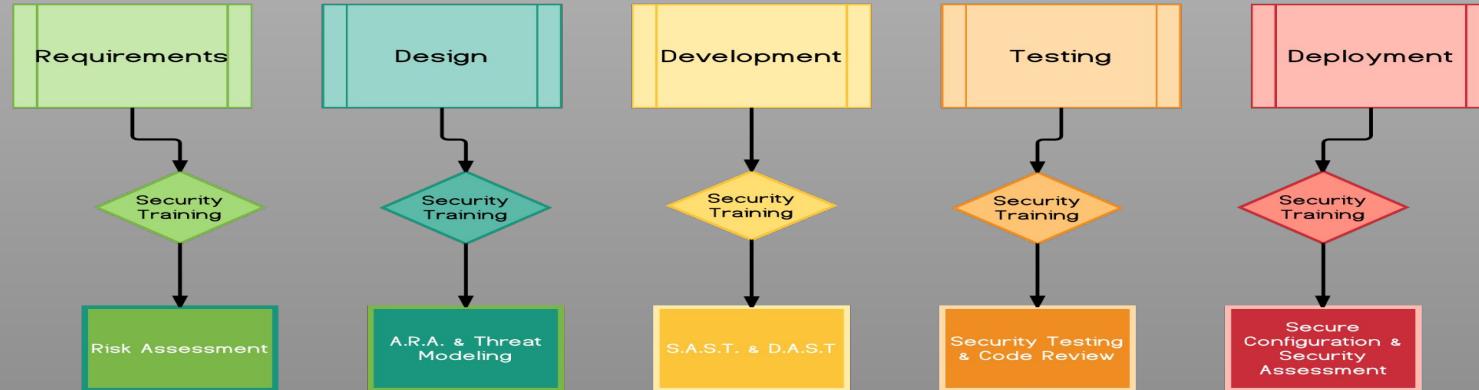
## 01. Seguridad en el ciclos de desarrollo Software

# La pregunta es...

**¿En cuál de estas fases  
introduzco la seguridad?**

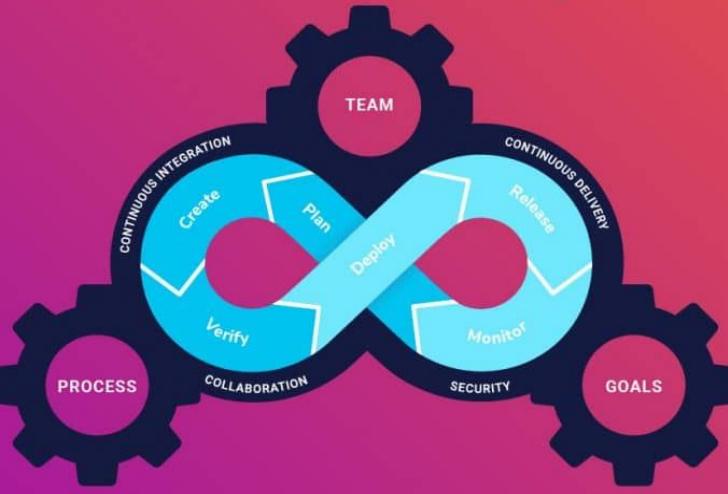
## 01. Seguridad en el ciclos de desarrollo Software

### FROM SDLC TO S-SDLC



## 01. Seguridad en el ciclos de desarrollo Software

# DevSecOps



### DevOps y SecDevOps

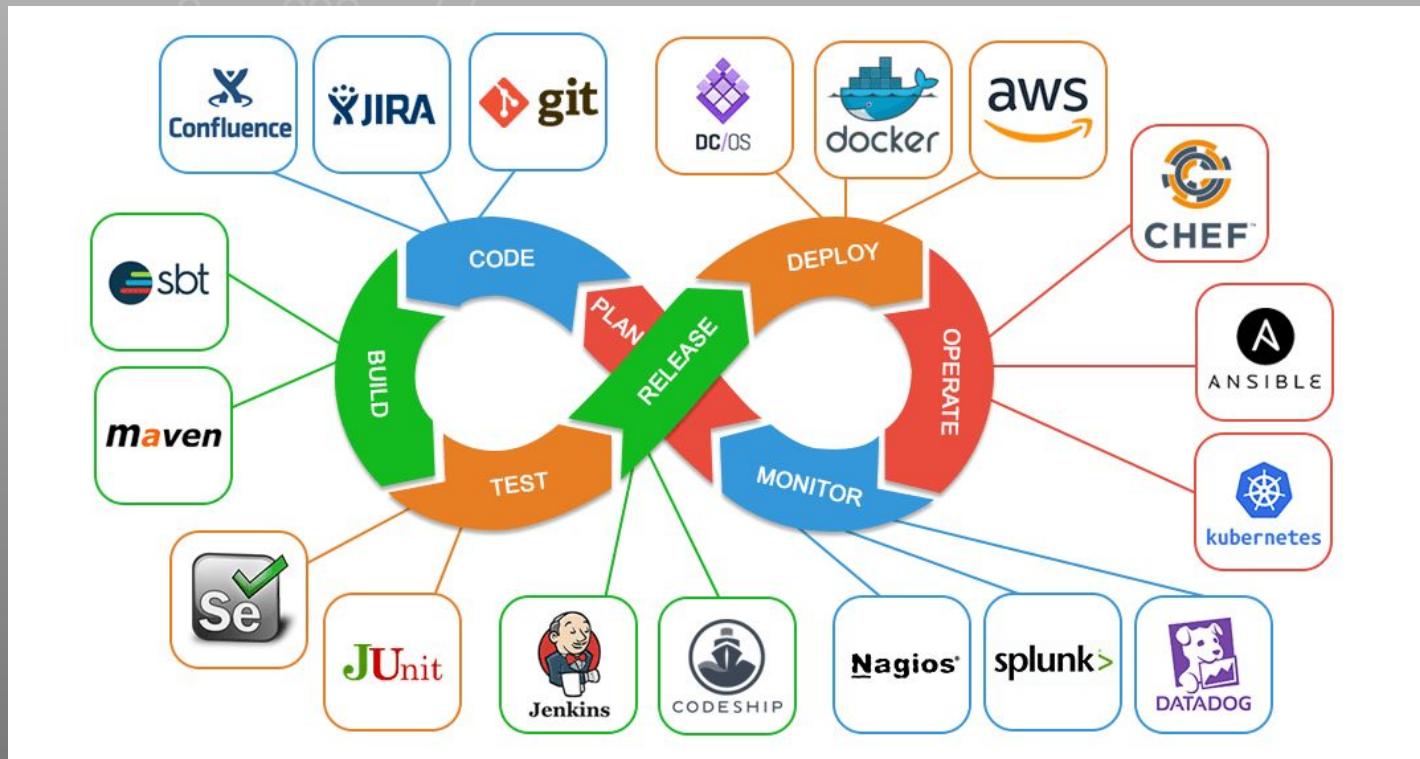
Developers y Operators....

### Fases del SDLC

- Planificación
- Construcción
- Integración continua
- Despliegue continuo
- Operación
- Feedback continuo

# 01. Seguridad en el ciclos de desarrollo Software

## Herramientas en DevOps



## 02. Principales amenazas de seguridad relacionadas con el desarrollo de software

¿De dónde provienen las principales amenazas o vulnerabilidades relacionadas con los desarrolladores?

¿Y con los técnicos de operación?



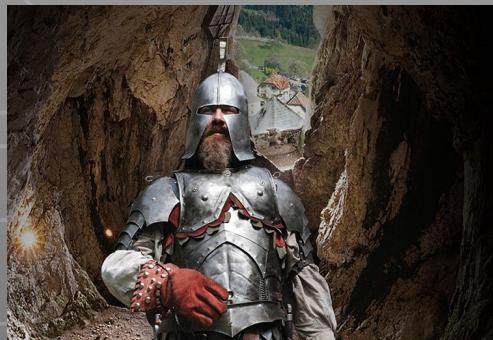


# ¿qué es una debilidad y a que elementos afecta? ¿y una vulnerabilidad?

## 02. Principales amenazas de seguridad

### Conceptos de ciberseguridad

- Sistema
- Activos
- Debilidad



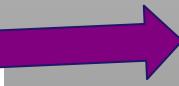
- Vector de ataque
- Vulnerabilidad
- Amenaza
- Ataque



Vector de ataque



Debilidad



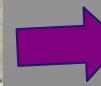
Vulnerabilidad



Amenaza



Ataque



Nuestros Activos



Nuestro Sistema  
Informático o  
aplicación

## 02. Principales amenazas de seguridad

### Organismos y organizaciones

Estas organizaciones mantienen bases de datos e información sobre debilidades, vulnerabilidades etc. También han establecido estándares de seguridad web, que son directrices y prácticas recomendadas para desarrollar, probar y mantener aplicaciones web seguras. Ayudan a prevenir, detectar y mitigar vulnerabilidades y amenazas web comunes.



## 02. Principales amenazas de seguridad

**CWE (Common Weakness Enumeration) es una lista de tipos de debilidades de software dirigida a desarrolladores y profesionales de la seguridad,**

Se puede ver como un catálogo de debilidades documentadas que se suelen cometer programando, y que podría derivar en vulnerabilidades.

Es muy utilizada por distintas herramientas de seguridad encargadas de identificar estas debilidades y para promover la identificación de las vulnerabilidades, mitigación y su prevención.

CWE satisface la necesidad que tienen las grandes organizaciones de conocer y tener catalogadas las distintas debilidades existentes, permitiendo asegurar sus productos frente a fallos de seguridad ya conocidos.



## 02. Principales amenazas de seguridad

**CVE (Common Vulnerabilities and Exposures) es una lista de vulnerabilidades de seguridad de la información públicamente conocidas.**

Es quizás el estándar más usado. Permite identificar cada vulnerabilidad, asignando a cada una un código de identificación único.

Se conoce como identificador CVE (CVE-ID) y está formado por las siglas de este diccionario seguidas por el año en que es registrada la vulnerabilidad o exposición y un número arbitrario de al menos cuatro dígitos según el siguiente formato:



<b>CVE</b>	<b>-2013</b>	<b>-7518</b>
Siglas de Common Vulnerabilities and Exposures	Año de registro	Número de cuatro cifras asignado a la vulnerabilidad

## 02. Principales amenazas de seguridad

**CAPEC (Common Attack Pattern Enumeration and Classification) es un catálogo en forma de esquema de clasificación exhaustiva de patrones de ataque con información relativa a ellos.**

Las entradas de esta lista intentan dar a conocer la perspectiva del atacante y los métodos utilizados para explotar los sistemas.

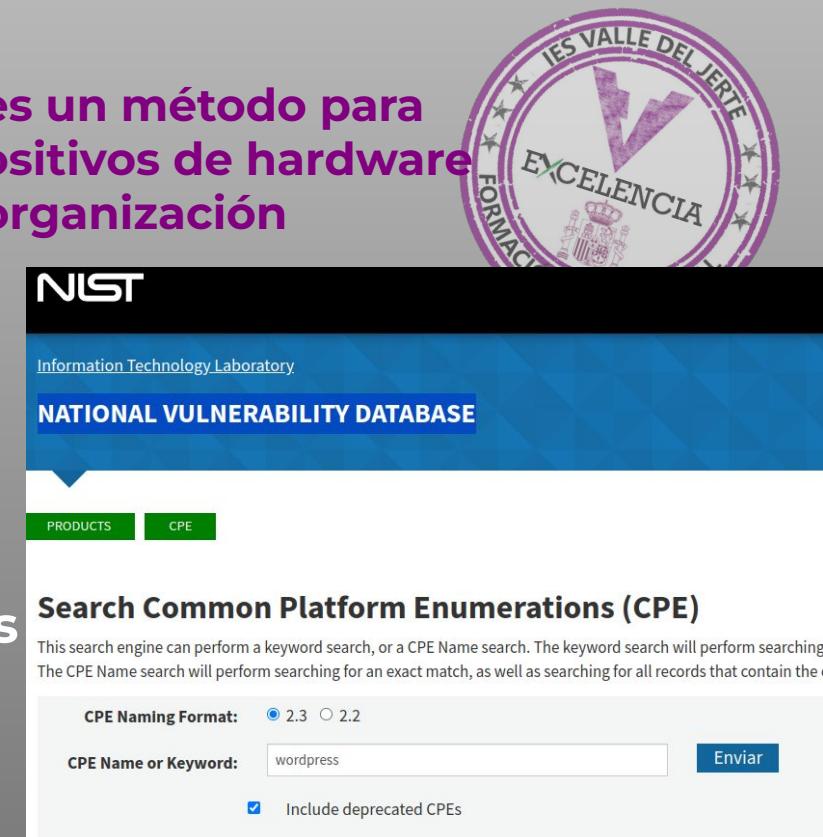
Al igual que los demás catálogos, CAPEC intenta ofrecer la información necesaria para ayudar a mejorar la seguridad en todo el ciclo de vida de desarrollo de software y también apoyar las necesidades de los desarrolladores.



## 02. Principales amenazas de seguridad

**CPE (Common Platform Enumerations) es un método para identificar sistemas, aplicaciones y dispositivos de hardware que forman parte de los activos de una organización**

**En este caso dentro de la NVD (National Vulnerability Database) del NIST, podemos hacer una búsqueda por palabras clave (Sistema Operativo, software, hardware, plataforma, etc. teniendo acceso a las vulnerabilidades asociadas con ellos.**



The screenshot shows the NIST National Vulnerability Database search interface. At the top, there's a navigation bar with the NIST logo and the text "Information Technology Laboratory" and "NATIONAL VULNERABILITY DATABASE". Below the navigation bar, there are two green buttons: "PRODUCTS" and "CPE". The main area features a search form titled "Search Common Platform Enumerations (CPE)". The search input field contains the text "wordpress". There are two radio buttons for "CPE Naming Format": one for "2.3" (which is selected) and one for "2.2". A checkbox labeled "Include deprecated CPEs" is checked. To the right of the search form is a blue "Enviar" button.



## 02. Principales amenazas de seguridad

Del top 10 de los principales riesgos del 2023 según la organización OWASP nos encontramos con que los siguientes tienen que ver con el diseño y desarrollo del software



- Rotura del control de acceso
- Fallos criptográficos
- Inyección

- Diseño inseguro
- Configuración de seguridad defectuosa
- Componentes vulnerables y obsoletos
- Fallos de identificación y autorización
- Fallos de integridad de software y datos
- Fallos en el registro y la supervisión de la seguridad
- Falsificación de Solicitud del Lado del Servidor SSRF

## 03. Mitigación y/o corrección de vulnerabilidades

Y... ¿Qué puedo hacer yo para prevenirlo o mitigarlo?



## 03. Mitigación y/o corrección de vulnerabilidades

- Formarnos e informanos.
- Introducir la seguridad en todo el ciclo de desarrollo software
- Controlar y tener actualizados los Sistemas, Aplicaciones, módulos y librerías que utilizamos.

Aparte, los desarrolladores:

- Controlar flujos de datos.
- Controlar errores.
- Mantener los procesos lo más simples posibles.



## 03. Mitigación y/o corrección de vulnerabilidades

- Sanitizar las entradas y preparar las información de salida.
- Cifrado de todos los datos en almacenamiento y transporte.
- Testear las vulnerabilidades conocidas.
- Implementar políticas eficaces de autorización y permisos.



## 03. Mitigación y/o corrección de vulnerabilidades

Aparte, los Técnicos de operación:

- Controlar los registros del sistema.
- Testear las vulnerabilidades conocidas.
- Implementar políticas eficaces de autorización y permisos.
- Implementar y mantener herramientas y escudos de red: firewall, WAF, etc.



Y aparte de todo esto:

## 03. Mitigación y/o corrección de vulnerabilidades

- Utilizar herramientas de detección de vulnerabilidades:
  - SAST: Análisis estático de código
  - DAST: Análisis dinámico
  - IAST (interactivo), etc...
- Verificar el cumplimiento de los requisitos de OWASP ASVS (Standard de verificación de seguridad en las aplicaciones).



## 04. Análisis estático de código

### ASVS: Estandar de Verificación de Seguridad en las Aplicaciones.

- Es un estandar creada por la Organización OWASP
- Establece 3 niveles de verificación de seguridad:
  - Nivel 1: Oportunista
  - Nivel 2: Standar
  - Nivel 3: Avanzado
- Cada aplicación, según el tipo de datos que maneje, deberá de cumplir los requisitos de seguridad del nivel correspondiente.
- Podemos utilizar ASVS como checklist de comprobación y también probar nuestra aplicación con herramientas automatizadas.





Y ahora para los laboratorios



Descarga el proyecto:  
`git clone`

[https://github.com/jmmedinac03vjp/  
IntroduccionCiberseguridadPP3IESVJP.  
git](https://github.com/jmmedinac03vjp/IntroduccionCiberseguridadPP3IESVJP.git)

# Agradecemos tu colaboración

Por favor rellena el  
siguiente  
formulario para  
evaluar la actividad:



# Y ahora un competición:

accede al siguiente  
enlace, completa las  
misiones y sé el  
primero en capturar la  
bandera:



# Gracias!

¿Alguna pregunta?



[informatica.iesvalledeljerteplasencia.es](http://informatica.iesvalledeljerteplasencia.es)



[coordinacion.cenfp@iesvp.es](mailto:coordinacion.cenfp@iesvp.es)



C/ Pedro y Francisco González, s/n  
10600, Plasencia (Cáceres)



927 01 77 74



**Las imágenes utilizadas corresponden al repositorio de wikimedia Commons, Wonderlane y están protegidos por la licencia Creative Commons.**

**Imagen de herramientas de DevOps perteneciente a geniusitt.com  
Logo de OWASP de OWASP Fundation.**



[informatica.iesvalledeljerteplasencia.es](http://informatica.iesvalledeljerteplasencia.es)



[coordinacion.cenfp@iesvp.es](mailto:coordinacion.cenfp@iesvp.es)



C/ Pedro y Francisco González, s/n  
10600, Plasencia (Cáceres)



927 01 77 74

