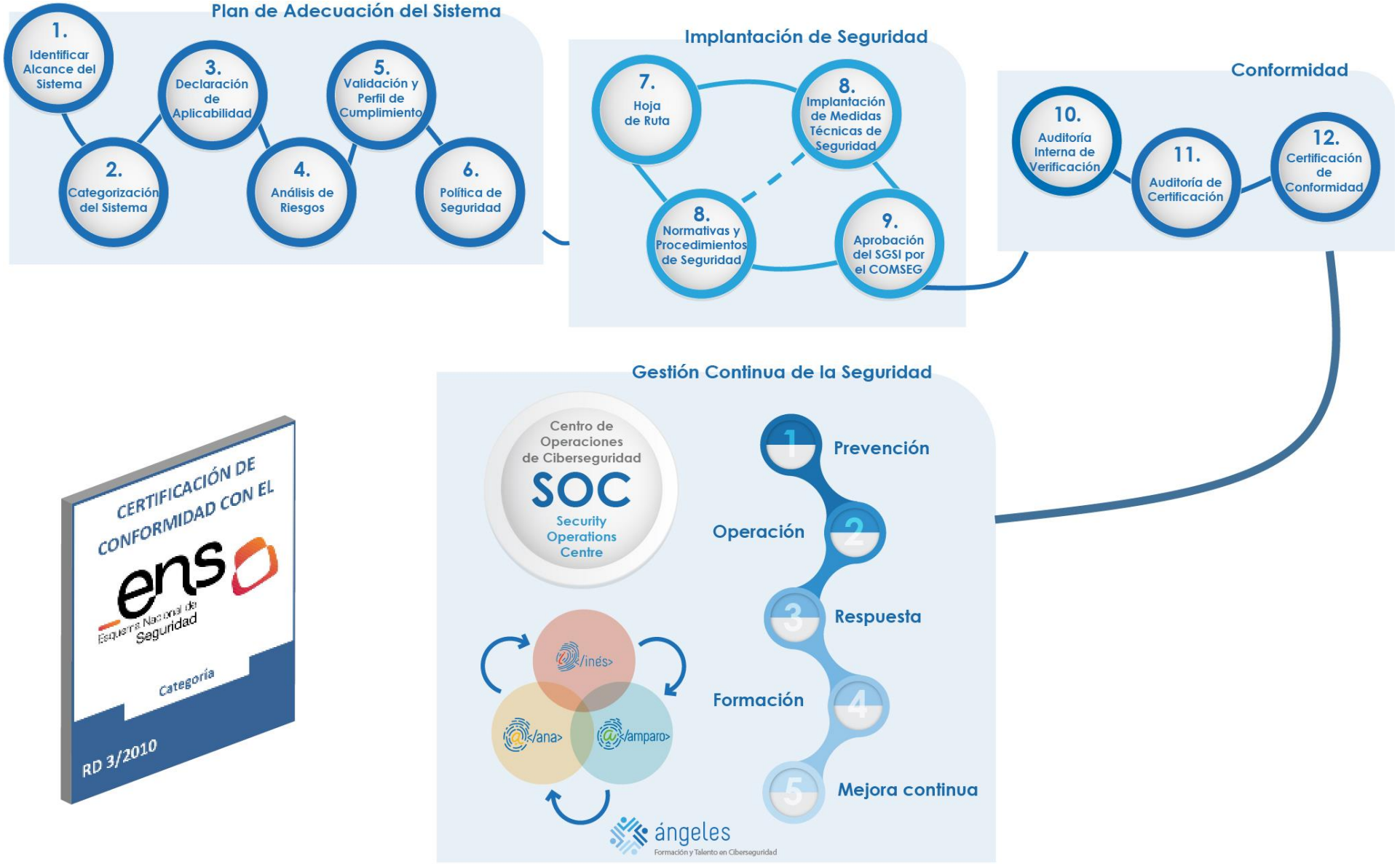
El Esquema Nacional de Seguridad

- ¿Por qué? Ya que nos lo van a pedir
  - “Tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos y está constituido por principios básicos y requisitos mínimos que permitan una protección adecuada de la información”

https://es.wikipedia.org/wiki/Esquema_Nacional_de_Seguridad

- RD 03/2010 “Esquema Nacional de Seguridad” (ENS)
- RD 951/2015 que lo modifica
- Dependiente del Centro Criptológico Nacional
  https://ens.ccn.cni.es/es
- Guías
  https://www.ccn-cert.cni.es/guias/guias-series-ccn-stic/800-guia-esquema-nacional-de-seguridad.html



Fuente: https://ens.ccn.cni.es/index.php/es/conformidad-y-cumplimiento

Fuente: https://ens.ccn.cni.es/index.php/es/conformidad-y-cumplimiento

3. OWASP Top 10

¿Sí, sí, pero cuál de ellos?

OWASP
(Open Web Application Security Project)

Fundación, sin ánimo de lucro que busca mejorar la seguridad del software.

Con multitud de proyectos, de los cuales el más conocido

No es OWASP TOP Ten … aunque sea conocida así por muchos …

… es el OWASP Top Ten Web Application Security **Risks**

Diferentes proyectos

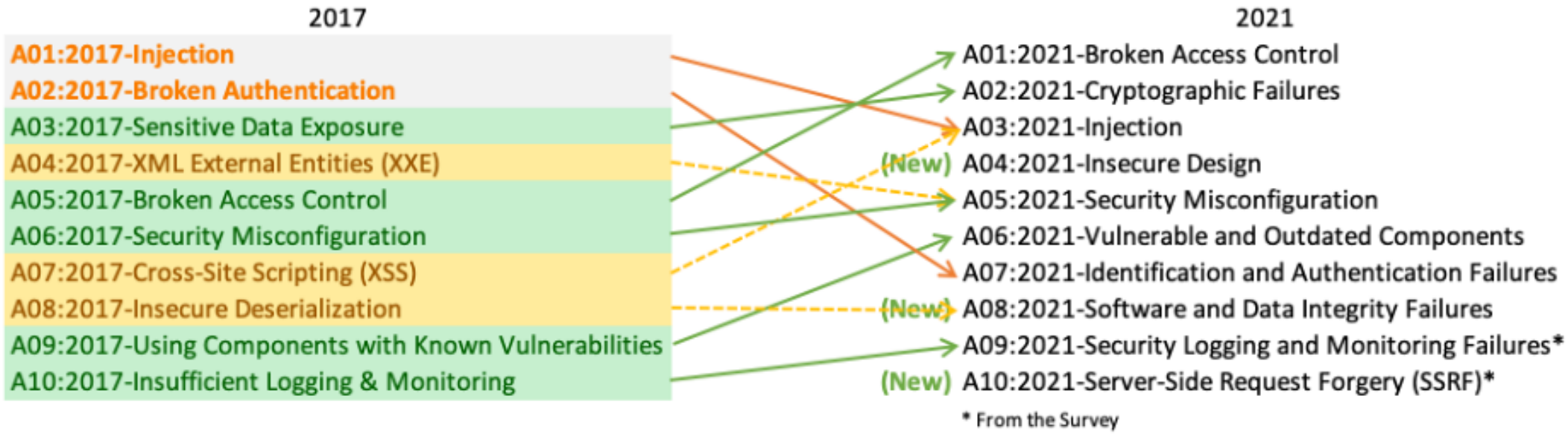
- Hemos resaltado:
  - OWASP ASVS (Application Security Verification Standard)
    - Requisitos y criterios de verificación
  - OWASP TG (Testing Guide)
    - Una referencia general de como acceder a sistemas
- Pero en realidad está dividido en multitud de proyectos que se relacionan entre sí (se complementan… y suplementan en ocasiones)
- Veamos en su web…

Otros proyectos de interés

- OWASP Proactive Controls (OPC)
- OWASP Cheat Sheet Series (OCSS)
- Software Assurance Maturity Model

ascentic/

Nos basamos en la 2017 … pero ya está la 2021

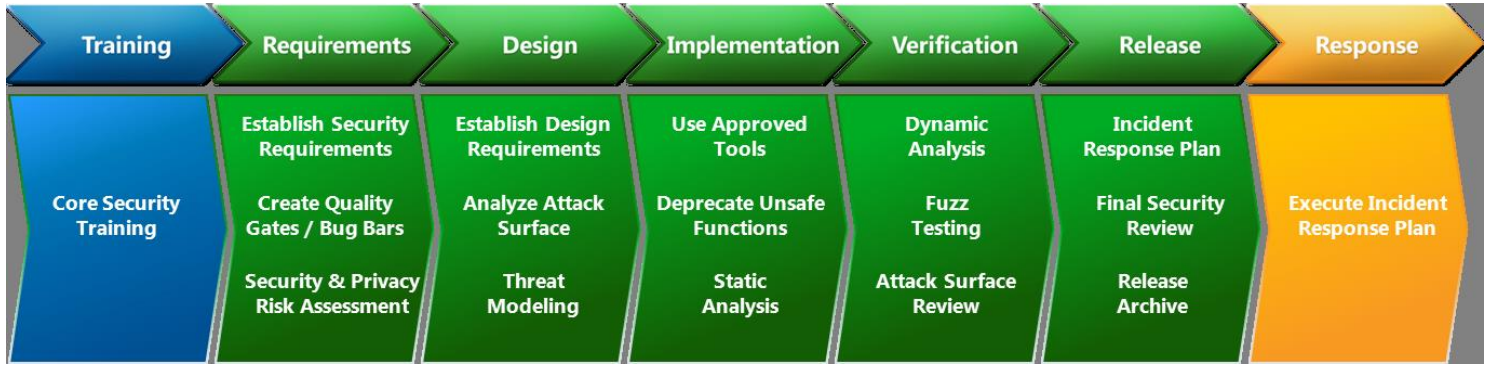


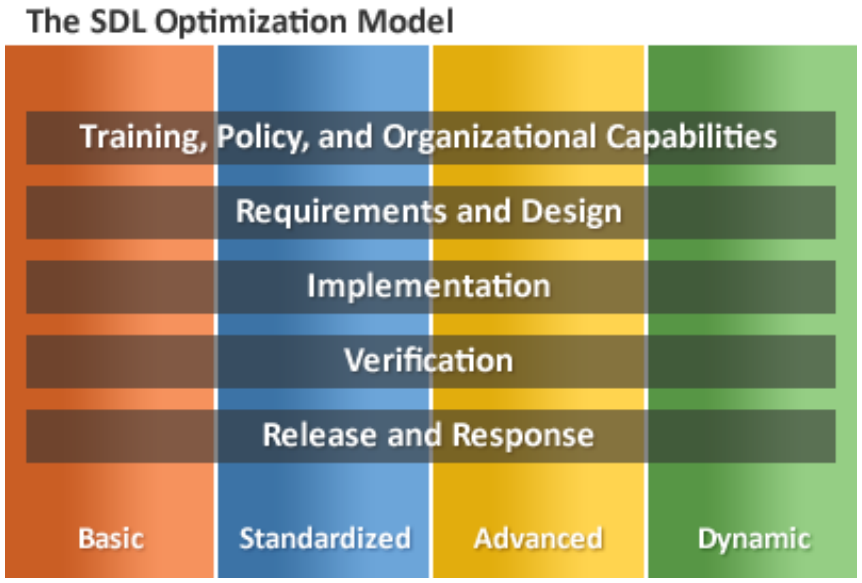
4. Ciclo de Vida de Desarrollo SW seguro

Tradicional y ágil

ascentic/

En el SDL de MicroSoft

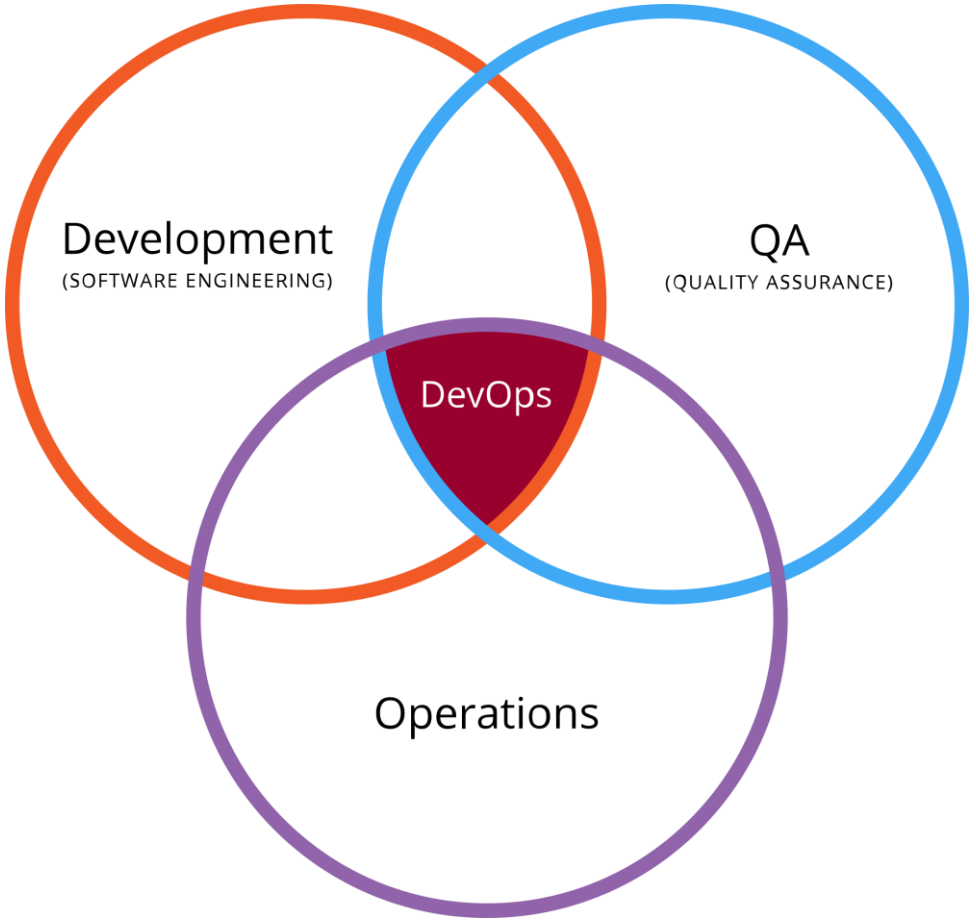




Simplified Implementation of the SDL.doc
http://www.microsoft.com/sdl

ascentic/

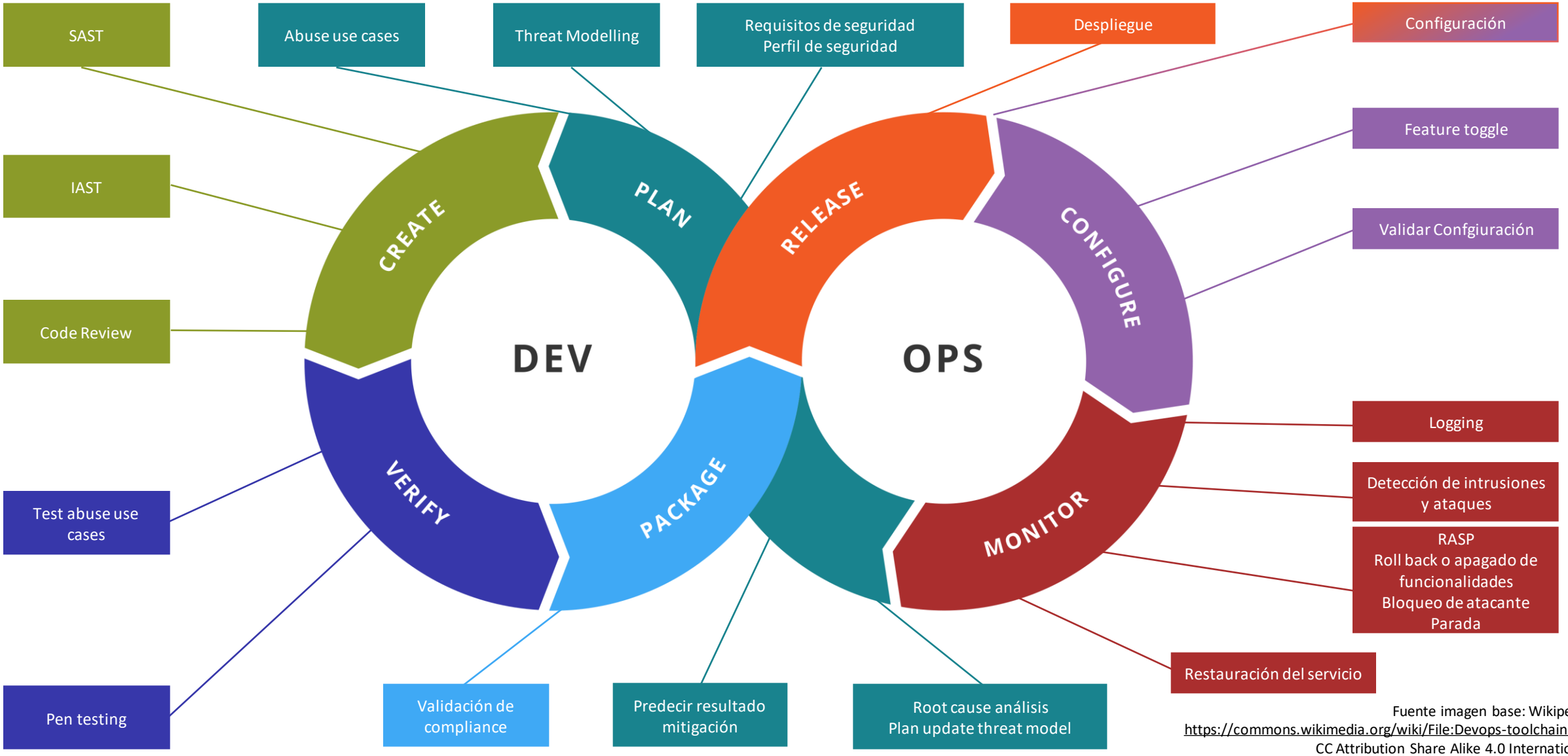
DevOps



Fuente: Wikipedia

ascentic/

DevSecOps



5. Herramientas para el desarrollo SW seguro

Tenemos para distintos usos

- SAST: Static Application Security Testing
- DAST: Dynamic Application Security Testing
- IAST: Interactive Application Security Testing
- WAF: Web Application Firewall
- RASP: Run-time Application Security Protection

ascentic/

6. Taller de pentesting

Manos a la obra

6.a Una aplicación insegura

…o dos

ascentic/

OWASP Juice Shop

https://owasp.org/www-project-juice-shop/

OWASP WebGoat

https://owasp.org/www-project-webgoat/

ascentic/

6.b Herramientas de pen-testing

… más algunas de base

Aislamiento del entorno de trabajo

Buscamos

- Un entorno controlado y aislado
- Optamos por ejecutar máquinas virtuales:
  - Vagrant para el control
  - VirtualBox como software de virtualización
  - Dentro del mismo instalaremos Docker (script)
- Alternativas durante el curso
  - Utilizar otro proveedor de virtualización
  - Crear manualmente una imagen propia, Ubuntu 20.04 based (Ubuntu, mint …)
  - Kali linux

Herramientas generales

Instalamos en la máquina virtual:

- git
- Chrome, Firefox
- Docker
- node/npm
- VSCode
- ZAP

Pentesting – Atendiendo al conocimiento del sistema

Puede ser realizado por equipos internos o externos.

- Black Box: Desconocemos detalles internos del sistema
- White Box: Podemos llegar a tener acceso a la documentación, fuentes…
- Grey Box: Escenario intermedio

Pen-testing

- OWASP ZAP (DEMO)
  - Proxy
  - Spider
  - Atacante
  - Automatización
- Burp Suite (alternativa)
- Metasploit (demasiado agresiva)
- … más muchas otras que vamos a encontrar en

https://owasp.org/www-project-web-security-testing-guide/v41/6-Appendix/A-Testing_Tools_Resource

ascentic/

6.c Ejecución de diferentes ataques

Comienza el taller