ascentic/

Programación Segura

Presentación

Sobre el profesor

- Más de 25 años de experiencia en el sector y todos estos años compaginando la formación con el desarrollo y el I+D+I
- En formación empecé sobre con asignaturas de programación y los últimos años sobre todo BootCamps así como formación a perfiles de desarrollo seniors.
- Actualmente perfil de arquitecto software, aunque he pasado por casi todos los roles.
- Especialidades:
  - SDLC (CI/CD)
  - Computación en la nube
  - Seguridad en el desarrollo, criptografía
  - Data Science
  - Arquitecturas distribuidas e Integración de sistemas

https://www.linkedin.com/in/juan-antonio-l-373571113/

Sobre vosotros

- Una pequeña encuestas:
  - Perfil
  - Experiencia
  - Objetivos
  - …

Objetivos

- El objetivo es doble:
  - se obtendrán conocimientos sobre las formas más habituales de ataques en cada uno de los entornos descritos (web y cliente pesado), y se diseccionará la forma de llevar a cabo dichos ataques, mediante ejercicios prácticos de Pentesting.
  - una vez conocido el problema, se le pondrá solución, mediante técnicas de remediación de vulnerabilidades, y se automatizará la ejecución de los planes de prueba.
- Para la estructuración del seminario se tendrá como referencia las guías, documentos y ejemplos editados por la OWASP Fundation, referente internacional en esta materia.
- El taller de pentesting consiste en una formación eminentemente práctica, durante la misma, el instructor mostrará en tiempo real cómo explotar vulnerabilidades, así como el diseño y ejecución de casos de prueba. Adicionalmente, planteará ejercicios que los asistentes tendrán que resolver individualmente, para posteriormente ser corregidos durante el curso.

Material base

- OWASP Application Security Verification Standard
- OWASP Testing Guide

ascentic/

Licencia

- Los distintos proyectos y contenidos del OWASP Fundation se referencia y/o distribuyen sin modificación bajo sus respectivas licencias:
  - Create Commons Attribution Share Alike 3.0 Unported (CheatSheet, ASVS, Top 10 2021 Security Risk, Top 10 Proactive Controls)
  - Create Commons Attribution Share Alike 4.0 International (Web-site, Web Security Testing Guide, SAMM, Top 10 2017 Security Risk, Risk Rating Methodology)
  - MIT License (Juice Shop)
  - Apache License (ZAP)
  - GPL (WebGoat)

- Los contenidos propios de este curso se construyen sobre los mismos y por tanto se proporcionan bajo el mismo tipo de licencia

  https://creativecommons.org/licenses/by-sa/4.0/

  Esto incluye:
  - las presentaciones
  - los repositorios de código.

  Excluye:
  - las grabaciones de las sesiones (si se aprueba esta posibilidad por los asistentes), ya que las mismas pueden contener datos de identificación personal de los participantes y se mantendrán exclusivamente como traza de auditoría para Fundae.

  Cambios realizados: Los contenidos de textos de OWASP se mantendrán en inglés para su identificación, y en el caso del código a desarrollar consistirá principalmente en procesos de automatización de las distintas pruebas (la licencia se incluirá en sus repositorios)

- Otras referencias breves cubiertos bajo las limitaciones de la Information Society Directive Europea: 5.3
- Contenidos de otros terceros serán mencionados y su licencia indicada (si procede), pero no se consideran como tal entregables del presente curso

Sí he visto más lejos es por estar sobre los hombros de gigantes

(Isaac Newton)

Así pues…

ascentic/

Programación Segura

Bloque 1 – Introducción al desarrollo seguro

Repositorio de ficheros

https://github.com/desarrollo-seguro/introducción-ds

Plan de trabajo

1. Introducción: atacantes y amenazas
2. Seguridad en el desarrollo: competencias, roles y equipos
3. OWASP TOP 10
4. Ciclo de Vida de Desarrollo SW seguro (tradicional y ágil)
5. Herramientas para el desarrollo SW seguro: SAST, DAST
6. Taller de pentesting
    a. Una aplicación insegura
    b. Herramientas de pentesting
    c. Ejecución de diferentes ataques

1.Introducción: atacantes y amenazas

Aclarando conceptos

Seguridad 101

Requisito 1:
La aplicación será segura

(Fin del requisito)

… vale… ¿y ahora qué hacemos?

ascentic/

… la seguridad es multidemensional y compleja, salvando las distancias

Rafael el Gallote referiéndose a Ortega y Gasset

¿Qué hace aquel “gachó” con pinta de estudiao?

¿Filo qué, ezo qué e?

… (silencio)…

Hay gente pa tó

Alguien

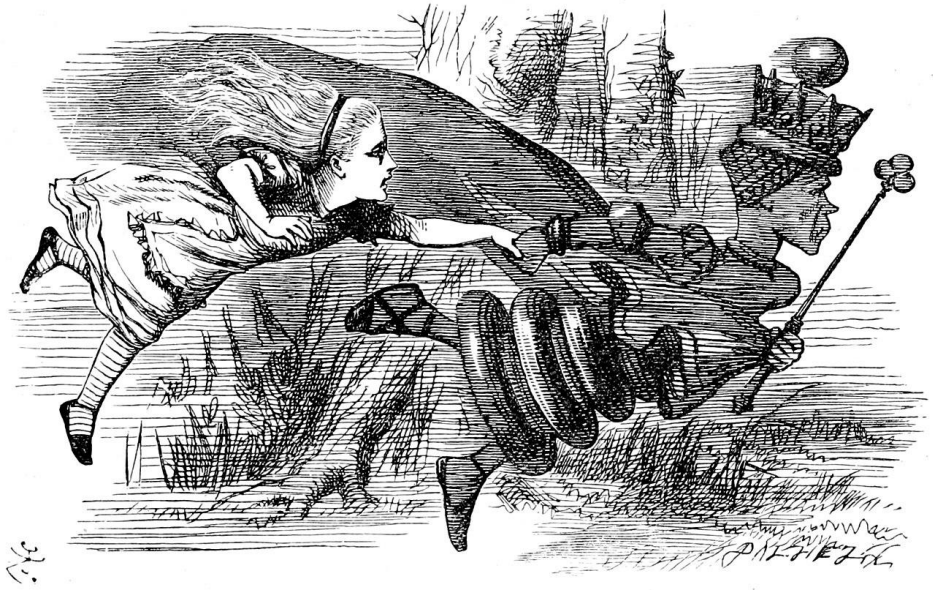
… es filósofo

Es alguien que analiza el pensamiento de la gente, que intentaba que las personas mejoraran en sus maneras de obrar

Una batalla perdida

My dear, here we must run as fast as we can, just to stay in place.

And if you wish to go anywhere you must run twice as fast as that.



Fuente: Alicia en el país de las maravillas, Lewis Carol

Fuente Imagen: Wikipedia, obtenida del libro original, capítulo 2

ascentic/

La seguridad: una medida de la confianza

Security is freedom from, or resilience against, potential harm (or other unwanted coercive change) caused by others. Beneficiaries (technically referents) of security may be of persons and social groups, objects and institutions, ecosystems or any other entity or phenomenon vulnerable to unwanted change.

Security mostly refers to protection from hostile forces, but it has a wide range of other senses: for example, as the absence of harm (e.g. freedom from want); as the presence of an essential good (e.g. food security); as resilience against potential damage or harm (e.g. secure foundations); as secrecy (e.g. a secure telephone line); as containment (e.g. a secure room or cell); and as a state of mind (e.g. emotional security).

The term is also used to refer to acts and systems whose purpose may be to provide security (e.g.: security companies, security forces, security guard, cyber security systems, security cameras, remote guarding).

Computer security, also known as cybersecurity or IT security, refers to the security of computing devices such as computers and smartphones, as well as computer networks such as private and public networks, and the Internet.

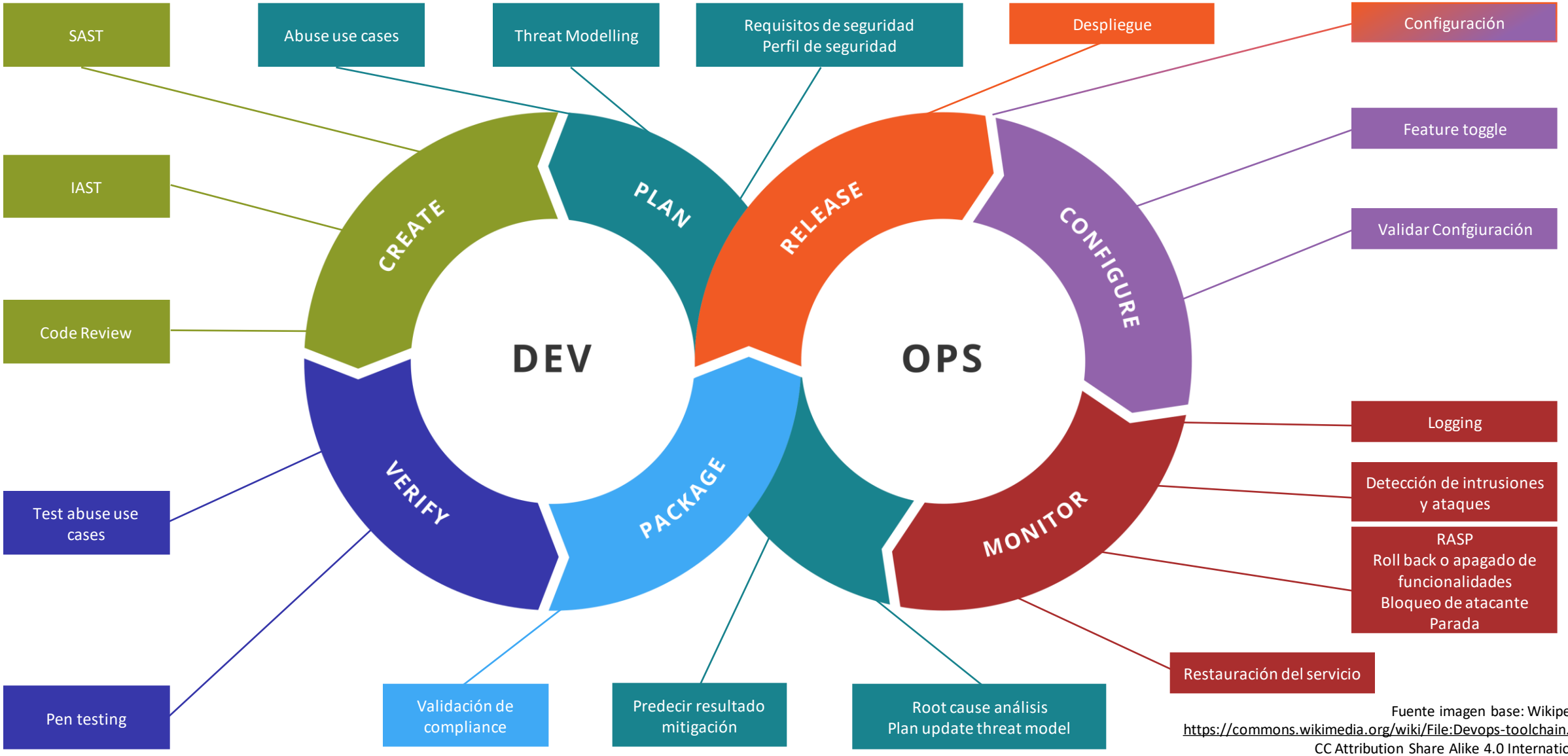
Fuente: Wikipedia

Una definición más informal… y tramposa

Lo que hacemos para proteger algún tipo de **activo** que puede ser **vulnerable** a un **ataque**

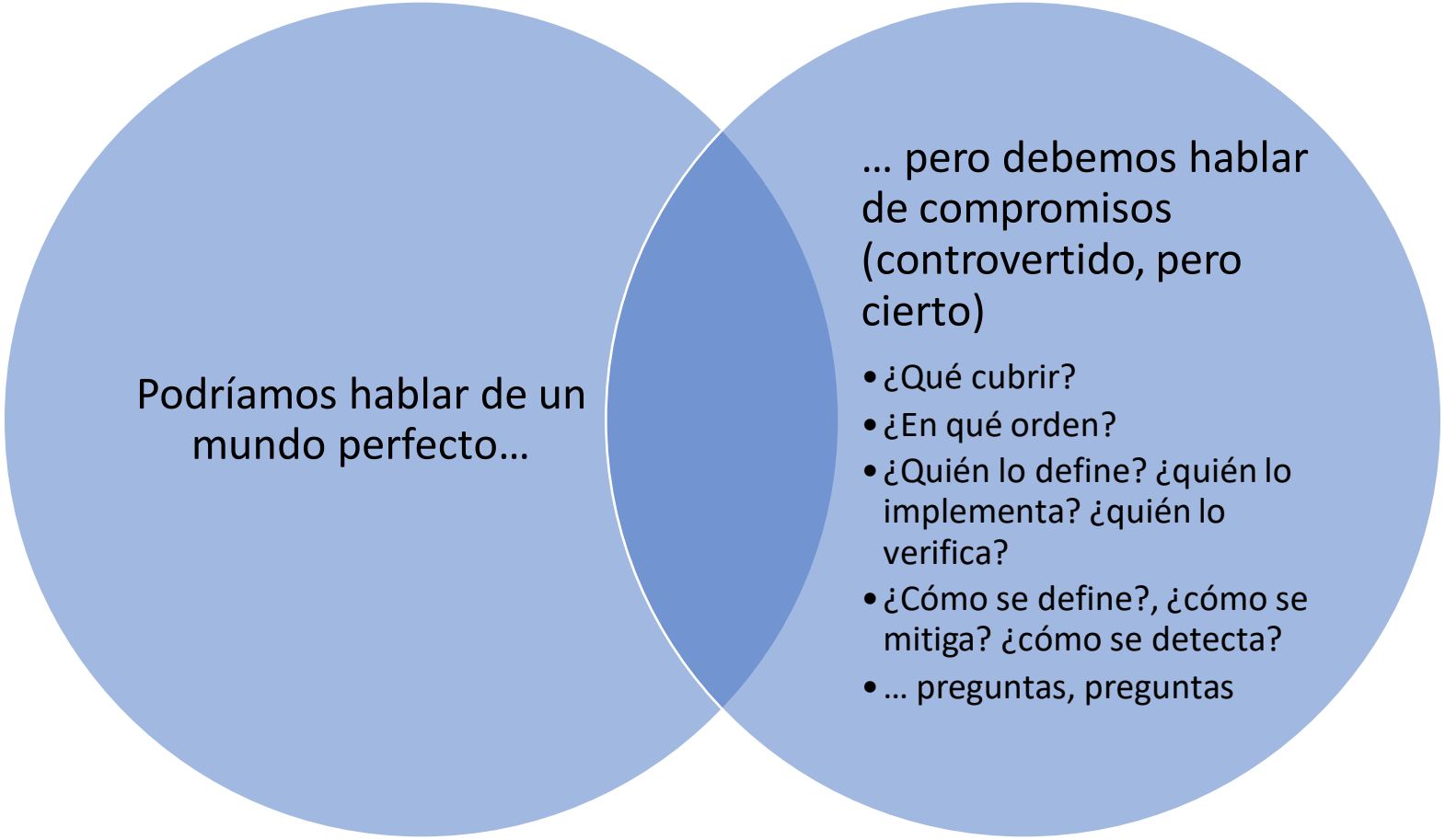
ascentic/

Desarrollo seguro… atención, spoilers



ascentic/

¿Se pueden eliminar todos los riesgos?



Objetivos o dimensiones de la seguridad

- **Confidencialidad**
- **Integridad**
- **Disponibilidad**
- Otros
  - **Autenticación**
  - **Trazabilidad**
  - **No repudio**

Nuestro perfil de seguridad: En base a cada objetivo

El **nivel** deseado para cada objetivo puede ser:

- Alto
- Medio
- Bajo

Normalmente establecido por la disrupción de negocio en caso de no alcanzarlo

El eslabón más débil define la fuerza de una cadena, así que el **Perfil de Seguridad de un Sistema** está basado sobre el mayor nivel de entre todos los objetivos

Confidencialidad:	Bajo
Integridad:	**Medio** <- Perfil de Seguridad del sistema
Disponibilidad:	Bajo
…	Bajo

Principios de diseño

- **Economy of mechanism**: Keep the design as simple and small as possible.
- **Fail-safe defaults**: Base access decisions on permission rather than exclusion.
- **Complete mediation**: Every access to every object must be checked for authority.
- **Open design**: The design should not be secret.
- **Separation of privilege**: Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible than one that allows access to the presenter of only a single key.
- **Least privilege**: Every program and every user of the system should operate using the least set of privileges necessary to complete the job.
- **Least common mechanism**: Minimize the amount of mechanism common to more than one user and depended on by all users.
- **Psychological acceptability**: It is essential that the human interface be designed for ease of use, so that users routinely and automatically apply the protection mechanisms correctly.
- **Work factor**: Compare the cost of circumventing the mechanism with the resources of a potential attacker.
- **Compromise recording**: It is sometimes suggested that mechanisms that reliably record that a compromise of information has occurred can be used in place of more elaborate mechanisms that completely prevent loss.

Fuente: Saltzer and Schroeder's design principles

https://web.mit.edu/Saltzer/www/publications/protection/Basic.html

Está muy bien pero…

… aun estamos lejos de tener una idea de como implementar la seguridad

Partiendo de la última definición de seguridad

Assets: including people, buildings, machines, systems and information assets

Threat: a potential source of harm.

Vulnerability: the degree to which something may be changed (usually in an unwanted manner) by external forces.

Risk: a possible event which could lead to damage, harm, or loss.

Vulnerabilidades

CVE Common Vulnerabilities and Exposure

https://cve.mitre.org/

CWE Common Weakness Enumeration

SANS/CWE 25

https://cwe.mitre.org/data/definitions/1337.html

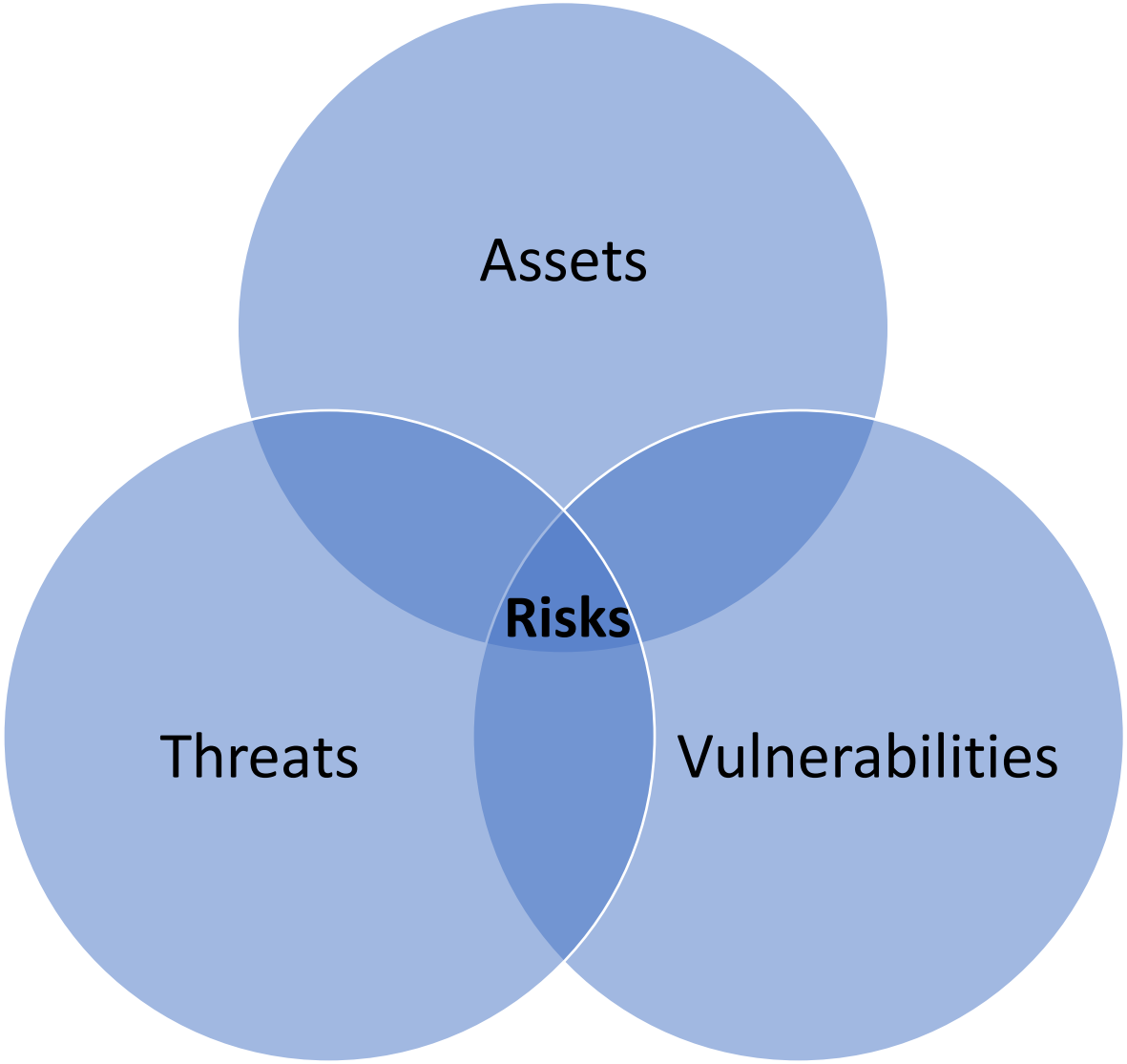
relación con OWASP 2017 Top 10

https://cwe.mitre.org/data/definitions/1026.html

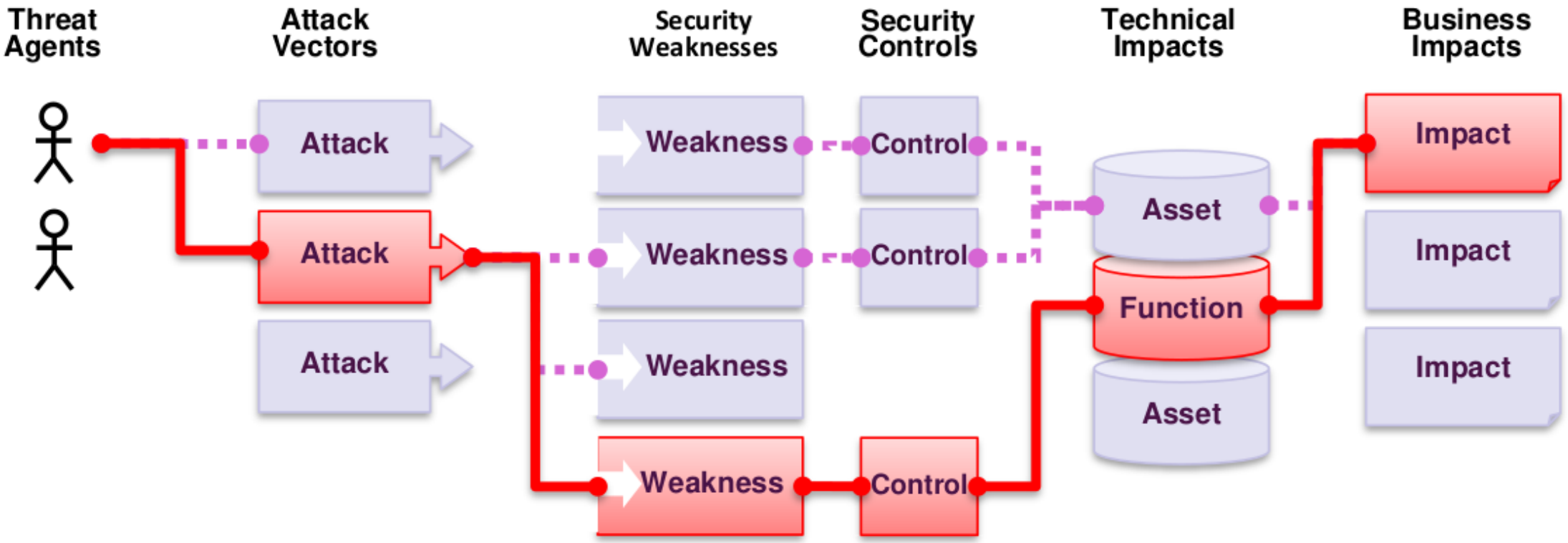
Common vulnerability Scoring System

https://www.first.org/cvss/calculator/3.1

Riesgos



Riesgo como proceso



Thread Modeling

- What are we working on?
- What can go wrong?
- What are we going to do about it?
- Did we do a good job?

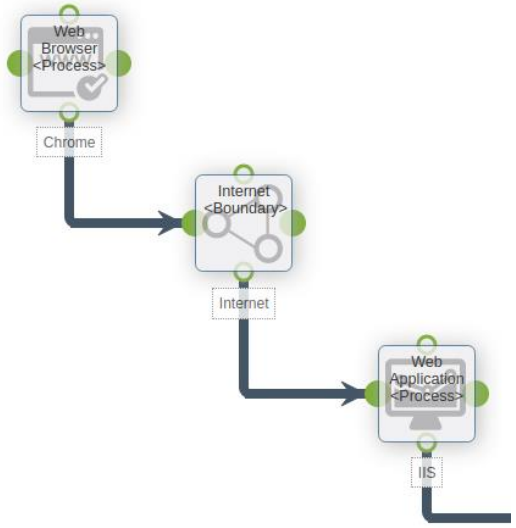
Fuente: Thread Modelling Manifesto

https://www.threatmodelingmanifesto.org/

ascentic/

Threat Modeling: cómo hacerlo

1. Scope: Diagrama de arquitectura
2. Threats STRIDE
   - Spoofing
   - Tampering
   - Repudiation
   - Information disclosure
   - Denial-of-service
   - Elevation privilege
3. Contramedidas o gestión del riesgo
4. Evaluar



Herramientas: Microsoft Thread Modeling Tool

https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling