SEG 118 – Desarrollo Seguro basado en OWASP

Ing. Carlos Carreño

Nov, 2021

MODULO 2: SOBRE EL PROYECTO OWASP

- ¿Qué es OWASP?
- Recursos que ofrece OWASP a la comunidad.
- Vulnerabilidades del Top Ten Owasp.

¿Que es OWASP?

- El Proyecto Abierto de Seguridad en Aplicaciones Web (OWASP por sus siglas en inglés) es una comunidad abierta dedicada a permitir que las organizaciones desarrollen, adquieran y mantengan aplicaciones y APIs en las que se pueda confiar.
- https://youtu.be/GJADjlBbv3Y

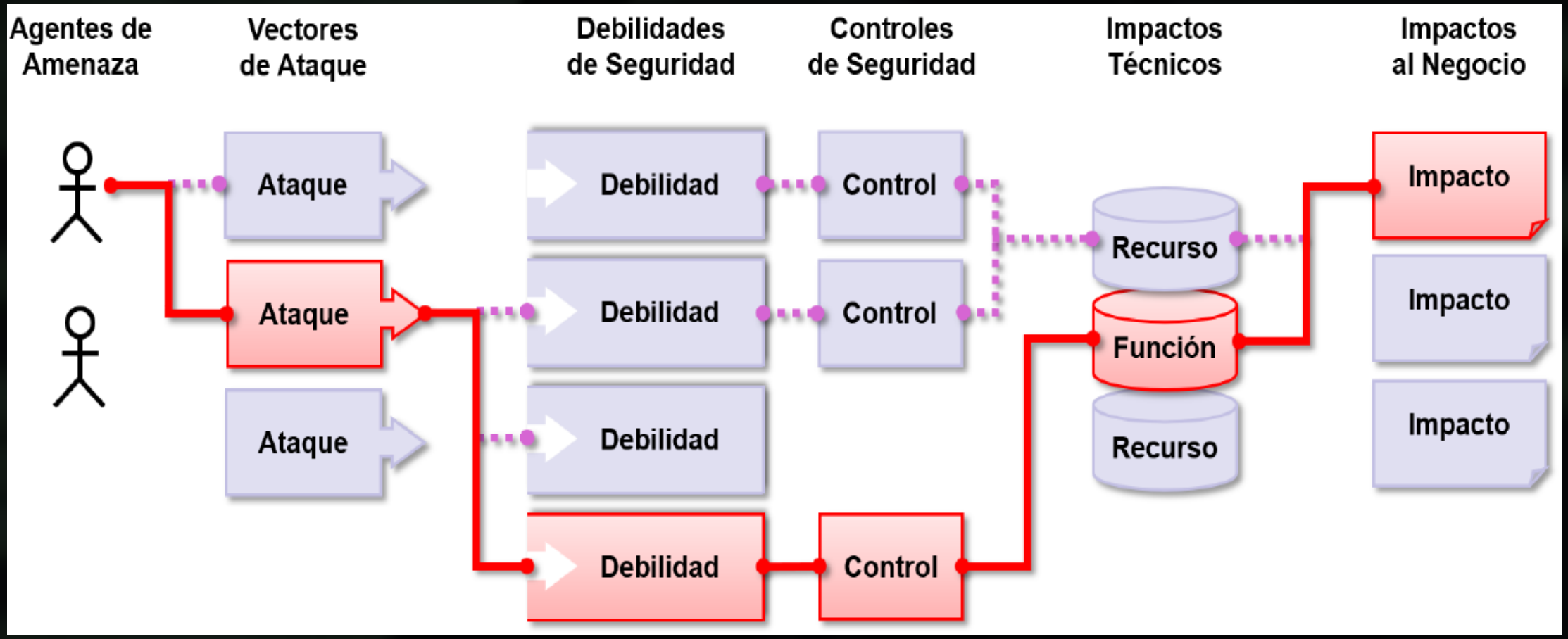
Recursos de OWASP

- Herramientas y estándares de seguridad en aplicaciones.
- Libros completos de revisiones de seguridad en aplicaciones, desarrollo de código fuente seguro y revisiones de seguridad en código fuente
- Presentaciones y videos.
- Hojas de trucos en varios temas comunes.
- Controles de seguridad estándar y bibliotecas.
- Capítulos locales en todo el mundo.
- Investigaciones de vanguardia.
- Numerosas conferencias alrededor del mundo.
- Listas de correo.

Vulnerabilidad y Amenaza

- Una **vulnerabilidad** es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la *integridad*, *disponibilidad* o *confidencialidad* de la misma, por lo que es necesario encontrarlas y eliminarlas lo antes posible.
- una **amenaza** es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento o sobre todo el sistema.

Riesgos en la Seguridad de Aplicaciones



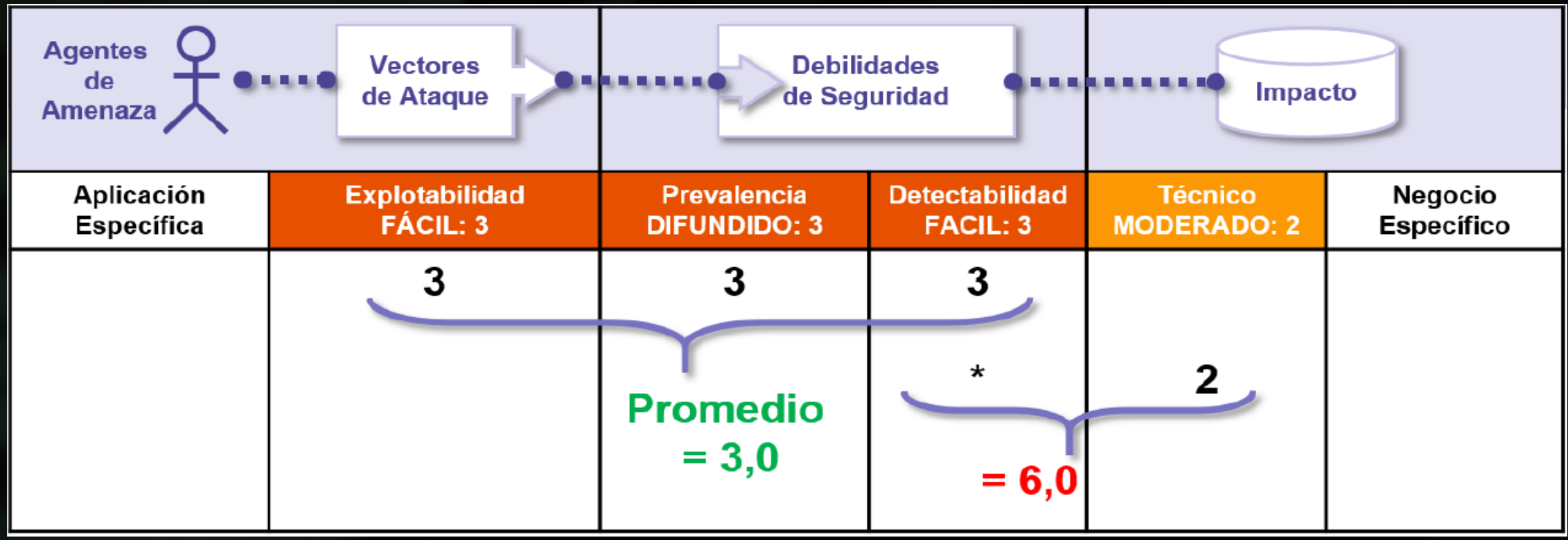
Cual es mi riesgo?

- El riesgo general será el promedio de las probabilidades multiplicado por el valor del impacto técnico.

Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

Ejemplo: Calculo de Riesgo

- Vulnerabilidad → A6:2017 Configuración de Seguridad Incorrecta.



Vulnerabilidades Top Ten según OWASP

- **A1:2017 Inyección**
- **A2:2017 Pérdida de Autenticación**
- **A3:201 Exposición de datos sensibles**
- **A4:2017 Entidades Externas XML (XXE)**
- **A5:2017 Pérdida de Control de Acceso**

Vulnerabilidades Top Ten según OWASP

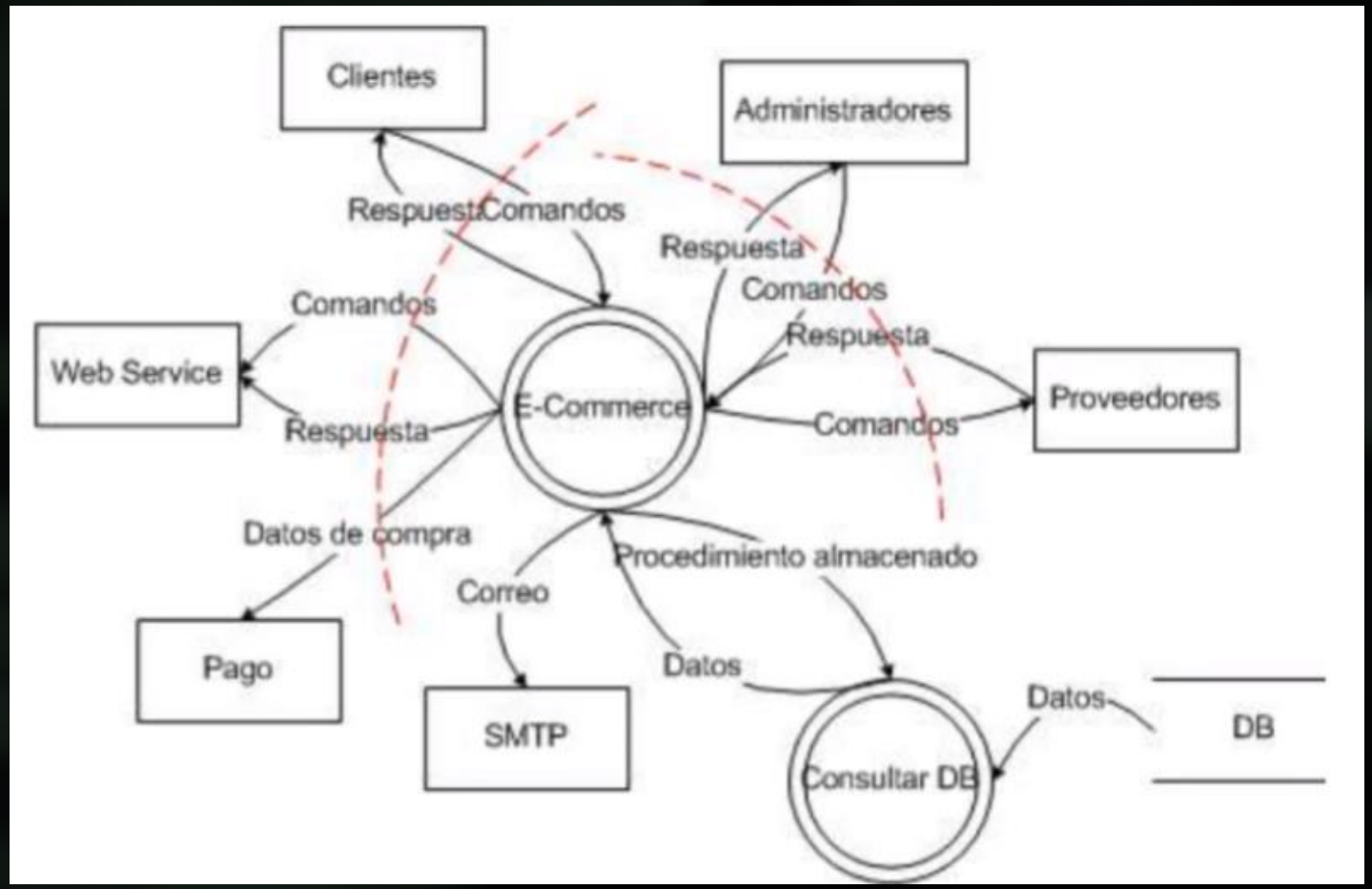
- **A6:2017 Configuración de Seguridad Incorrecta**
- **A7:2017 Secuencia de Comandos en Sitios Cruzados (XSS)**
- **A8:2017 Deserialización Insegura**
- **A9:2017 Componentes con vulnerabilidades conocidas**
- **A10:2017 Registro y Monitoreo Insuficientes**

Modelado de Amenazas

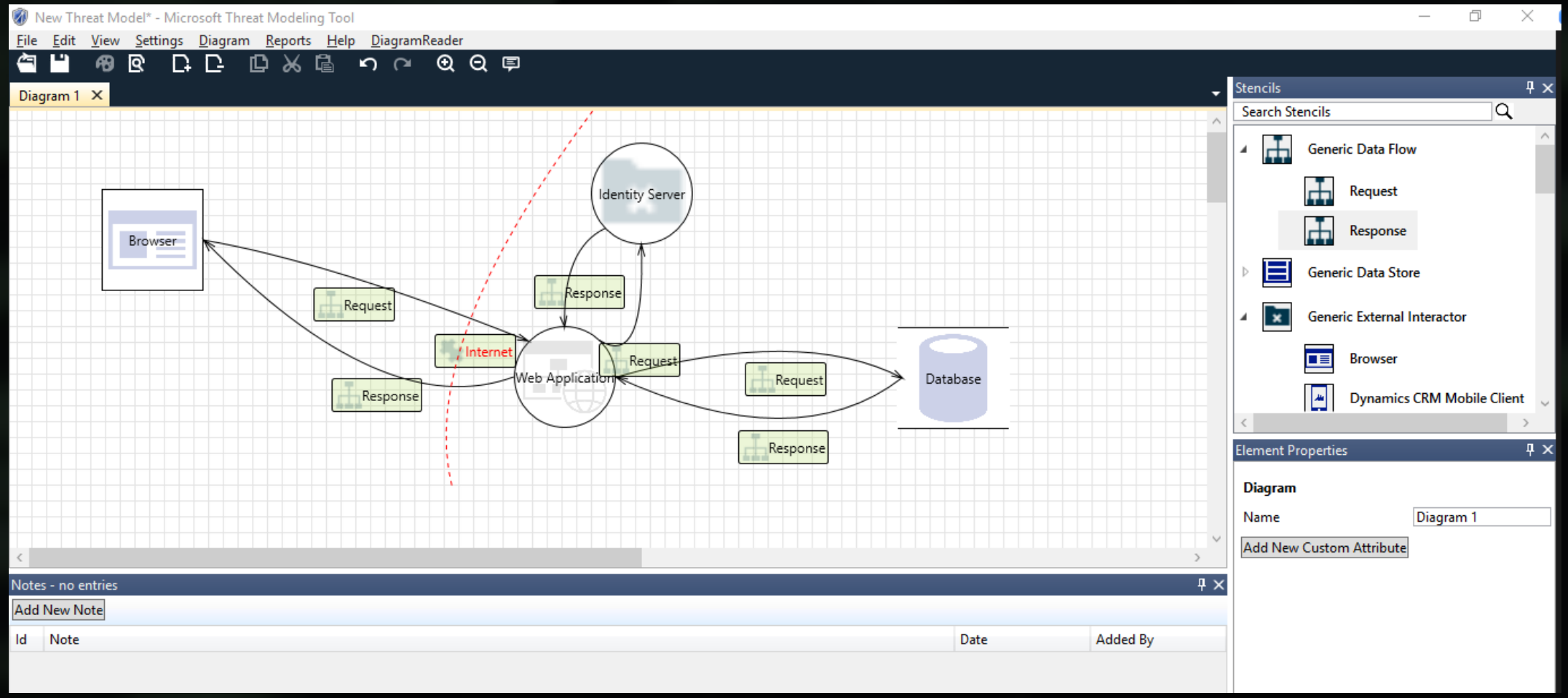
- Un modelo de amenaza generalmente incluye:
  - Descripción del tema a modelar
  - Supuestos que pueden verificarse o cuestionarse en el futuro a medida que cambia el panorama de amenazas
  - Amenazas potenciales al sistema
  - Acciones que se pueden tomar para mitigar cada amenaza
  - Una forma de validar el modelo y las amenazas, y verificar el éxito de las acciones tomadas.

Clasificación de Amenazas

Descomposición de la Aplicación



Microsoft Threat Modeling



Practica

- Realizar la lectura del modelado de amenazas del ejemplo en OWASP “Sitio web de la biblioteca de la universidad”.
- **Entregable**: LAB 2 Realizar el Modelo de Amenazas de una aplicación critica de la empresa usando el modelo MS DREAD y STRIDE crear el diagrama DFD en MS Threat Modeling Tool 2016.

Referencias

- [1] https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian
- [2] https://owasp.org/www-community/Threat_Modeling_Process
- [3] https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling