Secure Software Development Life Cycle

Fast Track

- S-SDLC. Secure Software Development.
- Threat Modeling. Modelado de Amenazas.
- BSIMM6. Bring Security in Maturity Model 6. Midiendo la madurez del SDL.

OWASP

The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Victor Figueroa

- Maestría Universitaria en Seguridad Informática.
Universidad Internacional de la Rioja. Madrid. España.

- Diplomado en Delitos Informáticos.
Universidad Blas Pascal. Córdoba. Argentina.

- Diplomado en Informática Forense.
Uni Colombia. Bogotá. Colombia.

- Licenciado en Informática.
Universidad Blas Pascal. Córdoba. Argentina.

- QMS Implementation & Audit Lead.
Bureau Veritas. IRCA Certified.

- Analista en Computación
Instituto Superior Juan XXIII. Bahía Blanca. Baires. Argentina.

❑ Saturno Hogar S. A.

Jefe de Desarrollo. Gerencia de Sistemas.

Mailto: rvfigueroa@saturno.com.ar
figueroa.rv@gmail.com
Twitter : @FigueroaRV
LinkedIn: https://www.linkedin.com/in/vfigueroa

FORENTICS
Ciencia Forense aplicada a las Tecnologías de Información y Comunicaciones

OWASP
The Open Web Application Security Project

FAST TRACK

- S-SDLC Overview
  - OWASP CLASP
  - Trustworthy Computing
  - Seven Touchpoints
- S-SDLC – Threat Modeling
  - Microsoft Threat Modeling
  - STRIDE
  - DREAD
  - Caso Práctico
- BSIMM6 – Building Security in Maturity Model
  - Midiendo la madurez de nuestro S-SDLC

OWASP
The Open Web Application Security Project

S-SDLC – Secure Software Development Life Cycle

Conjunto de principios de diseño y buenas prácticas a implantar en el SDLC, para ***detectar***, ***prevenir*** *y* ***corregir*** *los defectos de seguridad en el desarrollo y adquisición de aplicaciones, de forma que se obtenga* ***software de confianza y robusto*** *frente a taques maliciosos, que* ***realice solo las funciones para las que fue diseñado****, que esté libre de vulnerabilidades, ya sean intencionalmente diseñadas o accidentalmente insertadas durante su ciclo de vida y se asegure su* ***integridad***, ***disponibilidad*** *y* ***confidencialidad****”.*

OWASP
The Open Web Application Security Project

S-SDLC – Propiedades elementales Software Seguro

- **Integridad**: capacidad que garantiza que el código del software, activos manejados, configuraciones y comportamientos no puedan ser o no hayan sido modificados o alterados.

- **Disponibilidad:** capacidad que garantiza que el software es operativo y accesible por usuarios.

- **Confidencialidad:** capacidad de preservar que cualquiera de sus características, activos manejados, están ocultos a usuarios no autorizados.

S-SDLC – Propiedades Software Seguro

OWASP
The Open Web Application Security Project

S-SDLC – OWASP CLASP

Comprehensive, Lightweight Application Security Process

Modelo prescriptivo, basado en roles y buenas prácticas, que permite a los equipos de Desarrollo implementar seguridad en cada una de las fases del Ciclo de Vida de Desarrollo en forma estructurada, medible y repetible.

Estructura CLASP

- **CLASP View [5]**

Prespectivas de alto nivel, interconectadas entre sí.

- **CLASP Best Practices [7]**

Agrupación de las Activitidades de Seguridad.

- **CLASP Activities [24]**

Diseñadas para permitir una facil integración entre actividades de seguridad y el SDL.

- **CLASP Resources**

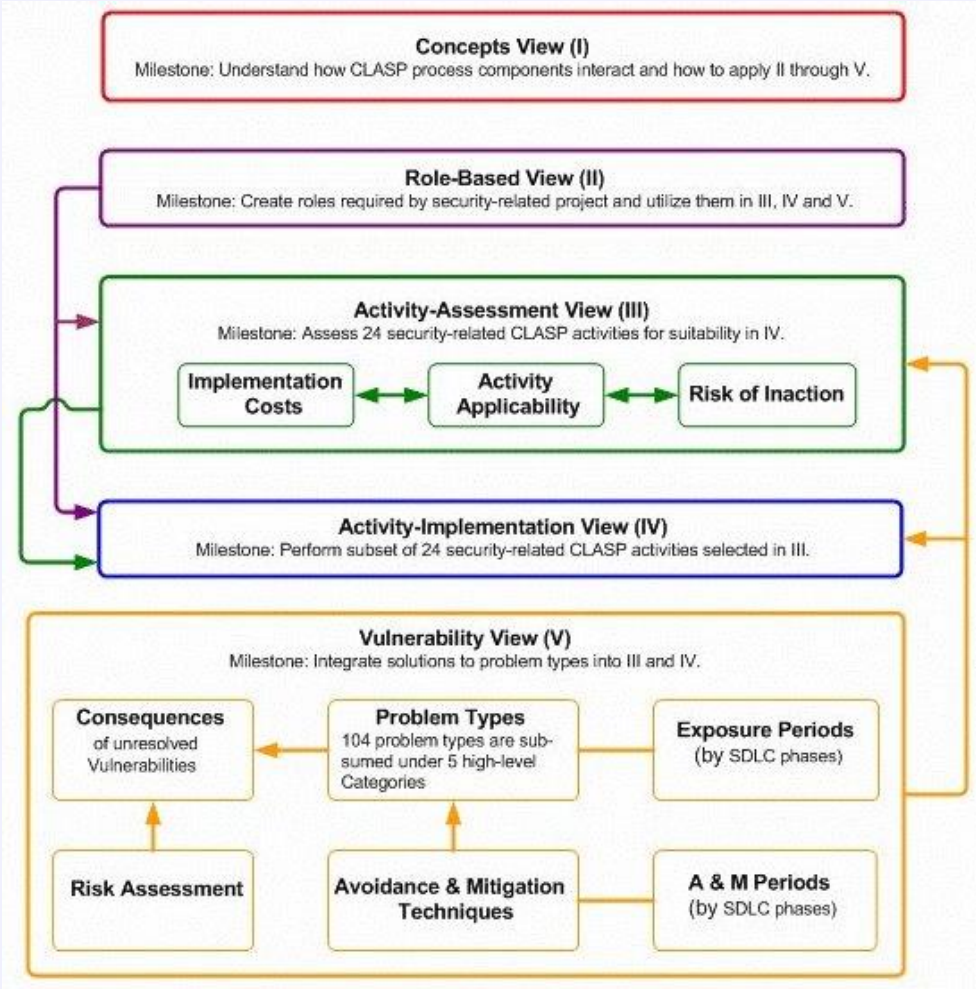
Ayudan a la planificación, ejecución y cumplimiento de las actividades.

- **CLASP Taxonomy**

Clasificación de alto nivel de 104 tipos de problemas o vulnerabilidades, divididos en 5 categorías de alto nivel.

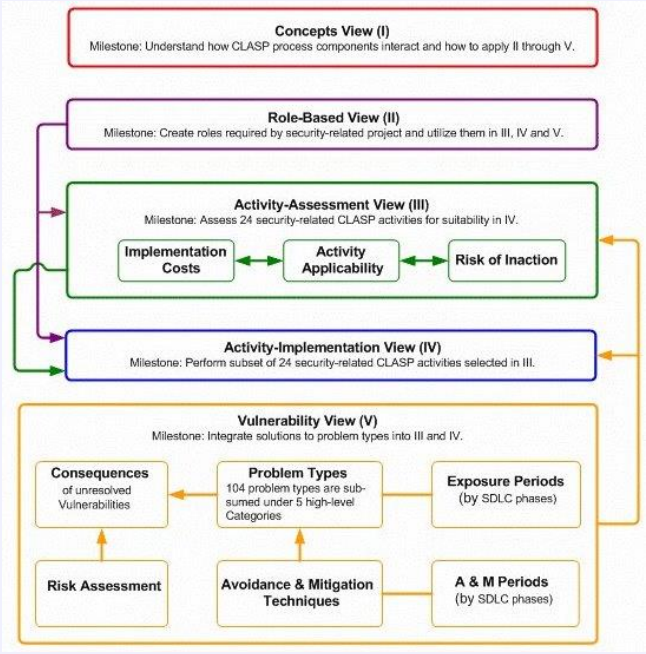
OWASP
The Open Web Application Security Project

S-SDLC – OWASP CLASP



CLASP Best Practices	CLASP Activities	Related Project Roles
1. Institute awareness programs	Institute security awareness program	Project manager
2. Perform application assessments	Perform security analysis of system requirements and design (threat modeling)	Security auditor
	Perform source-level security review	Owner: security auditor Key contributor: implementer, designer
	Identify, implement, and perform security tests	Test analyst
	Verify security attributes of resources	Tester
	Research and assess security posture of technology solutions	Owner: designer Key contributor: component vendor
3. Capture security requirements	Identify global security policy	Requirements specifier
	Identify resources and trust boundaries	Owner: architect Key contributor: requirements specifier
	Identify user roles and resource capabilities	Owner: architect Key contributor: requirements specifier
	Specify operational environment	Owner: requirements specifier Key contributor: architect
	Detail misuse cases	Owner: requirements specifier Key contributor: stakeholder
	Identify attack surface	Designer
	Document security-relevant requirements	Owner: requirements specifier Key contributor: architect
4. Implement secure development practices	Apply security principles to design	Designer
	Annotate class designs with security properties	Designer
	Implement and elaborate resource policies and security technologies	Implementer
	Implement interface contracts	Implementer
	Integrate security analysis into source management	Integrator
	Perform code signing	Integrator
5. Build vulnerability remediation procedures	Manage security issue disclosure process	Owner: project manager Key contributor: designer
	Address reported security issues	Owner: designer Fault reporter
6. Define and monitor metrics	Monitor security metrics	Project manager
7. Publish operational security guidelines	Specify database security configuration	Database designer
	Build operational security guide	Owner: integrator Key contributor: designer, architect, implementer

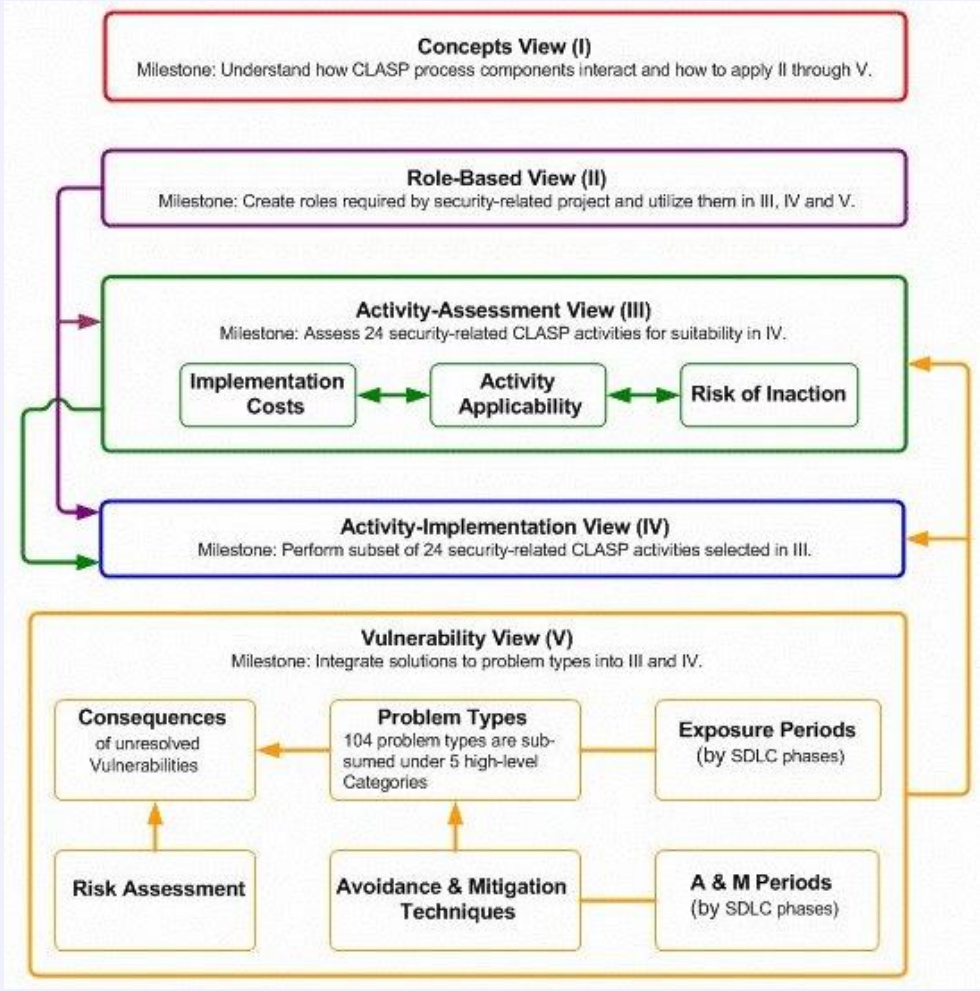
S-SDLC – OWASP CLASP

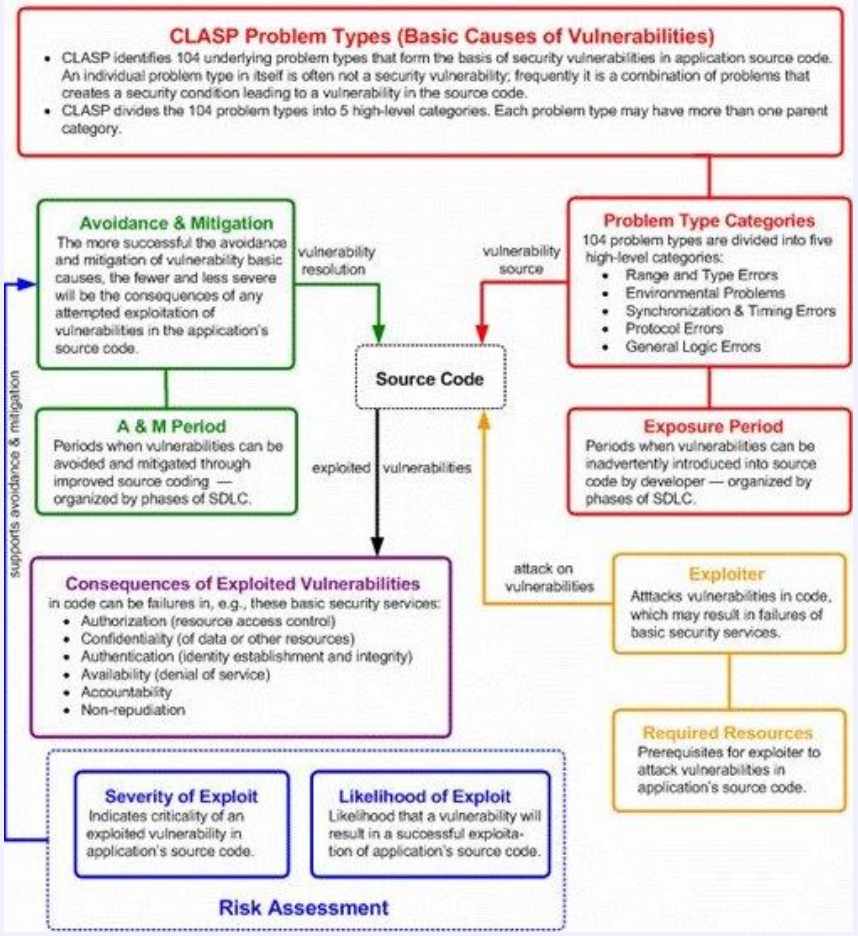


CLASP Best Practices	CLASP Activities	Related Project Roles
1. Institute awareness programs	Institute security awareness program	Project manager
2. Perform application assessments	Perform security analysis of system requirements and design (threat modeling)	Security auditor
	Perform source-level security review	Owner: security auditor Key contributor: implementer, designer
	Identify, implement, and perform security tests	Test analyst
	Verify security attributes of resources	Tester
	Research and assess security posture of technology solutions	Owner: designer Key contributor: component vendor
3. Capture security requirements	Identify global security policy	Requirements specifier
	Identify resources and trust boundaries	Owner: architect Key contributor: requirements specifier
	Identify user roles and resource capabilities	Owner: architect Key contributor: requirements specifier
	Specify operational environment	Owner: requirements specifier Key contributor: architect
	Detail misuse cases	Owner: requirements specifier Key contributor: stakeholder
	Identify attack surface	Designer
	Document security-relevant requirements	Owner: requirements specifier Key contributor: architect
4. Implement secure development practices	Apply security principles to design	Designer
	Annotate class designs with security properties	Designer
	Implement and elaborate resource policies and security technologies	Implementer
	Implement interface contracts	Implementer
	Integrate security analysis into source management	Integrator
	Perform code signing	Integrator
5. Build vulnerability remediation procedures	Manage security issue disclosure process	Owner: project manager Key contributor: designer
	Address reported security issues	Owner: designer Fault reporter
6. Define and monitor metrics	Monitor security metrics	Project manager
7. Publish operational security guidelines	Specify database security configuration	Database designer
	Build operational security guide	Owner: integrator Key contributor: designer, architect, implementer

OWASP
The Open Web Application Security Project

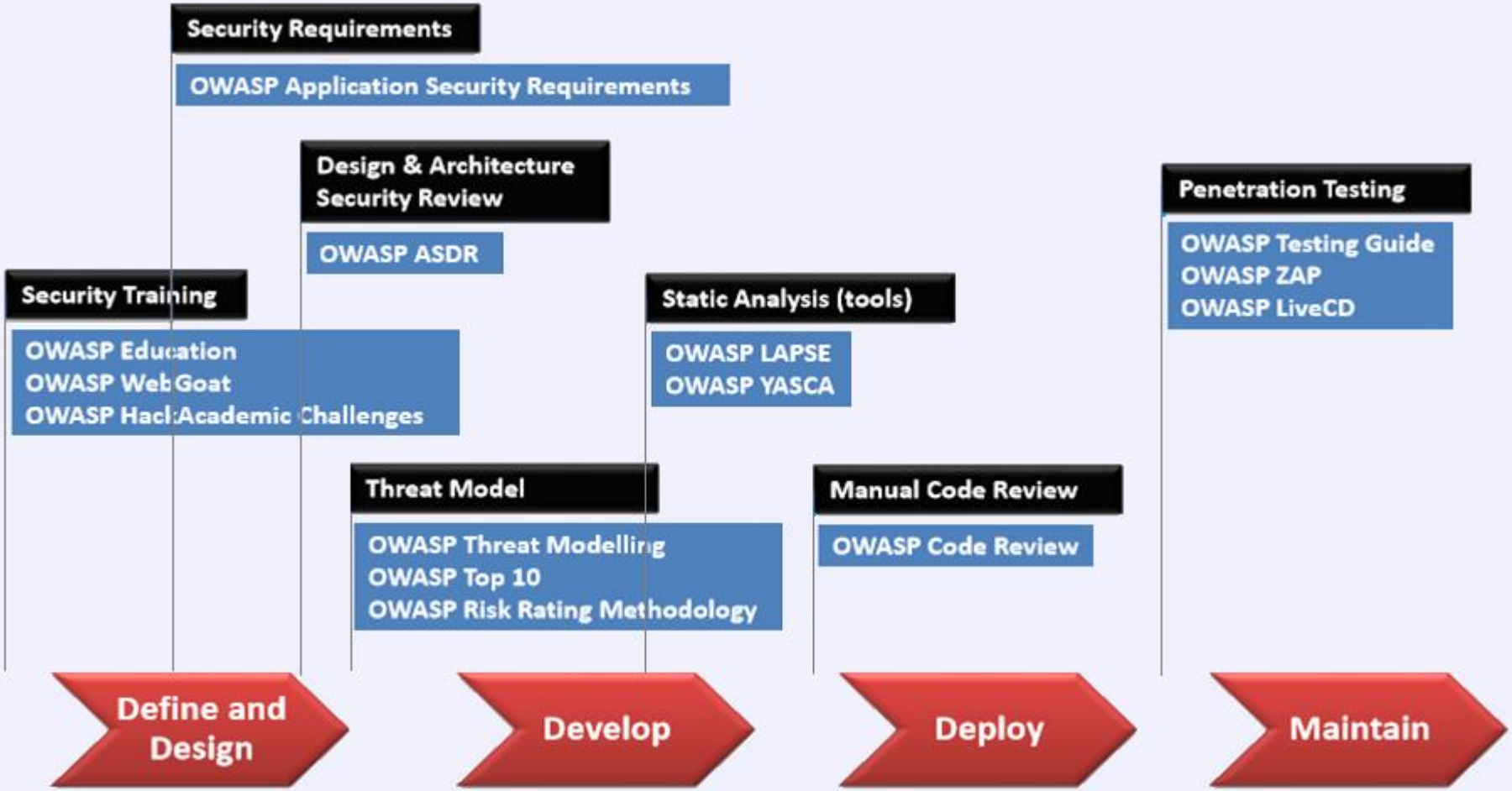
S-SDLC – OWASP CLASP





OWASP
The Open Web Application Security Project

S-SDLC – OWASP CLASP



S-SDLC – Trustworthy Computing SDL

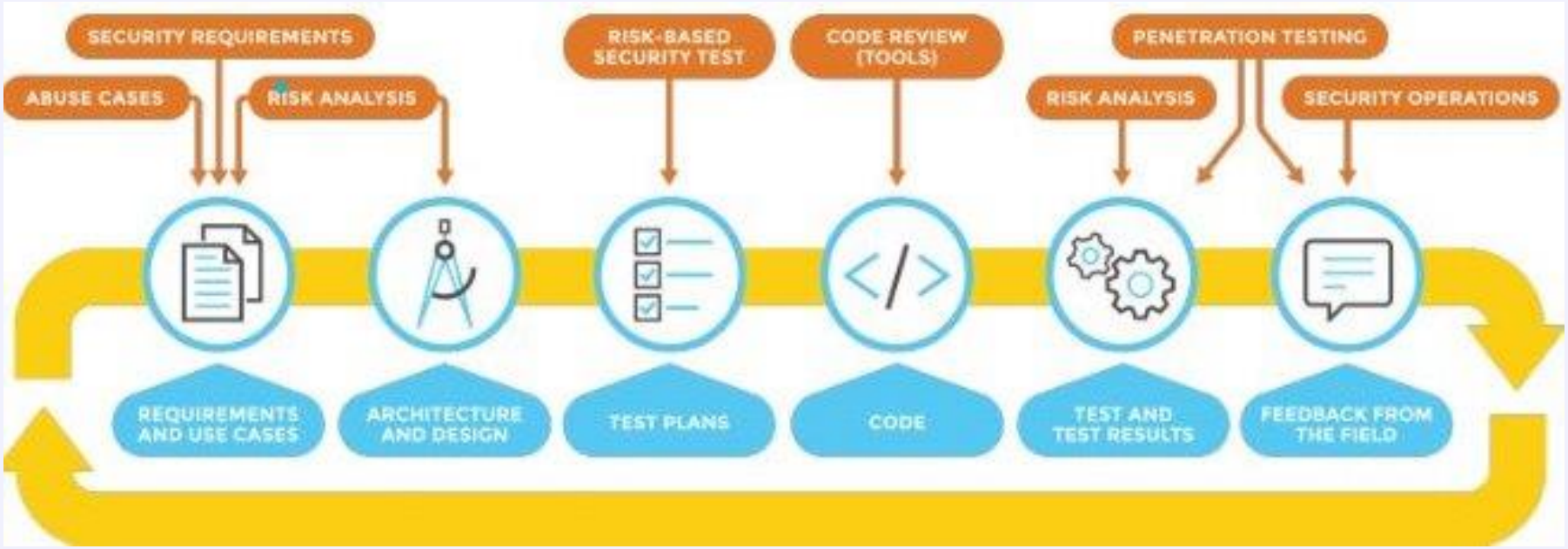
"Trustworthy Computing is computing that is as available, reliable and secure as electricity, water services and telephony." Bill Gates, 2002.

Training	Requirements	Design	Implementation	Verification	Release	Response
1. Core Security Training	2. Establish Security Requirements 3. Create Quality Gates/Bug Bars 4. Perform Security and Privacy Risk Assessments	5. Establish Design Requirements 6. Perform Attack Surface Analysis/ Reduction 7. Use Threat Modeling	8. Use Approved Tools 9. Deprecate Unsafe Functions 10. Perform Static Analysis	11. Perform Dynamic Analysis 12. Perform Fuzz Testing 13. Conduct Attack Surface Review	14. Create an Incident Response Plan 15. Conduct Final Security Review 16. Certify Release and Archive	Execute Incident Response Plan

OWASP
The Open Web Application Security Project

S-SDLC – Seven Touchpoints

"Conjunto de buenas prácticas de seguridad que pueden ser aplicadas sobre los artefactos de software durante la fase de Desarrollo". Gary McGraw, Cigital.



S-SDLC – Threat Modeling

Amenaza

"Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización."

ISO/IEC 27000:2014

Vulnerabilidad

"Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. "

Magerit:2012

Riesgo

"El riesgo de seguridad de la información se relaciona con la posibilidad de que las amenazas exploten vulnerabilidades de un activo o grupo de activos de información y causen daño a una organización."

ISO/IEC 27000:2014

CCN STIC 401 Glosario de Seguridad

OWASP
The Open Web Application Security Project

S-SDLC – Threat Modeling

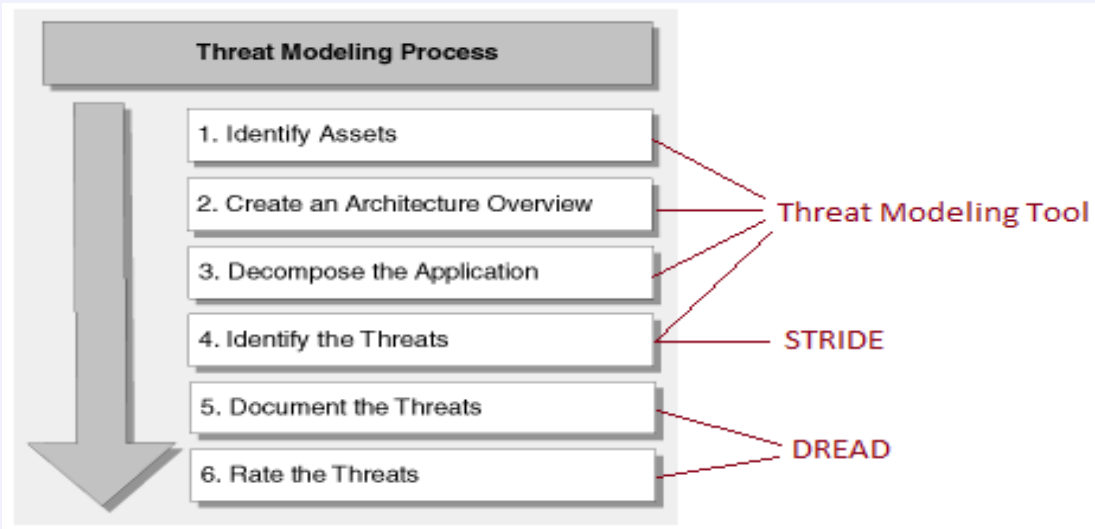
El Modelado de Amenazas, como metodología y práctica de Ingeniería de Software, se introduce dentro del S-SDLC, constituyendo un framework específico para el proceso de análisis de riesgo estructurado, que permite **identificar las amenazas** de una aplicación, **cuantificar los riesgos** a los que la misma estará expuesta, y definir **contramedidas de mitigación**.

Permite contar, desde las etapas iniciales del desarrollo, con una visión de la seguridad que alcanza todo el ciclo de vida, a través de la evaluación de riesgos y la determinación de contramedidas.

El objetivo del modelado de amenazas es **asegurar las propiedades** esenciales de Integridad, Disponibilidad y Confidencialidad que constituyen un **Software Seguro**.

S-SDLC – Microsoft Threat Modeling

Es una metodología fomentada por Microsoft y soportada con su herramienta Microsoft Threat Modeling Tool, ***disponible de forma gratuita****. Es reconocida como una de las mejores metodologías para esta tarea dada su simpleza y claridad de los conceptos involucrados.*



S-SDLC – Microsoft Threat Modeling

STRIDE: Metodología de identificación de **Amenazas**. Su nombre surge de la abreviatura de las categorías de Amenazas que caracteriza.

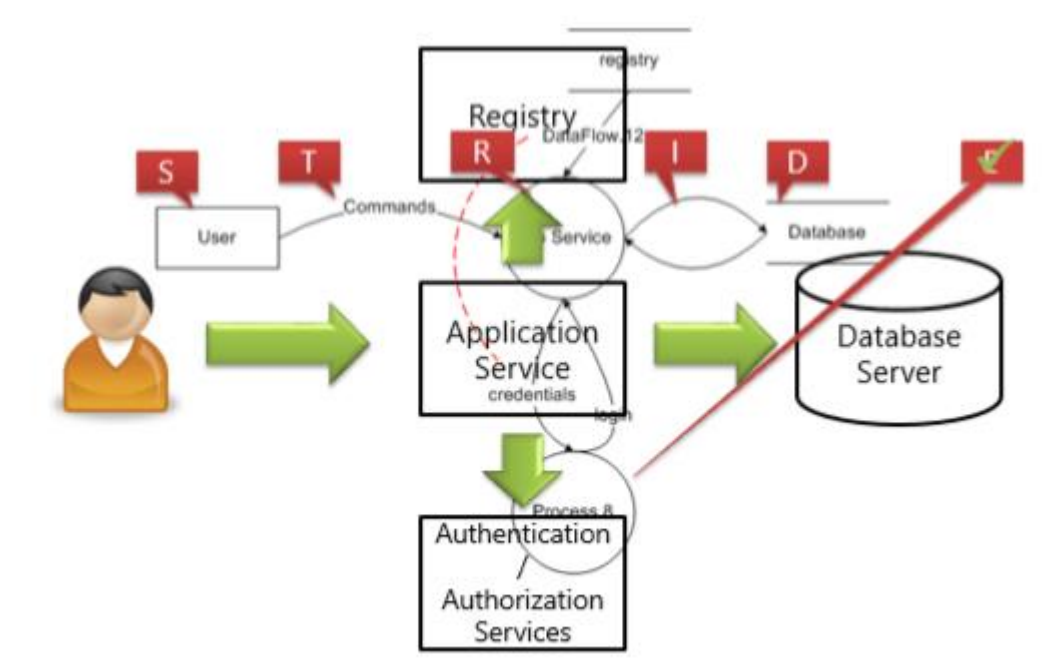
Se aplica sobre cada uno de los objetos del diagrama de flujo de datos, para especificar la amenaza a la que éste se encuentra expuesto.

Desired Property	Threat	Definition
Authentication	Spoofing	Impersonating something or someone else
Integrity	Tampering	Modifying code or data without authorization
Non-repudiation	Repudiation	The ability to claim to have not performed some action against an application
Confidentiality	Information Disclosure	The exposure of information to unauthorized users
Availability	Denial of Service	The ability to deny or degrade a service to legitimate users
Authorization	Elevation of Privilege	The ability of a user to elevate their privileges with an application without authorization

S-SDLC – Microsoft Threat Modeling

STRIDE: Metodología de identificación de **Amenazas**. Su nombre surge de la abreviatura de las categorías de Amenazas que caracteriza.

Se aplica sobre cada uno de los objetos del diagrama de flujo de datos, para especificar la amenaza a la que éste se encuentra expuesto.



S-SDLC – Microsoft Threat Modeling

DREAD: Metodología que permite puntuar la probabilidad que tiene una amenaza de materializarse. Esto permite priorizar la definición de contramedidas para mitigar las amenaza, dado que el riesgo se puede cuantificar como el resultado de multiplicar la probabilidad de que la amenaza se produzca, por el daño potencial de esta, presenta la siguiente ecuación.

Riesgo = Probabilidad * Daño Potencial

Luego:

Riesgo_DREAD = (Damage + Reproductibility + Exploitability + Afected Users + Discoverability) / 5

Este enfoque, si bien, un poco simplista, permite de forma simple clasificar las amenazas en una escala entre 1-100 que podemos dividir en tres niveles según su riesgo: Alto, Medio, Bajo.

S-SDLC – Microsoft Threat Modeling

DREAD

Damage Potential	Daño Potencial	Si una amenaza fuese explotada, ¿Cuánto daño causaría? 0 = Nada 5 = Datos de los usuarios individuales comprometidos o afectados. 10 = Destrucción de datos del sistema completo
Reproducibility	Grado de Reproducibilidad	¿Es fácil de reproducir la amenaza a explotar? 0 = Muy difícil o imposible, incluso para los administradores de la aplicación. 5 = Uno o dos pasos necesarios, puede ser necesario un usuario autorizado. 10 = Sólo un navegador web y la barra de direcciones es suficiente, sin necesidad de autenticación.
Exploitability	Grado de Explotabilidad	Lo que se necesita para aprovechar esta amenaza. 0 = Conocimientos avanzados de programación y de redes, con herramientas de ataque personalizadas o avanzadas. 5 = Malware existente en el Internet, o un exploit fácil de realizar con las herramientas disponibles en la web. 10 = Sólo un navegador web.
Affected users	Usuarios afectados	¿Cuántos usuarios se verán afectados? 0 = Ninguno 5 = Algunos usuarios, pero no todos. 10 = Todos los usuarios. En esta categoría se aplica matemáticamente un punto por cada 10% de posibles usuarios afectados.
Discoverability	Detectabilidad	¿Es fácil descubrir esta amenaza? 0 = Muy difícil o imposible, requiere el código fuente o acceso administrativo. 5 = ¿Se puede averiguar de adivinar o mediante el control de trazas de red? 9 = Detalles de fallas de este tipo son ya de dominio público y puede ser fácilmente descubierto usando un motor de búsqueda.

S-SDLC – Microsoft Threat Modeling

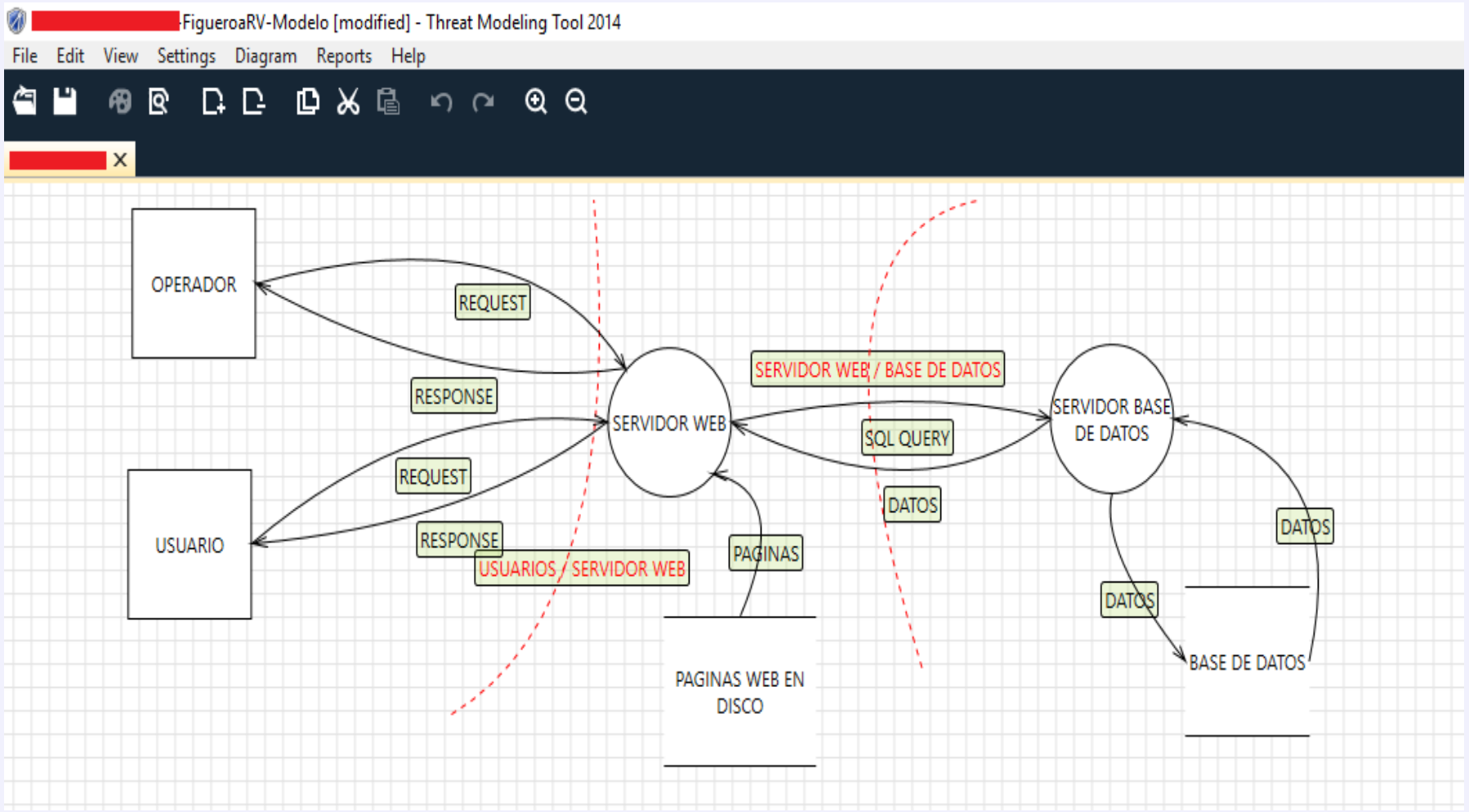
DREAD

Categoría Amenaza STRIDE	Amenaza Descripción	Contexto / Objeto	D	R	E	A	D	Riesgo DREAD
Denegación de Servicio	Data Flow RESPONSE Is Potentially Interrupted	Usuario y Servidor web	5	10	0	10	10	7
Divulgación de Información	Weak Authentication Scheme	Servidor web y Servidor db	5	5	0	10	10	6
Denegación de Servicio	Potential Excessive Resource Consumption for SERVIDOR BASE DE DATOS or BASE DE DATOS	Servidor db y archivos físicos	5	0	0	10	9	4,8
Tampering	Potential SQL Injection Vulnerability for BASE DE DATOS	Servidor db y archivos físicos	5	5	5	10	9	6,8
Suplantación	Spoofing of Destination Data Store BASE DE DATOS	Servidor db y archivos físicos	5	5	0	10	5	5
Divulgación de Información	Weak Access Control for a Resource	Servidor db y archivos físicos	5	5	0	10	5	5
Suplantación	Spoofing of Source Data Store BASE DE DATOS	Servidor db y archivos físicos	10	0	0	10	9	5,8

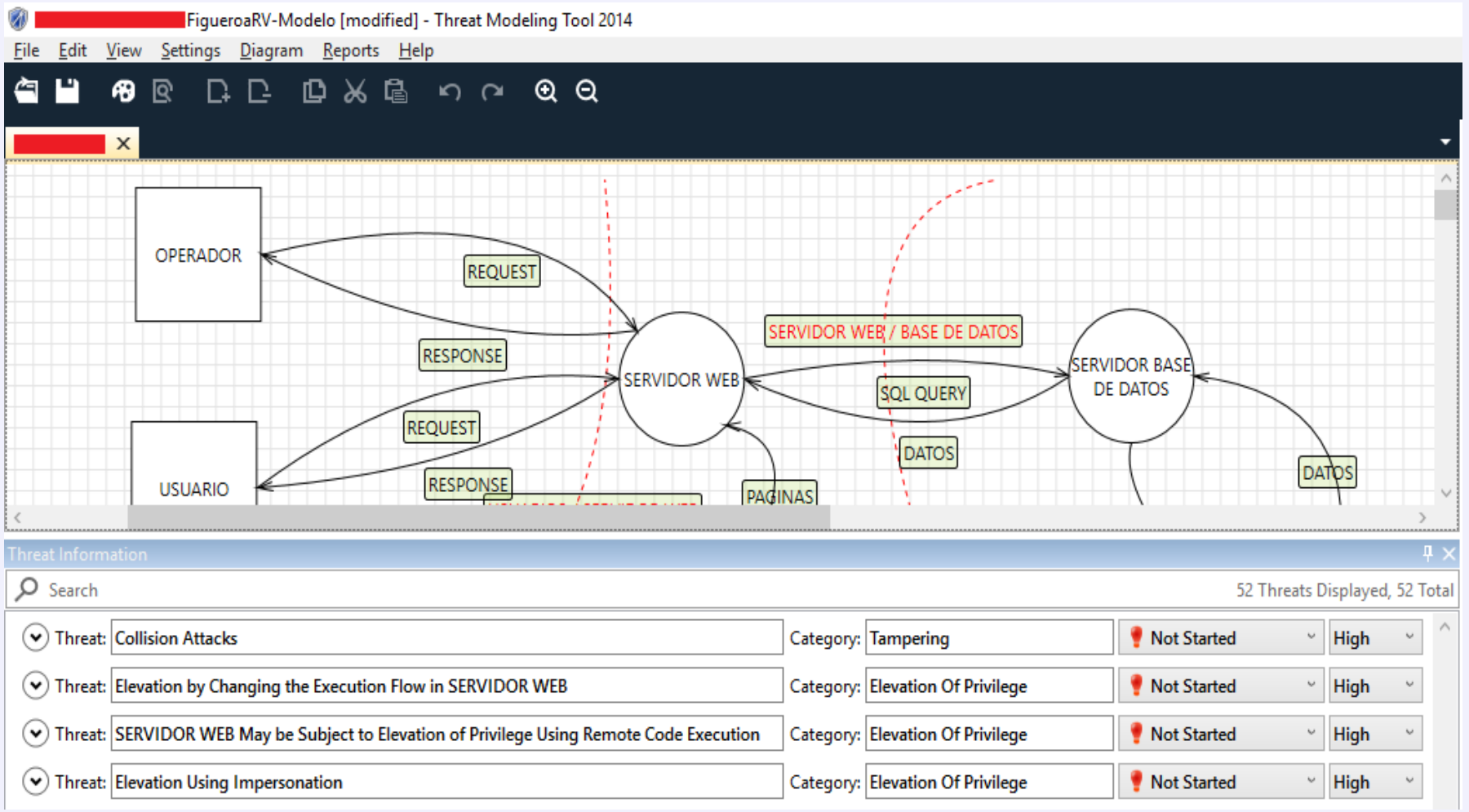
Categoría Amenaza STRIDE	Amenaza Descripción	Contexto / Objeto	Riesgo DREAD	Nivel Riesgo
Denegación de Servicio	Potential Process Crash or Stop for SERVIDOR WEB	Servidor web y Servidor db	7,8	Alto
Denegación de Servicio	Data Flow RESPONSE Is Potentially Interrupted	Usuario y Servidor web	7	Alto
Denegación de Servicio	Potential Process Crash or Stop for SERVIDOR BASE DE DATOS	Servidor web y Servidor db	7	Alto

OWASP
The Open Web Application Security Project

S-SDLC – Microsoft Threat Modeling. Caso Práctico.

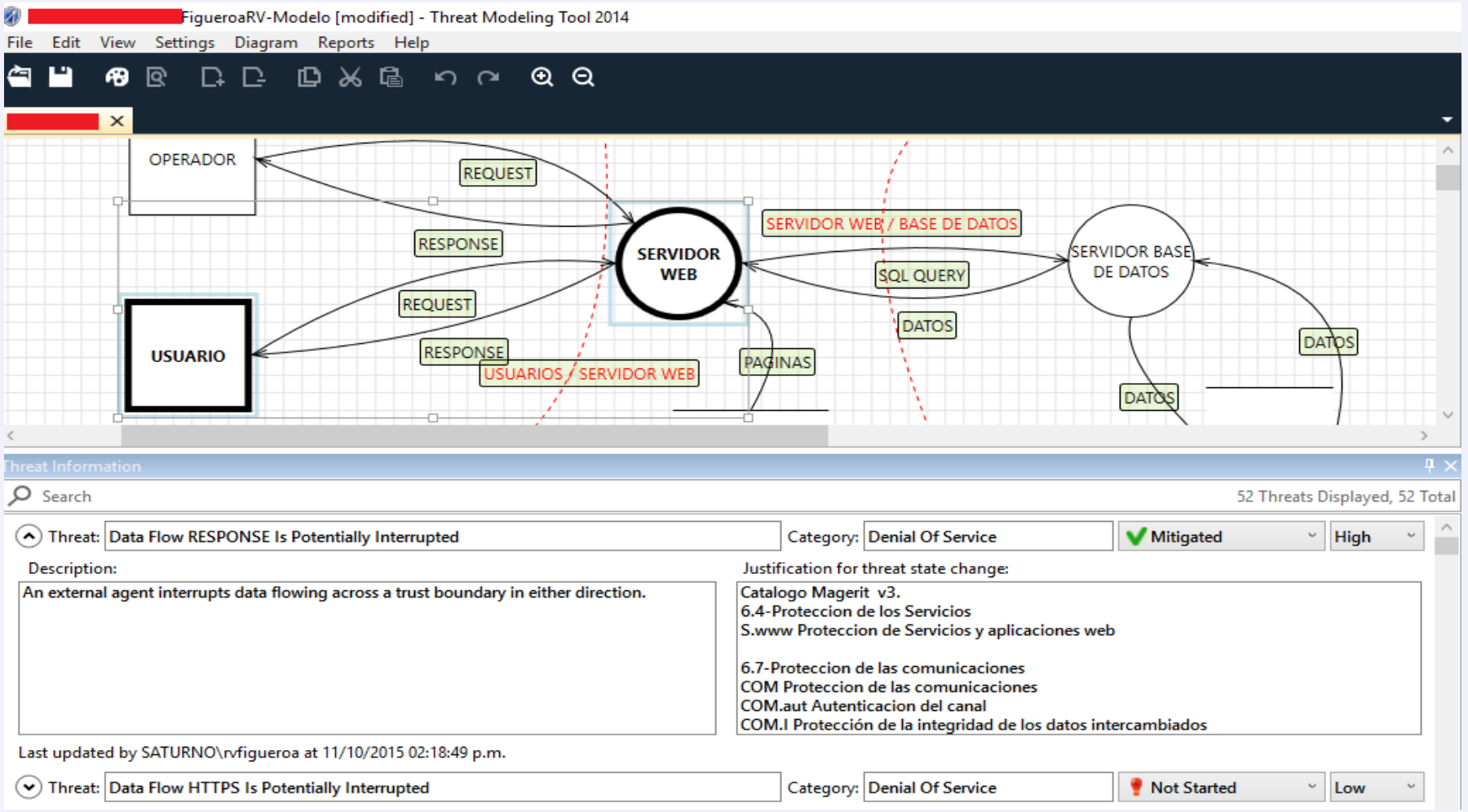


S-SDLC – Microsoft Threat Modeling. Caso Práctico.



OWASP
The Open Web Application Security Project

S-SDLC – Microsoft Threat Modeling. Caso Práctico.



OWASP
The Open Web Application Security Project

BSIMM6. Build Security in Maturity Model. Overview.

"Is not about how to eat bananas…"

Es un estudio de iniciativas existentes de Seguridad del Software.

Al cuantificar las prácticas de muchas organizaciones diferentes, se puede describir la base común compartida por varias de ellas, así como la variación que hace que cada una sea única.

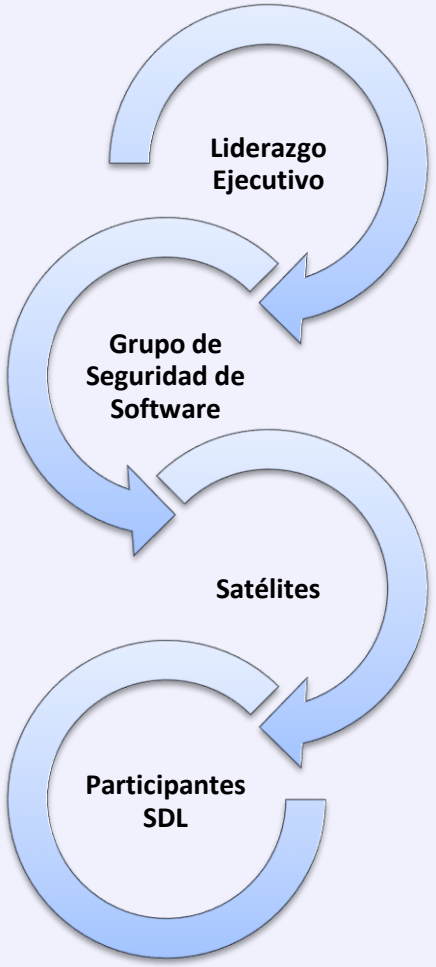
El objetivo es ayudar a la vasta comunidad de seguridad del software a planificar, llevar a cabo y medir sus propias iniciativas.

BSIMM no es una guía de los "cómo", ni una prescripción aplicable a todos. BSIMM es, en cambio, un reflejo de lo más avanzado en Seguridad del Software.

OWASP
The Open Web Application Security Project

BSIMM6. Build Security in Maturity Model. Overview.

Modelo de Referencia para la Seguridad del Software (MRSS)			
Gobernanza	**Inteligencia**	**Puntos de Contacto con el SSDL**	**Despliegue**
Estrategia y Métricas	Modelos de Ataque	Análisis de la Arquitectura	Pruebas de Penetración
Cumplimiento y Política	Características de Seguridad y Diseño	Revisión de Código	Entorno del Software
Capacitación	Normas y Requisitos	Pruebas de Seguridad	Gestión de Configuración y Gestión de Vulnerabilidades



OWASP
The Open Web Application Security Project

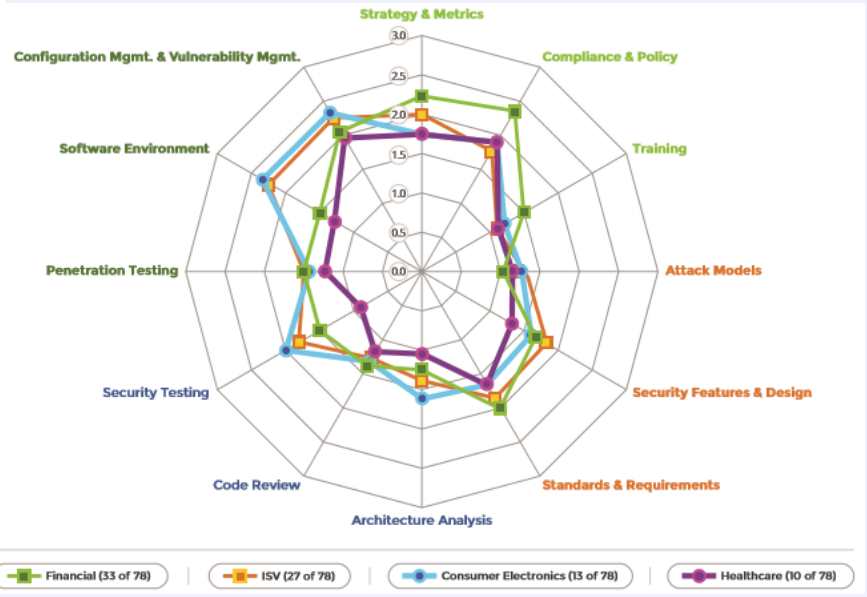
BSIMM6. Build Security in Maturity Model. Overview.

GOVERNANCE			INTELLIGENCE			SSDL TOUCHPOINTS			DEPLOYMENT		
ACTIVITY	BSIMM6 FIRMS	FIRM	ACTIVITY	BSIMM6 FIRMS	FIRM	ACTIVITY	BSIMM6 FIRMS	FIRM	ACTIVITY	BSIMM6 FIRMS	FIRM
STRATEGY & METRICS			ATTACK MODELS			ARCHITECTURE ANALYSIS			PENETRATION TESTING		
[SM1.1]	41	1	[AM1.1]	17	1	[AA1.1]	67	1	[PT1.1]	69	1
[SM1.2]	40		[AM1.2]	51		[AA1.2]	29	1	[PT1.2]	47	1
[SM1.3]	36	1	[AM1.3]	31		[AA1.3]	22	1	[PT1.3]	47	
[SM1.4]	66	1	[AM1.4]	8	1	[AA1.4]	46		[PT2.2]	20	1
[SM2.1]	36		[AM1.5]	46	1	[AA2.1]	12		[PT2.3]	17	
[SM2.2]	29		[AM1.6]	11		[AA2.2]	9	1	[PT3.1]	10	1
[SM2.3]	30		[AM2.1]	6		[AA2.3]	13		[PT3.2]	8	
[SM2.5]	17		[AM2.2]	8	1	[AA3.1]	6				
[SM2.6]	29		[AM3.1]	4		[AA3.2]	1				
[SM3.1]	15		[AM3.2]	2							
[SM3.2]	7										
COMPLIANCE & POLICY			SECURITY FEATURES & DESIGN			CODE REVIEW			SOFTWARE ENVIRONMENT		
[CP1.1]	45	1	[SFD1.1]	61		[CR1.1]	18		[SE1.1]	37	
[CP1.2]	61		[SFD1.2]	59	1	[CR1.2]	53	1	[SE1.2]	69	1
[CP1.3]	41	1	[SFD2.1]	24		[CR1.4]	55	1	[SE2.2]	31	1
[CP2.1]	19		[SFD2.2]	39		[CR1.5]	24		[SE2.4]	25	
[CP2.2]	23		[SFD3.1]	8		[CR1.6]	27	1	[SE3.2]	10	

LEGEND:		
	ACTIVITY	112 BSIMM6 activities, shown in 4 domains and 12 practices
	BSIMM6 FIRMS	count of firms (out of 78) observed performing each activity
		most common activity within a practice
		most common activity not observed in this assessment
	1	most common activity was observed in this assessment
		a practice where firm's high-water mark score is below the BSIMM6 average

OWASP
The Open Web Application Security Project

BSIMM6. Build Security in Maturity Model. Overview.



OWASP
The Open Web Application Security Project

Bibliografía Recomendada

OWASP CLASP
https://www.owasp.org/index.php/Category:OWASP_CLASP_Project/es

Microsoft Trustworthy Computing SDL
https://msdn.microsoft.com/en-us/library/ff648644.aspx
http://www.wired.com/2002/01/bill-gates-trustworthy-computing/

SDL Touchpoints
https://www.cigital.com/blog/what-is-the-secure-software-development-lifecycle/

OWASP CLASP vs Microsoft SDL vs SDL TouchPoints
https://lirias.kuleuven.be/bitstream/123456789/242084/1/comparison.pdf

S-SDLC vs Desarrollo Agil, un desafío…
https://buildsecurityin.us-cert.gov/articles/knowledge/sdlc-process/secure-software-development-life-cycle-processes

Microsoft Threat Modeling
https://www.microsoft.com/en-us/sdl/adopt/threatmodeling.aspx
https://www.owasp.org/index.php/Threat_Risk_Modeling

P.A.S.T.A. (Process for Attack Simulation and Threat Analysis)
http://myappsecurity.com/comparison-threat-modeling-methodologies/

Ministerio de Justicia – Dir. Nacional de Protección de Datos Personales – Guía de Buenas Prácticas para el Desarrollo de Aplicaciones
http://www.jus.gob.ar/media/3075908/guiabpsoftware.pdf

Cigital BSIMM
Official Site: https://www.cigital.com
BSIMM-V Versión Español http://www.fundacionsadosky.org.ar/wp-content/uploads/2014/07/BSIMM-V-esp.pdf
BSIMM 6 https://www.cigital.com/services/software-security-strategy/bsimm-assessment/

OWASP
The Open Web Application Security Project

S-SDLC – Threat Modeling - BSIMM

Dudas, consultas…

OWASP
The Open Web Application Security Project

S-SDLC – Threat Modeling - BSIMM

¡Muchas gracias!