ANÁLISIS DE RIESGOS APLICANDO LA METODOLOGÍA OWASP

OWASP
The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

- Alvaro Machaca Tola
- Experiencia laboral en áreas de seguridad de la información, seguridad informática y auditoria de sistemas en entidades financieras, bolsa de valores y empresas de medios de pago electrónico.
- CCNA | CEH | ISO 27001 Internal Auditor.
- Actualmente consultor experimentado en la firma global Ernst & Young (EY).

- alvaro_machaca@hotmail.com
- alvaro.machaca@bo.ey.com
- https://bo.linkedin.com/pub/alvaro-machaca-tola/42/85b/7

OWASP
The Open Web Application Security Project

¿Dónde se encuentra el Riesgo?

OWASP
The Open Web Application Security Project

Riesgos en la Empresa

OWASP
The Open Web Application Security Project

Riesgo Tecnológico

Es la **probabilidad de sufrir pérdidas por caídas** o fallos en los sistemas informáticos o transmisión de datos, errores de programación u otros, siendo un componente del riesgo operativo.

Fuente: ASFI 207/13 – Dic/2013 Directrices Básicas para la Gestión del Riesgo Operativo

OWASP
The Open Web Application Security Project

Riesgos Materializados

OWASP
The Open Web Application Security Project

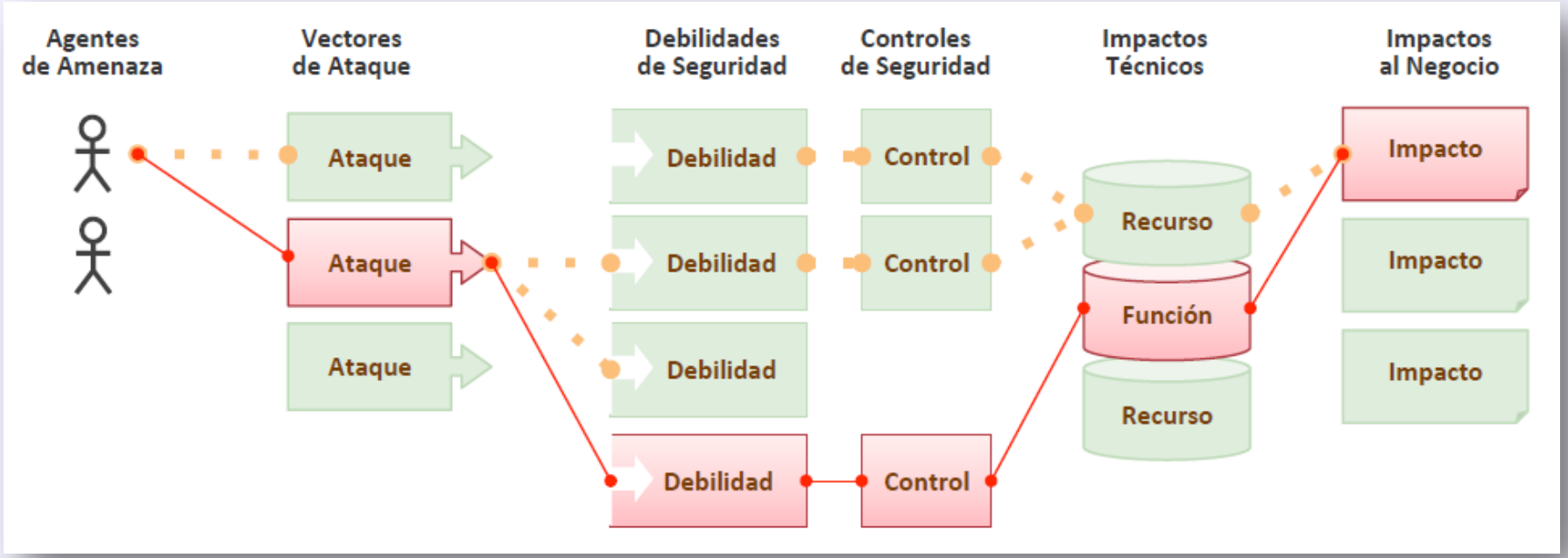
Riesgos en Aplicaciones

Los atacantes pueden usar potencialmente rutas diferentes a través de la aplicación para hacer daño al negocio u organización, estas rutas representan un riesgo que puede, o no, ser lo suficientemente grave como para justificar la atención.

Fuente: OWASP Top 10

OWASP
The Open Web Application Security Project

Representación del Riesgo



Fuente: OWASP Top 10 - 2013

OWASP
The Open Web Application Security Project

OWASP Risk Rating Methodology

Para valorar el riesgo, se deben tomar en cuenta los siguientes aspectos:

- **Una vulnerabilidad critica para un tipo de negocio no lo es necesariamente para otro negocio.**
- **Existen metodologías y estándares internacionales para la gestión de riesgos las cuales deben adaptarse al negocio.**

OWASP
The Open Web Application Security Project

Identificar el Riesgo

El primer paso es identificar un riesgo de seguridad que necesita ser tratado:

- Identificar agentes de amenaza.
- Identificar vulnerabilidades que pueden ser explotados por los agentes de amenaza.
- Estimar el impacto sobre el negocio de una materialización de la amenaza.

Estimar la Probabilidad

Una vez identificados los riesgos, debe estimarse:

- La probabilidad de que una vulnerabilidad en particular sea descubierta y explotada.
- Inicialmente es recomendable definir parámetros de calificación cualitativos para estimar la probabilidad. Para un calculo con mayor certeza s recomendable el calculo cuantitativo.

ALTA

Vulnerabilidad que si es explotada comprometería la seguridad de la información ocasionando un impacto negativo sobre la empresa. Debe solucionarse inmediatamente.

MEDIA

Vulnerabilidad que si es explotada tendría un impacto leve sobre la operativa del negocio. Puede solucionarse en un tiempo prudente.

BAJA

Vulnerabilidad que si es explotada no ocasionaría mayores inconvenientes. Su solución no necesariamente será inmediata.

OWASP
The Open Web Application Security Project

Agentes de Amenaza

- Penetration tester **(1)**
- Redes y Programación **(3)**
- Usuario avanzado en computación **(4)**
- Habilidades técnicas medias **(6)**
- No cuenta con habilidades técnicas **(9)**

- Baja o sin motivación **(1)**
- Algo de interés **(4)**
- Bastante interesado **(9)**

- Acceso total **(0)**
- Acceso especial **(4)**
- Algunos accesos **(7)**
- Sin acceso **(9)**

- * Desarrolladores **(2)**
- Administradores de sistemas **(2)**
- Usuarios internos **(4)**
- Socios de negocio **(5)**
- Usuarios autenticados **(6)**
- Anónimos **(9)**

Vulnerabilidades

- Dificultad alta **(1)**
- Dificultad media **(3)**
- Sencilla **(7)**
- Herramientas automatizadas disponibles **(9)**

- Complejo **(1)**
- Dificultad media **(3)**
- Sencilla **(5)**
- Herramientas automatizadas disponibles **(9)**

- Desconocido **(1)**
- Medianamente conocido **(4)**
- Común **(6)**
- De conocimiento público **(9)**

- Detección activa en la aplicación **(1)**
- Autenticado y monitoreado **(3)**
- Autenticado sin monitoreo **(8)**
- No autenticado **(9)**

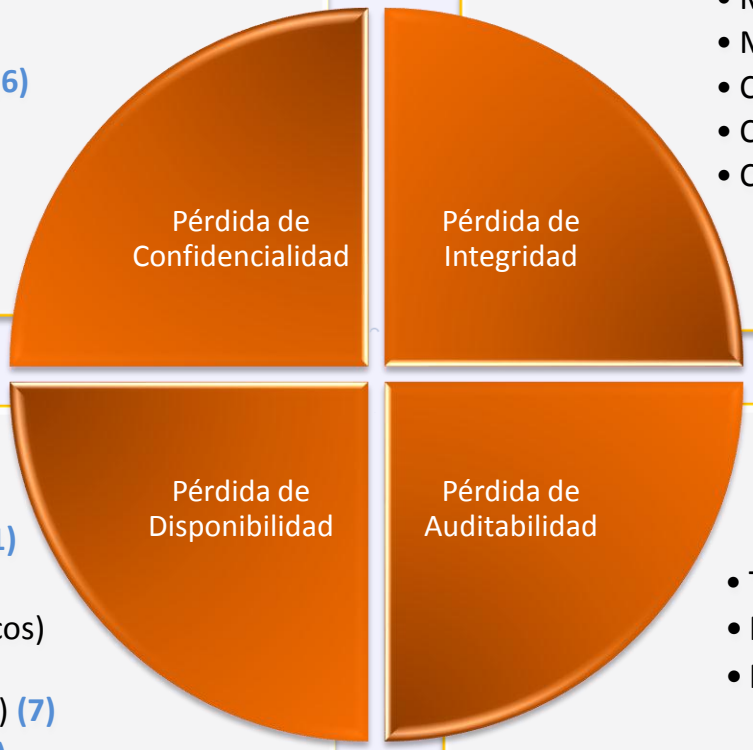
Estimar el Impacto

Cuando una amenaza es materializada, deben considerarse dos tipos de impacto:

- Impacto Técnico.
- Impacto sobre el Negocio.

Impacto Técnico

- Mínima (data no critica) (2)
- Mínima (data critica) (6)
- Considerable (data no critica) (6)
- Considerable (data critica) (7)
- Corrupción de datos total (9)



- Mínima (data no critica) (1)
- Mínima (data critica) (3)
- Considerable (data no critica) (5)
- Considerable (data critica) (7)
- Corrupción de datos total (9)

- Mínima (servicios no críticos) (1)
- Mínima (servicios críticos) (5)
- Considerable (servicios no críticos) (5)
- Considerable (servicios críticos) (7)
- Pérdida total de los servicios (9)

- Totalmente auditable (1)
- Posiblemente auditable (7)
- No auditable (9)

OWASP
The Open Web Application Security Project

Impacto en el Negocio

- Menor que el costo de la solución total (1)
- Efecto menor en el costo anual (3)
- Efecto significante en el costo anual (7)
- Efecto devastador (bancarrota) (9)

- Daño mínimo (1)
- Pérdida de grandes cuentas (4)
- Pérdida de credibilidad a gran escala (5)
- Daño total de imagen (9)

- Mínimo (2)
- Medio (5)
- Alto (7)

- Una persona (3)
- Cientos de personas (5)
- Miles de personas (7)
- Millones de personas (9)

Determinar la Severidad del Riesgo

Para determinar la severidad del riesgo, se debe trabajar con los siguientes valores:

- **Probabilidad de la ocurrencia de la amenaza.**
- **Impacto generado sobre el negocio.**

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Ejemplo – Cálculo de la probabilidad

Threat agent factors			
Skill level	Motive	Opportunity	Size
5	2	7	1

Vulnerability factors			
Ease of discovery	Ease of exploit	Awareness	Intrusion detection
3	6	9	2

$\sum$ Variables de agentes de amenaza y Variable de factores de vulnerabilidad

8

Overall likelihood=4.375 (MEDIUM)

Ejemplo – Cálculo del Impacto

Technical Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability
9	7	5	8
Overall technical impact=7.25 (HIGH)			

$\sum$ Variables de Impacto técnico

4

$\sum$ Variables de Impacto sobre el negocio

4

Business Impact			
Financial damage	Reputation damage	Non-compliance	Privacy violation
1	2	1	5
Overall business impact=2.25 (LOW)			

Resultado

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	edium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

http://paradoslabs.nl/owaspcalc/

OWASP
The Open Web Application Security Project

Priorizar Planes de Acción

Luego de que se hayan clasificado los riesgos de la aplicación, debe desarrollarse una lista de priorización para dar solución inmediata a los riesgos identificados con prioridad ALTA.

OWASP
The Open Web Application Security Project

Personalizar el modelo de clasificación de Riesgos

Es fundamental crear un modelo o marco de clasificación y de riesgos para las aplicaciones del negocio, los siguientes son puntos que deben considerarse en el modelo:

- **Adicionar Factores de Riesgo: define que deben identificarse factores de riesgo que sean representativos para el negocio en específico.**
- **Personalización de Factores de Riesgo define que la personalización de los factores de riesgos es adecuada para la eficacia del mismo y permite una adecuación sobre los procesos reales del negocio.**
- **Ponderar Factores de Riesgo: define que deben ponderarse los factores de riesgos, esto requiere de un mayor análisis pero es lo mas adecuado para lograr una clasificación y análisis detallada.**

OWASP
The Open Web Application Security Project

GRACIAS