

OWASP Top 10 – 2010
Caso práctico en Chile

Alejandro Bedini G.

abq@bedinialejandro.com

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation
<http://www.owasp.org/>

Agenda

- Supuestos
- Las tipicas preguntas
- Ejemplo práctico
- Resultados y Conclusiones

OWASP - 2010 

Supuestos

- La presentación se basa en experiencias reales pero datos "sanitizados".
- Se concentrará respecto a la Norma PCI , ítem código de Software con enfoque a OWASP.
- Se orienta a caso práctico, fácil y rápido de implantar.
- Se basa en que se conoce los Top Ten OWASP.

OWASP - 2010 

OWASP 2010 Top 10

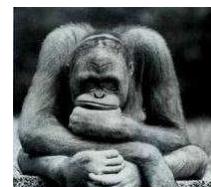
OWASP Top 10 – 2010 (New)

- | |
|--|
| A1 – Injection |
| A2 – Cross Site Scripting (XSS) |
| A3 – Broken Authentication and Session Management |
| A4 – Insecure Direct Object References |
| A5 – Cross Site Request Forgery (CSRF) |
| A6 – Security Misconfiguration (NEW) |
| A7 – Insecure Cryptographic Storage |
| A8 – Failure to Restrict URL Access |
| A9 – Insufficient Transport Layer Protection |
| A10 – Unvalidated Redirects and Forwards (NEW) |

OWASP - 2010 

Preguntas fáciles respuestas difíciles

- ¿ Quién ?
- ¿ Por qué ?
- ¿ Cómo ?
- ¿ Cuándo ?



OWASP - 2010 

¿ Quién ?



6

OWASP - 2010 

¿ Quién ?

- A quiénes debemos convencer de revisar código
 - ▶ Determinar sponsor, técnicos, desarrolladores, clientes y proveedores.
- Quién me financia
 - ▶ Mi empresa, mi cliente o el mercado.



7 OWASP - 2010



¿ Por qué ?



8

OWASP - 2010



¿ Por qué ?

- Por qué debemos revisar
 - ▶ Por seguridad, por una exigencia de industria, por una norma, o por decisión de la empresa.
- Determinar los drivers de decisión y defenderlos a muerte.
- Evangelizar e implantar un plan de gestión del cambio.

9

OWASP - 2010



¿ Cómo ?



OWASP - 2010



¿ Cómo ?

- Establecer sinergia.
- Establecer estrategia de implantación.
- Siempre basarse en procesos o una metodología.
- Institucionalización que incluya ciclo de mejora.

11

OWASP - 2010



¿ Cuándo ?



12

OWASP - 2010



¿ Cuándo ?

- Establecer en que momento de tu proceso de desarrollo efectúas revisión de código.
- Establecer en que momento se corrige y por tipo de hallazgos.
- Considera en tu planificación revisiones, correcciones y re-revisiones.

13

OWASP - 2010



Caso Práctico

- Los informes o casos que se presentan son reales. Los datos que se muestran son “sanitizados” o ficticios.



14

OWASP - 2010

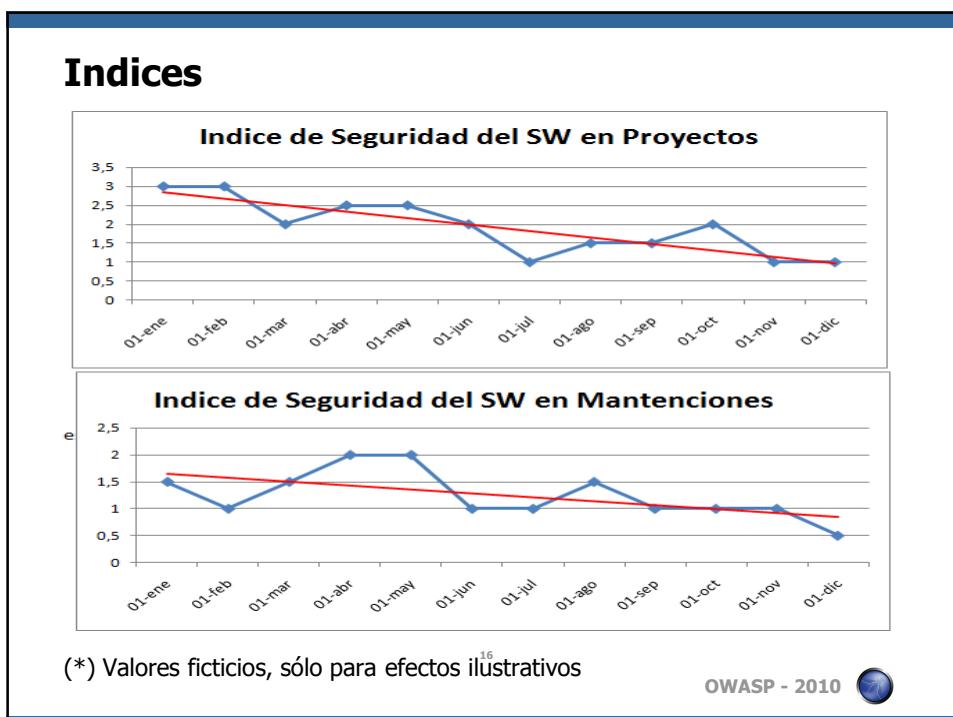


BSC, Balanced score Card

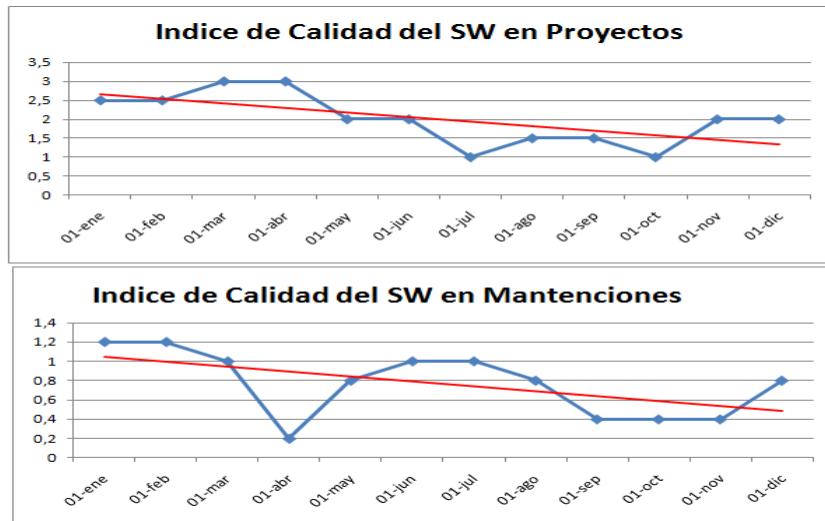
Balanced Scorecard for
Strategic Objectives and Critical Factors

01 Finances	
Low process costs	Actual Time Period: 93,3% Target Time Period: 100%
High revenue growth	Actual Time Period: 91,7% Target Time Period: 100%
High return equity	Actual Time Period: 86,7% Target Time Period: 100%
02 Customers	
High customer satisfaction	Actual Time Period: 98% Target Time Period: 100%
Broad performance spectrum	

15 OWASP - 2010



Indices -2-



(*) Valores ficticios, sólo para efectos ilustrativos¹⁷

OWASP - 2010



Reportes

- Servicio Inspección de código (ICOD)
- Conceptos a revisar e inspeccionar

Tipificación	Segmentado por Severidad o Gravedad			
	Grave	Leve	Medio	Total general
Calidad	16	8	12	36
Rendimiento	11	1	5	17
Seguridad	20			20
Total general	47	9	17	73

Revisión – Calidad

LÍNEA	CÓDIGO	DESCRIPCIÓN	NIVEL	ESTADO	FECHA	HORA	USUARIO
1	E001	Sección no se ajusta a criterios de programación (ej: documento de "función principal" que no es la función principal).	grave	A	1	1	
2	E002	Existe una sección que no cumple con las normas de programación.	grave	A	1	101	
3	E003	No se ejecuta el algoritmo de acuerdo a lo que se especifica.	grave	A	1	1	
4	E004	El código no cumple con los estándares de programación.	grave	A	1	1	
5	E005	El código no cumple con los estándares de programación para C/C++.	grave	A	1	1	

36 ítems de calidad a revisar.

Revisión – Rendimiento

LÍNEA	CÓDIGO	DESCRIPCIÓN	NIVEL	ESTADO	FECHA	HORA	USUARIO
1	E001	Prácticas para la programación de tipo C/C++ que no cumplen con las normas de rendimiento.	grave	A	1	1	
2	E002	No se ejecuta el algoritmo de acuerdo a lo que se especifica.	grave	A	1	101	
3	E003	Los datos ingresados son una dimensión mayor que la variable o buffer que les asignó.	grave	A	1	1	
4	E004	No se ejecuta el algoritmo de acuerdo a lo que se especifica.	grave	A	1	1	
5	E005	Se ejecutan bucles que no cumplen con las normas de rendimiento.	grave	A	1	1	
6	E006	Se ejecutan bucles que no cumplen con las normas de rendimiento.	grave	A	1	1	
7	E007	Se ejecutan bucles que no cumplen con las normas de rendimiento.	grave	A	1	1	
8	E008	Se ejecutan bucles que no cumplen con las normas de rendimiento.	grave	A	1	1	
9	E009	Se ejecutan bucles que no cumplen con las normas de rendimiento.	grave	A	1	1	
10	E010	Se ejecutan bucles que no cumplen con las normas de rendimiento.	grave	A	1	1	

17 ítems de rendimiento a revisar.

Revisión – Seguridad

LÍNEA	CÓDIGO	DESCRIPCIÓN	NIVEL	ESTADO	FECHA	HORA	USUARIO
1	E001	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
2	E002	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	101	
3	E003	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
4	E004	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
5	E005	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
6	E006	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
7	E007	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
8	E008	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
9	E009	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
10	E010	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
11	E011	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
12	E012	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
13	E013	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
14	E014	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
15	E015	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
16	E016	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
17	E017	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
18	E018	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
19	E019	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	
20	E020	No se ejecuta el algoritmo de tipo C/C++.	grave	A	1	1	

20 ítems de seguridad a revisar.

19 ítems basados en OWASP

Reportes

Información de Gestión: Calidad / Seguridad / Rendimiento

Medición Para el Total de Piezas

Total de Piezas	
Cantidad de piezas revisadas.	
Cantidad total de defectos detectados por piezas de código.	
Cantidad de defectos severidad grave detectados por piezas de código.	
Cantidad de defectos severidad media detectados por piezas de código.	

Métrica	Unidad de medida
Cantidad total de defectos detectados por piezas de código.	Defectos / piezas de código
Cantidad de defectos severidad grave detectados por piezas de código.	Defectos / piezas de código
Cantidad de defectos severidad media detectados por piezas de código.	Defectos / piezas de código

De lo anterior, se calcula el indicador de calidad:

$$\sum_{i=1}^{n^3} ((a - 3) - b) + n$$

y "n" representa el total de métricas.

(*) Fórmula ficticia, sólo para efectos ilustrativos

Tendencia Mensual

Mes	Rendimiento	Seguridad	Calidad
mes1	8	4	3
mes2	8	4	3
mes3	8	5	4
mes4	12	6	5

Reportes

Información de Gestión: Calidad / Seguridad / Rendimiento

RESUMEN EJECUTIVO

SEGURIDAD	TOTAL PIEZAS		PIEZAS NUEVAS	
	SEGURIDAD MEDIA	Índice de Seguridad $I_S = 1,0$	SEGURIDAD MEDIA	Índice de Seguridad $I_S = 1,0$
Metodologías	Total de Piezas	Total de Piezas Nuevas		
	<ul style="list-style-type: none"> • 31 piezas de código = 31.106 LOCs. • 71,43% (15 piezas) con hallazgos. • 28,57% (6 piezas) no presentan hallazgos. 	<ul style="list-style-type: none"> • 19 piezas de código = 17.129 LOCs. • 40,00% (4 piezas) con hallazgos. • 60,00% (6 piezas) no presentan hallazgos. 		
Total Hallazgos	Código Hallazgo	Total	Porcentaje	
	<p>PC0111 (Grave. Rotación de información. La pieza incluye código duro (jávaparser, parser, etc.) que no tienen un significado claro dentro de la pieza).</p> <p>SEB001 (Media. La pieza incluye la instrucción GO TO).</p> <p>SEB002 (Media. La pieza incluye valores numéricos que no tienen un significado claro dentro de la pieza).</p> <p>SEB003 (Crít. La pieza incluye código duro).</p> <p>SEB004 (Lew. La pieza incluye código duro en comentarios).</p>	14	6,00%	
Total Hallazgos Piezas Nuevas	Código Hallazgo	Total	Porcentaje	
	<p>PC0111 (Grave. Rotación de información. La pieza incluye código duro (jávaparser, parser, etc.) que no tienen un significado claro dentro de la pieza).</p> <p>SEB001 (Media. La pieza incluye la instrucción GO TO).</p> <p>SEB002 (Media. La pieza incluye valores numéricos que no tienen un significado claro dentro de la pieza).</p>	3	1,45%	

Indicadores identificados por código

Indicadores identificados por pieza

Indicadores identificados por pieza

Indicaciones de código críticas

Calidad

OWASP - 2010

Resultados y Conclusiones

- Sin basarse en una norma o un esquema metodológico no sirve.
- No pierdas el tiempo en la justificación económica.
- Si estableces sinergia consigues aumento de la calidad y seguridad del código.
- Todos se benefician aunque existan detractores.
- Obligas a incorporar buenas prácticas al desarrollo del código.

21

OWASP - 2010



Consultas y gracias

- Sino los convences...confúndelos.



22

OWASP - 2010

