



The slide header features a blue top bar. Below it, on the left, is a decorative vertical bar with blue and green squares. The main content area is light gray. At the top left of this area is the OWASP logo (a blue sphere with a white spiderweb). To its right, the text "OWASP Top 10 – 2010" is in bold, followed by "Caso práctico en Chile". Below this, the name "Alejandro Bedini G." is displayed, followed by the email address "abg@bedinialejandro.com" in blue. At the bottom of the gray area, a small copyright notice reads: "Copyright © The OWASP Foundation. Permission is granted to copy, distribute and/or modify this document under the terms of the OWASP License." The bottom of the slide has a blue bar with the text "The OWASP Foundation" and the URL "http://www.owasp.org/".

OWASP Top 10 – 2010
Caso práctico en Chile

Alejandro Bedini G.
abg@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 típicas preguntas
- Ejemplo práctico
- Resultados y Conclusiones

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 faciles respuestas dificiles

- ¿ 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

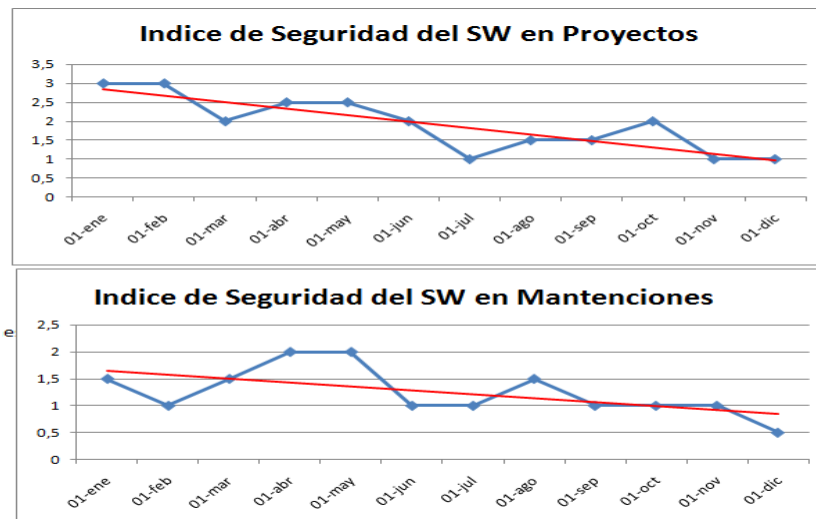


15

OWASP - 2010



Indices



(*) Valores ficticios, sólo para efectos ilustrativos¹⁶

OWASP - 2010



Reportes

Información de Gestión: Calidad / Seguridad / Rendimiento

Medición Para el Total de Piezas

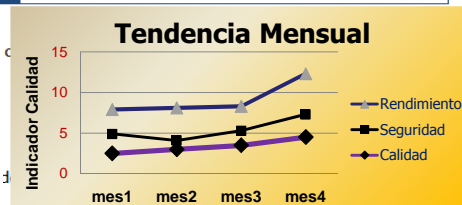
Total de Piezas	
Cantidad de piezas revisadas.	
Cantidad total de defectos detectados por piezas de código.	
Cantidad de defectos severidad grave detectados por piezas de código.	
Cantidad de defectos severidad media detectados por piezas de código.	
Métrica	Unidad de medida
Cantidad total de defectos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

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

y "n" representa el total de métricas.

(*) Formula ficticia, sólo para efectos ilustrativos

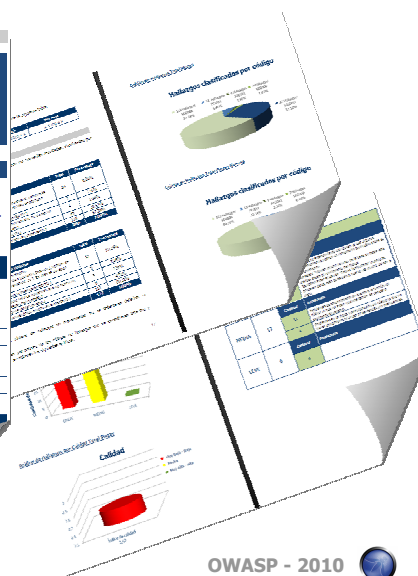


Reportes

Información de Gestión: Calidad / Seguridad / Rendimiento

RESUMEN EJECUTIVO

SEGURIDAD	TOTAL PIEZAS	PIEZAS NUEVAS
	SEGURIDAD MEDIA Índice de Seguridad $I_{(a)} = 1.0$ Meta < 1 Seguridad Alta	SEGURIDAD MEDIA Índice de Seguridad $I_{(a)} = 1.0$
Medicinnec	Total de Piezas	Total de Piezas Nuevas
	<ul style="list-style-type: none"> 21 piezas de código = 31.10% LOC. 71.43% (15 piezas) con hallazgos. 28.57% (6 piezas) no presentan hallazgos. 	<ul style="list-style-type: none"> 10 piezas de código = 17.12% LOC. 40.00% (4 piezas) con hallazgos. 60.00% (6 piezas) no presentan hallazgos.
Total Hallazgos	Código Hallazgo	
	PC011 (Grav. Revelación de información (La pieza incluye código duro (seriación, parámetros, nombre de seriación, archivos, parámetros, etc.). En Web se agregan también URL, etc.).	14 6.00%
	SE001 (Medio. La pieza incluye la instrucción GO TO.)	3 1.46%
	SE002 (Medio. La pieza incluye valores numéricos que no tienen un significado claro dentro de contexto.)	4 1.94%
	SE003 (Leve. La pieza incluye código muerto.)	67 32.52%
Total Hallazgos Piezas Nuevas	SE004 (Leve. La pieza incluye código muerto en contexto.)	118 57.88%
	Total General	206 100%
Total Hallazgos Piezas Nuevas	Código Hallazgo	
	PC011 (Grav. Revelación de información (La pieza incluye código duro (seriación, parámetros, nombre de seriación, archivos, parámetros, etc.). En Web se agregan también URL, etc.).	
	SE001 (Medio. La pieza incluye la instrucción GO TO.)	



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 