OWASP Top 10 – 2010
Caso práctico en Chile

Alejandro Bedini G.

abg@bedinialejandro.com

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

Agenda

- Supuestos
- Las tipicas 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 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)

Preguntas faciles respuestas dificiles

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

¿ Quién ?

6

¿ 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

¿ Por qué ?

8

¿ 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.

¿ Cómo ?

¿ Cómo ?

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

¿ Cuándo ?

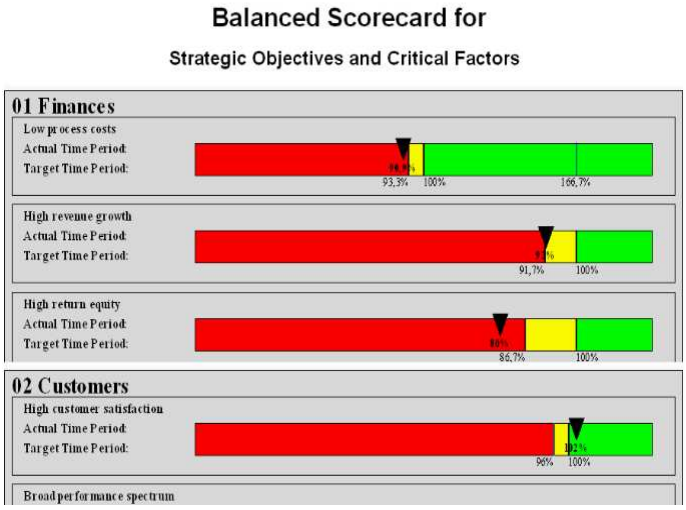
¿ Cuándo ?

- 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.

Caso Práctico

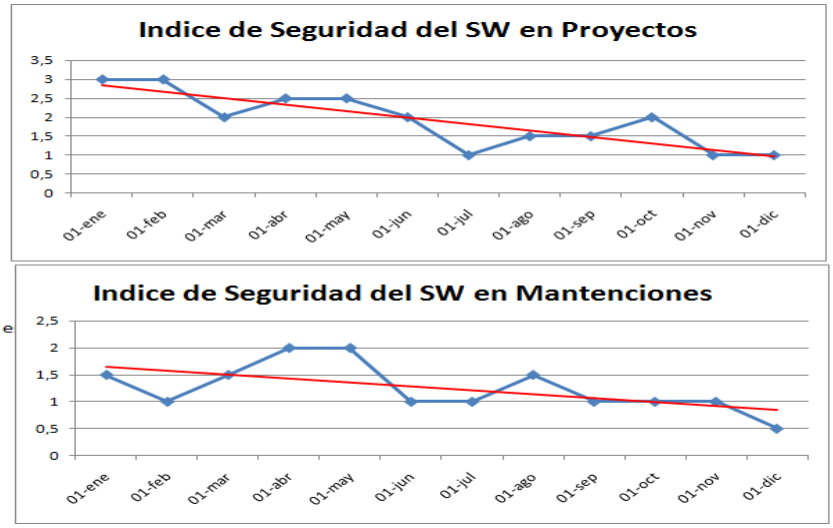
- Los informes o casos que se presentan son reales. Los datos que se muestran son "sanitizados" o ficticios.

BSC, Balanced score Card



15

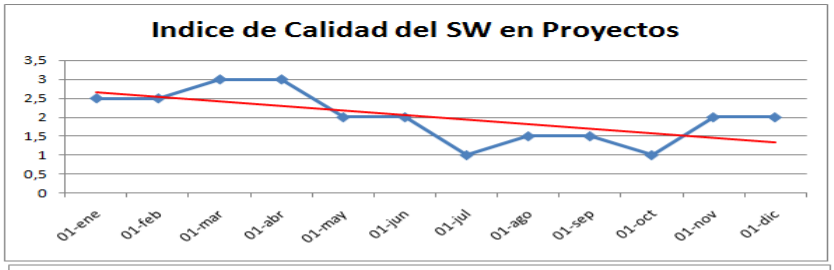
Indices

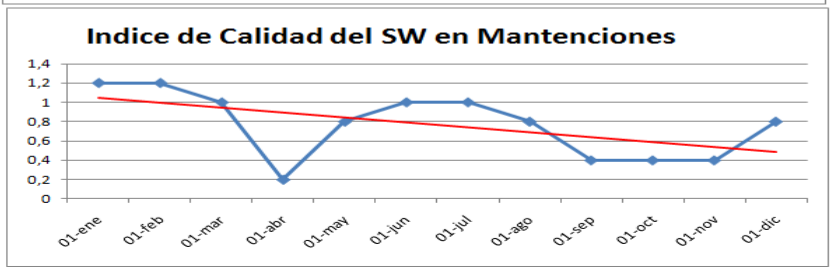


(*) Valores ficticios, sólo para efectos ilustrativos

16

Indices -2-



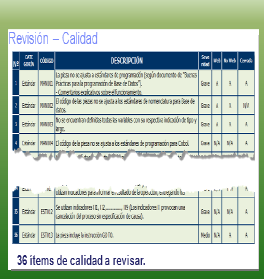


(*) Valores ficticios, sólo para efectos ilustrativos

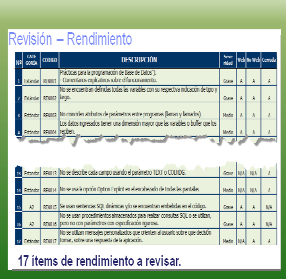
Reportes

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

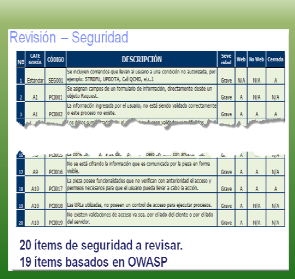
	Segmentado por Severidad o Gravedad			
Tipificación	**Grave**	**Leve**	**Medio**	**Total general**
Calidad	16	8	12	36
Rendimiento	11	1	5	17
Seguridad	20			20
Total general	**47**	**9**	**17**	**73**


Revisión – Calidad

36 ítems de calidad a revisar.


Revisión – Rendimiento

17 ítems de rendimiento a revisar.


Revisión – Seguridad

20 ítems de seguridad a revisar.
19 ítems basados en OWASP

Reportes

Información de Gestión: Calidad / Seguridad / Rendimiento

Medición Para el Total de Piezas

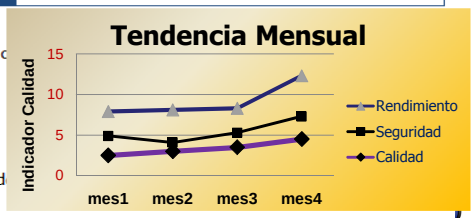
Total de Piezas
Cantidad de piezas revisadas.
Cantidad total de defectos detectados por piezas de código.
Cantidad de defectos severidad grave detectados por piezas de código.
Cantidad de defectos severidad media detectados por piezas de código.

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 c

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

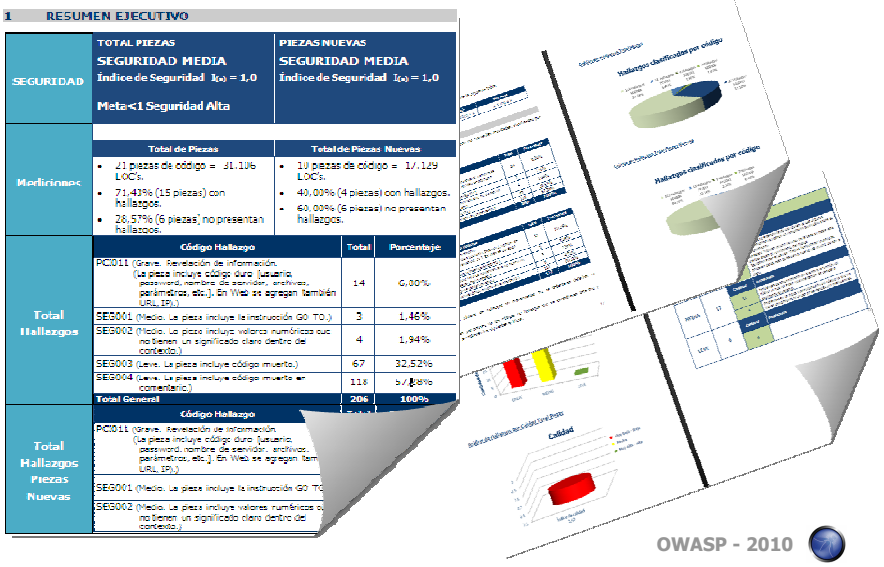
y "n" representa el total de métricas.



(*) Formula ficticia, sólo para efectos ilustrativos

Reportes

Información de Gestión: Calidad / Seguridad / Rendimiento



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.

Consultas y gracias

- Sino los convences…confúndelos.