

OWASP LatamTour
Chile 2016

Desarrollo Seguro

¿Y esto cómo me ayuda a
cumplir PCI-DSS?

Carlos Allendes
Presidente Owasp Chile



OWASP
The Open Web Application Security Project



OWASP LatamTour
Honduras 2016



OWASP
The Open Web Application Security Project

Desarrollo Seguro

¿Y esto cómo me ayuda a
cumplir PCI-DSS?




**OWASP**
The Open Web Application Security Project

Antecedentes
del Expositor

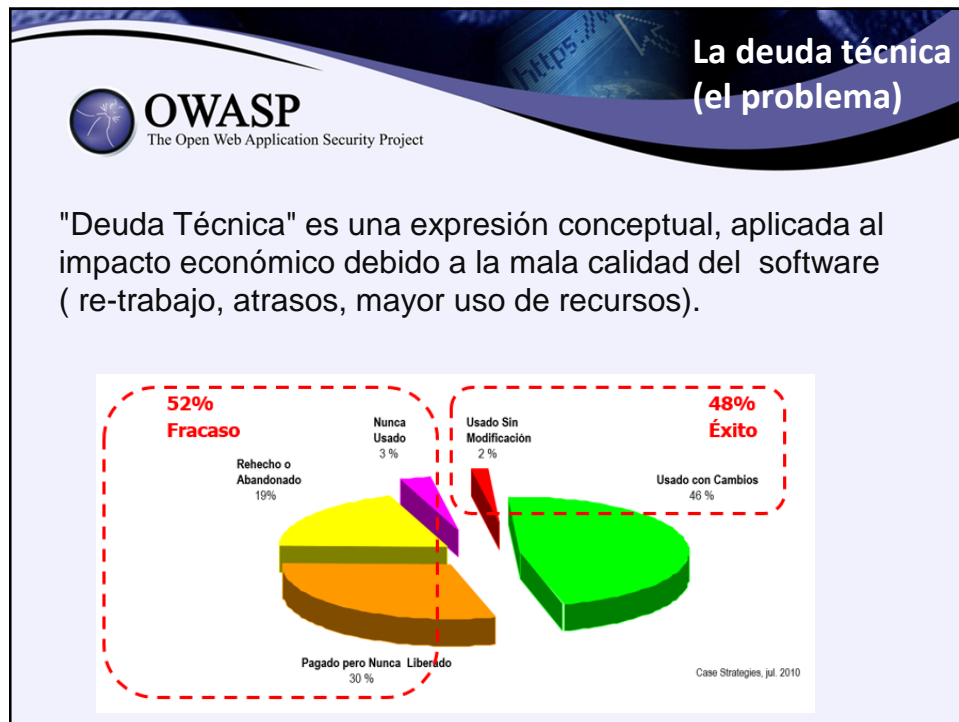
Carlos Allendes Droguett (carlos.allendes@owasp.org)

- Ingeniero Civil en Informática, USACH
- Presidente capítulo chileno OWASP
- Co-fundador capítulo OWASP Honduras y Rep.Dominicana
- Owner en www.qualityfactory.cl (callendes@qualityfactory.cl)
- Asociado en www.dataactiva.cl (callendes@dataactiva.cl)
- Experiencia y proyectos
 - CMMi, AGILE, Ingeniería de Software aplicada.
 - QA y Testing, Testing como servicio externalizado.
 - PCI DSS, acreditación en seguridad.
 - ITIL, implantación de procesos.

**OWASP**
The Open Web Application Security Project

Agenda

- Presentación del expositor
- **La deuda técnica (el problema)**
- Ingeniería de Software (la solución)
- El modelo CMMi
- El modelo SAMM
- Aplicación de SAMM en el mundo real



OWASP
The Open Web Application Security Project

La deuda técnica (el problema)



El Desarrollo de Software es una ARTESANIA...

...y en las artes, el producto final depende del artista.

Y en Desarrollo de Software abundan los artistas...

OWASP
The Open Web Application Security Project


La deuda técnica (el problema)

Cómo el cliente lo explica	Cómo el líder del proyecto lo entiende	Cómo el analista lo diseña	Cómo el programador lo escribe	Cómo el asesor lo describe
Cómo se documenta el proyecto	Qué aplicaciones se instalan	Cómo se factura al cliente	Así se le dará soporte	Lo que el cliente realmente necesitaba

OWASP
The Open Web Application Security Project

La deuda técnica (el problema)

**Otras industrias lograron estandarizarse...
Que necesita la industria del software?**

**OWASP**
The Open Web Application Security Project

Agenda


- Presentación del expositor
- La deuda técnica (el problema)
- **Ingeniería de Software (la solución)**
- El modelo CMMi
- El modelo SAMM
- Aplicación de SAMM en el mundo real

**OWASP**
The Open Web Application Security Project

Ingeniería de Software (la solución)

La ingeniería de Software.
“Aplicación de un enfoque sistemático, disciplinado y medible al desarrollo, operación y mantenimiento del software”.
[IEEE, 1993]

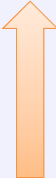





OWASP
The Open Web Application Security Project

Ingeniería de Software (la solución)

Capas de la Ingeniería de Software.



1. Herramientas: Entregan soporte, son un facilitador para el proceso.
2. Métodos: Indican como realizar tareas técnicas para construir el sw.
3. Proceso: Define formas de trabajo en **conjunto de áreas claves**.
4. Enfoque de Calidad: Son la base o cimientos de la Ingeniería de SW



ISO/IEC 14598

ISO 9000-3

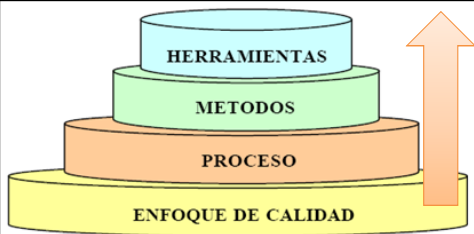



Fig. 2.1. Capas de la ingeniería del software




OWASP
The Open Web Application Security Project

Agenda


- Presentación del expositor
- La deuda técnica (el problema)
- Ingeniería de Software (la solución)
- **El modelo CMMi**
- El modelo SAMM
- Aplicación de SAMM en el mundo real




OWASP
The Open Web Application Security Project

Agenda


- Presentación del expositor
- La deuda técnica (el problema)
- Ingeniería de Software (la solución)
- El modelo CMMi
- **El modelo SAMM**
- Aplicación de SAMM en el mundo real


OWASP
The Open Web Application Security Project

El modelo SAMM

Premisas para un Modelo de Madurez

- Las organizaciones cambian lentamente en el tiempo
 - Cada cambio debe tener un objetivo concreto
 - Los cambios deben aplicarse secuencialmente
- Toda solución debe “adaptarse” a la realidad individual
 - Flexibilidad adaptada al riesgo de la organización
- Las actividades relativas a seguridad deben ser “recetas”
 - Entregar suficiente detalle claro y preciso (guías técnicas)
 - Evitar ambigüedades que confunden al personal no técnico
- Sobre todo, debe ser sencillo, bien definido y medible.


**OWASP**
The Open Web Application Security Project

El modelo
SAMM

Historia de SAMM

- Versión Beta liberada en Agosto de 2008
- Creada originalmente por Fortify (ahora HP)
- Autores aún involucrados activamente
- Publicada bajo licencia Creative Commons
- Donada al proyecto OWASP
- Cambia su nombre a OpenSAMM




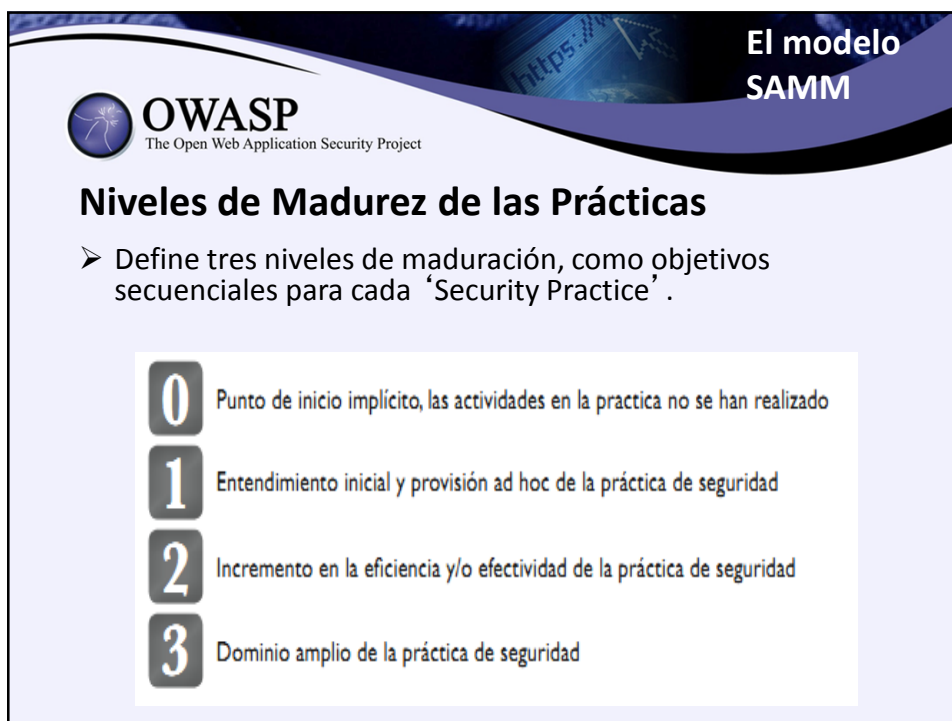
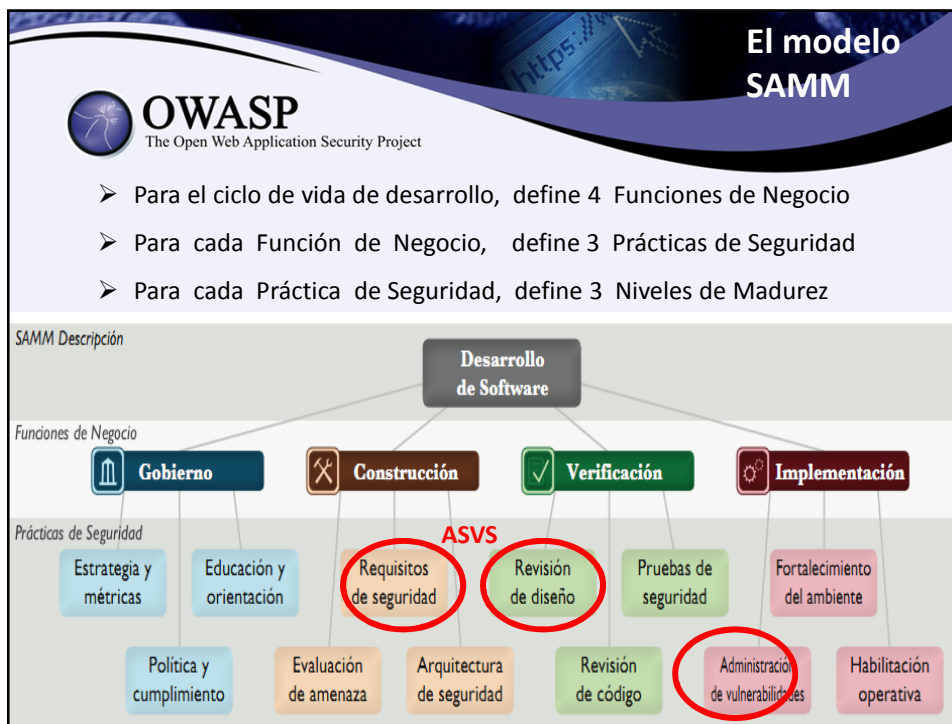
**OWASP**
The Open Web Application Security Project

El modelo
SAMM

Utilidad de SAMM

- Metodología que sirve para evaluar las practicas de desarrollo seguro en una organización.
- Sirve para implementar un programa de "Seguridad de aplicativos" en forma iterativa e incremental.
- Muestra objetivamente los avances en el programa de mejoras de seguridad de aplicaciones.
- Define y mide actividades relacionadas a la seguridad en toda la organización.





Ejemplo aplicado
Definir Objetivo


OWASP
 The Open Web Application Security Project

>> Función de Negocio: Verificación (Testing)
>> Práctica Segura: Revisar el Código

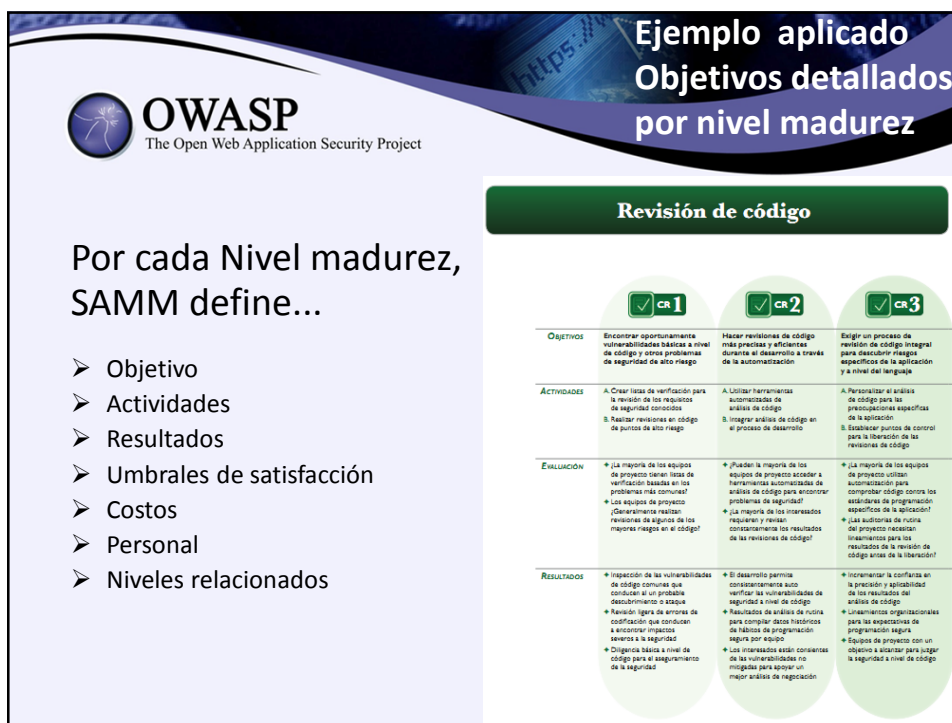
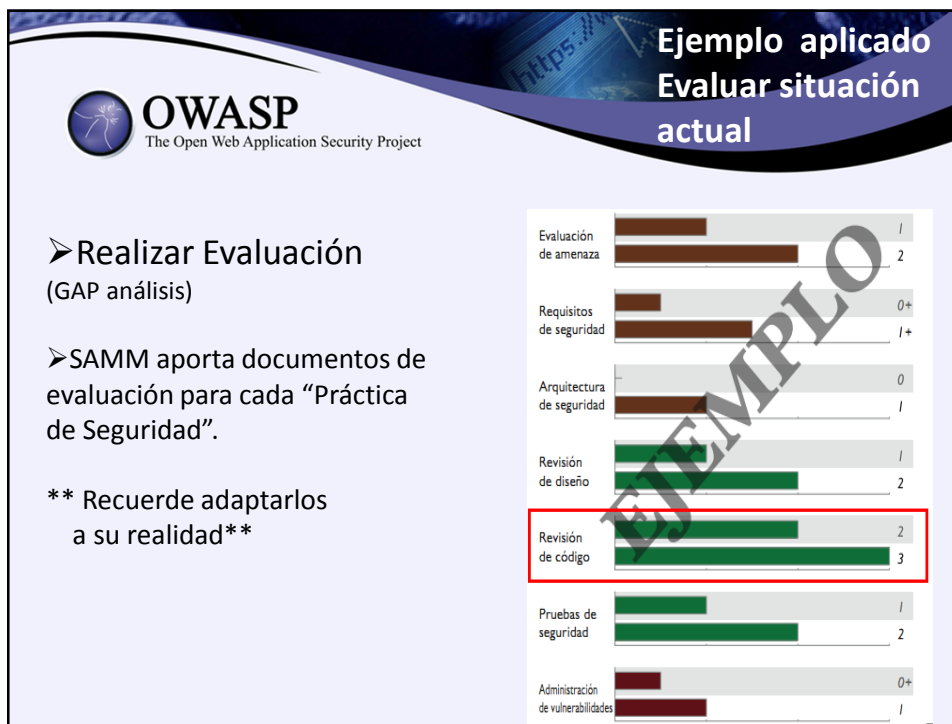
Verificación			
Resumen de actividades			
Revisión de código ...continúa en página 62			
	 CR 1	 CR 2	 CR 3
OBJETIVOS	Encontrar oportunamente vulnerabilidades básicas a nivel de código y otros problemas de seguridad de alto riesgo	Hacer revisiones de código más precisas y eficientes durante el desarrollo a través de la automatización	Exigir un proceso de revisión de código integral para descubrir riesgos específicos de la aplicación y a nivel del lenguaje
ACTIVIDADES	A. Crear listas de verificación para la revisión de los requisitos de seguridad conocidos B. Realizar revisiones en código de puntos de alto riesgo	A. Utilizar herramientas automatizadas de análisis de código B. Integrar análisis de código en el proceso de desarrollo	A. Personalizar el análisis de código para las preocupaciones específicas de la aplicación B. Establecer puntos de control para la liberación de las revisiones de código

Ejemplo aplicado
Evaluar situación actual


OWASP
 The Open Web Application Security Project

>> Checklist para evaluación del GAP

Verificación	
Hoja de trabajo para evaluación	
Revisión de código	Si/No
<ul style="list-style-type: none"> ¿La mayoría de los equipos de proyecto tienen listas de verificación basadas en los problemas más comunes? 	 CR 1
<ul style="list-style-type: none"> Los equipos de proyecto ¿Generalmente realizan revisiones de algunos de los mayores riesgos en el código? 	
<ul style="list-style-type: none"> ¿Pueden la mayoría de los equipos de proyecto acceder a herramientas automatizadas de análisis de código para encontrar problemas de seguridad? 	
<ul style="list-style-type: none"> ¿La mayoría de los interesados requieren y revisan constantemente los resultados de las revisiones de código? 	 CR 2
<ul style="list-style-type: none"> ¿La mayoría de los equipos de proyecto utilizan automatización para comprobar código contra los estándares de programación específicos de la aplicación? 	
<ul style="list-style-type: none"> ¿Las auditorías de rutina del proyecto necesitan lineamientos para los resultados de la revisión de código antes de la liberación? 	 CR 3





OWASP
The Open Web Application Security Project

Ejemplo aplicado
Plantillas de roadmap
por tipo de Industria

Plantillas de Planes de Mejora (Roadmap)

- SAMM entrega Plantillas de Planes de mejora (Roadmaps) para diferentes tipos de Organización (industria)
- Desarrolladores de Software Independientes
 - Organizaciones de servicios financieros (FSO)
 - Administraciones Públicas (AAPP)
- Organizaciones tipo se han elegido porque:
 - Representan los casos de uso más comunes
 - La definición de un "Plan de mejora de la seguridad" optimizado.... es diferente en cada caso.



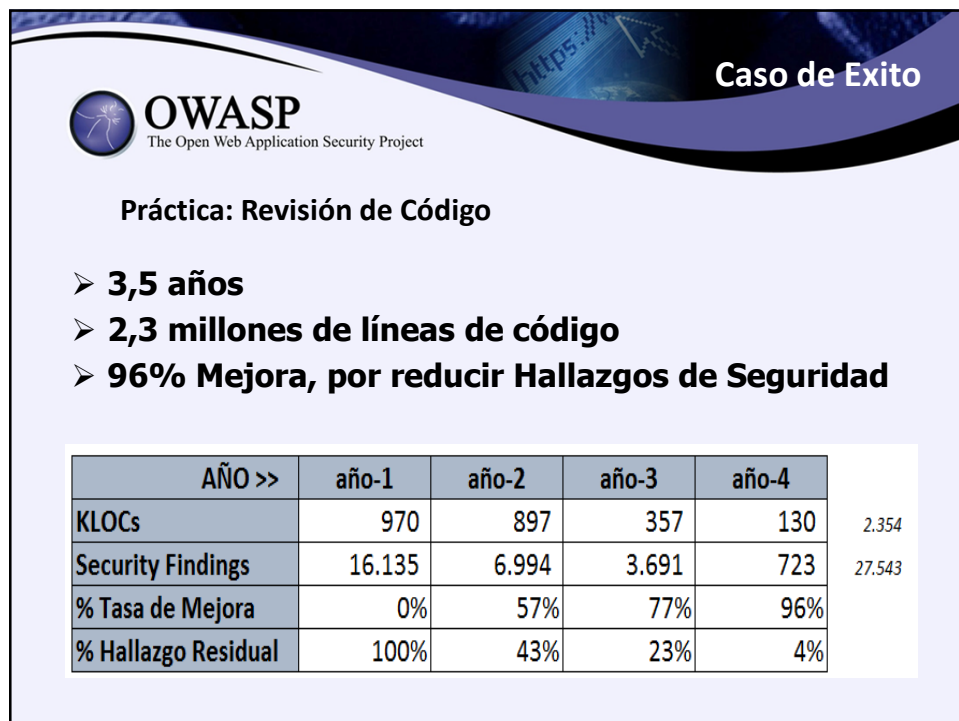
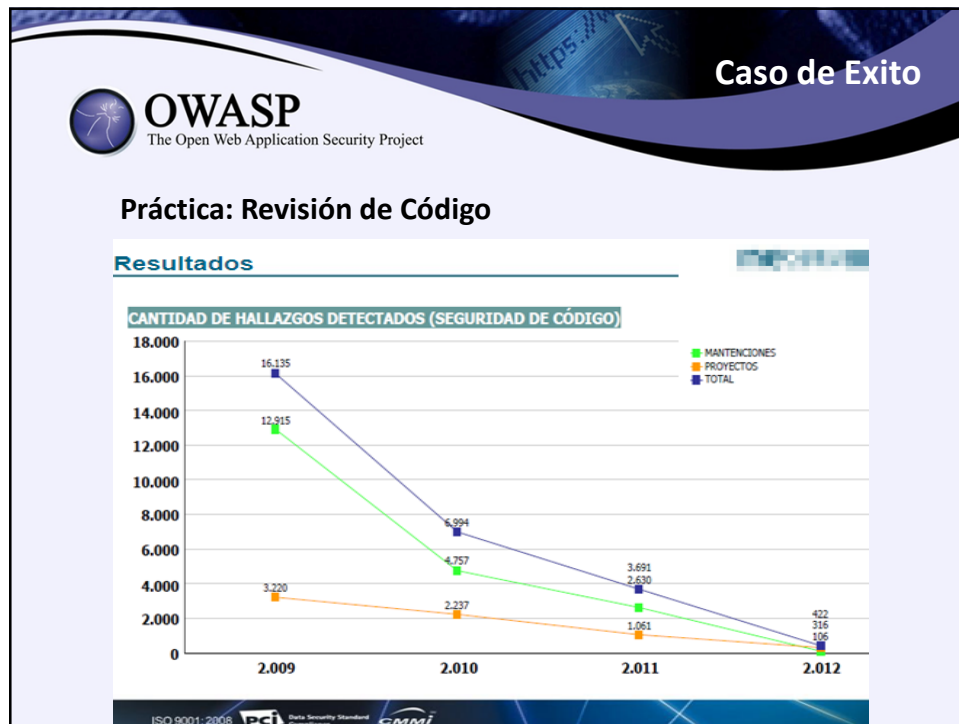


OWASP
The Open Web Application Security Project

Caso de Exito

CASOS DE EXITO






**OWASP**
The Open Web Application Security Project

Caso de Exito

- Otros Casos de exito.. disponibles en diversos referentes de la industria TI:




**OWASP**
The Open Web Application Security Project

Repaso...

Pasos metodológicos... para implantar
DESARROLLO SEGURO

- Evaluar las prácticas de seguridad existentes en la organización.
- Definir un plan ad-hoc de mejora en la seguridad del software basado en iteraciones bien definidas.
- Cuantificar mejoras concretas durante la aplicación del plan de mejora en la seguridad.
- Definir y medir actividades relacionadas con la seguridad en una organización.



OWASP
The Open Web Application Security Project

**Dudas...
Preguntas?**

Desarrollo Seguro

¿Y esto cómo me ayuda a

Mejorar mi trabajo!

~~cumplir PCI-DSS~~

Al usar técnicas de programación segura, que logren un código más estable en las aplicaciones, se inyecta un cambio cultural y una "Maduración de Capacidades"

requeridas para existir, competir y prosperar en el mundo laboral y tecnológico.



OWASP
The Open Web Application Security Project

**Dudas...
Preguntas?**



Carlos Allendes Droguett
carlos.allendes@owasp.org