

OWASP LatamTour  
Honduras 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

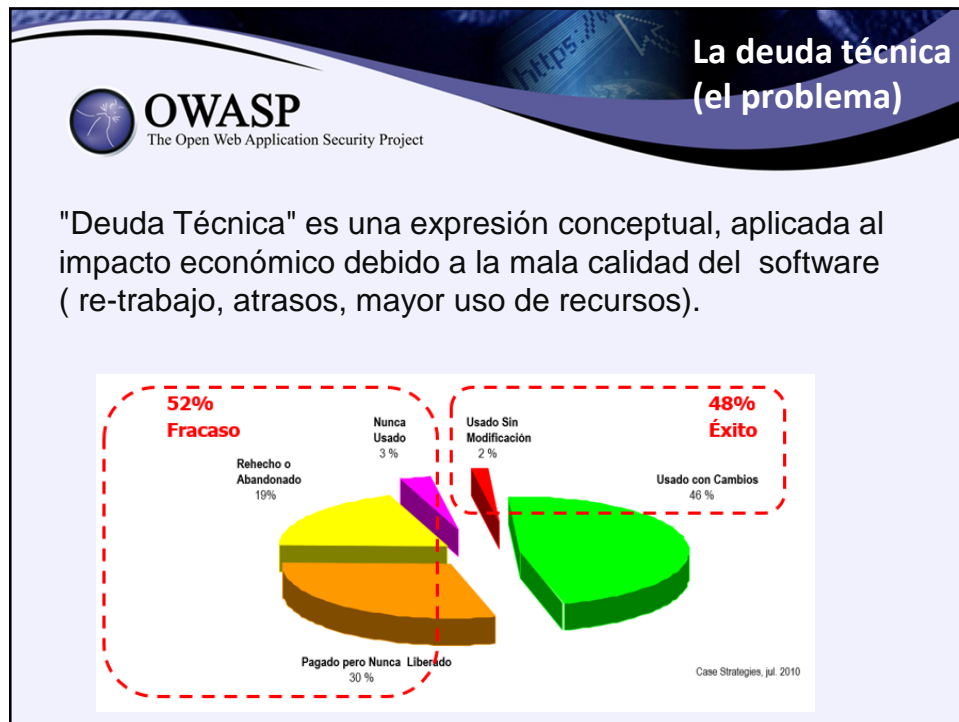
**Carlos Allendes Droguett** ( [carlos.allendes@owasp.org](mailto:carlos.allendes@owasp.org) )

- Ingeniero Civil en Informática, USACH
- Presidente capítulo chileno OWASP
- Co-fundador capítulo OWASP Honduras
  
- Socio en [www.dataactiva.cl](http://www.dataactiva.cl) ( [callendes@dataactiva.cl](mailto: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



**La deuda técnica (el problema)**

**OWASP**  
The Open Web Application Security Project

**El Desarrollo de Software es una ARTESANIA...**



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

... el "PRODUCTO" depende fuertemente del "ARTISTA"




**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.**

Ingeniería del software es la “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

El modelo SAMM


## Y PARA DESARROLLO SEGURO?... HAY UN CAMINO PARA CRECER Y MADURAR



**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.





**OWASP**  
The Open Web Application Security Project

## El modelo SAMM


### Estructura de SAMM

- Para el ciclo de vida de desarrollo, define 4 Funciones de Negocio
- Para cada Función de Negocio, define 3 Prácticas de Seguridad
- Para cada Práctica de Seguridad, define 3 Niveles de Madurez



```

graph TD
    subgraph "SAMM Descripción"
        A[Desarrollo de Software]
    end
    subgraph "Funciones de Negocio"
        B[Gobierno]
        C[Construcción]
        D[Verificación]
        E[Implementación]
    end
    subgraph "Prácticas de Seguridad"
        B1[Estrategia y métricas]
        B2[Educación y orientación]
        B3[Política y cumplimiento]
        C1[Requisitos de seguridad]
        C2[Evaluación de amenaza]
        C3[Arquitectura de seguridad]
        D1[Revisión de diseño]
        D2[Revisión de código]
        D3[Pruebas de seguridad]
        E1[Fortalecimiento del ambiente]
        E2[Administración de vulnerabilidades]
        E3[Habilitación operativa]
    end
    A --- B
    A --- C
    A --- D
    A --- E
    B --- B1
    B --- B2
    B --- B3
    C --- C1
    C --- C2
    C --- C3
    D --- D1
    D --- D2
    D --- D3
    E --- E1
    E --- E2
    E --- E3
  
```



**OWASP**  
 The Open Web Application Security Project

**El modelo SAMM**

## Niveles de Madurez de las Prácticas

➤ Define tres niveles de maduración, como objetivos secuenciales para cada 'Security Practice'.

<b>0</b>	Punto de inicio implícito, las actividades en la práctica no se han realizado
<b>1</b>	Entendimiento inicial y provisión ad hoc de la práctica de seguridad
<b>2</b>	Incremento en la eficiencia y/o efectividad de la práctica de seguridad
<b>3</b>	Dominio amplio de la práctica de seguridad



**OWASP**  
 The Open Web Application Security Project

**Ejemplo aplicado**  
**Definir Objetivo**

>> Función de Negocio: Verificación  
 >> Práctica de Seguridad: Revisión de Código

Verificación			
Resumen de actividades			
Revisión de código <span style="float: right;">...continúa en página 62</span>			
	 <b>CR 1</b>	 <b>CR 2</b>	 <b>CR 3</b>
<b>OBJETIVOS</b>	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
<b>ACTIVIDADES</b>	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



**OWASP**  
 The Open Web Application Security Project


**Ejemplo aplicado**  
**Evaluar situación**  
**actual**

>> Checklist para evaluación del GAP

Verificación

Hoja de trabajo para evaluación

Revisión de código	Si/No
♦ ¿La mayoría de los equipos de proyecto tienen listas de verificación basadas en los problemas más comunes?	
♦ Los equipos de proyecto ¿Generalmente realizan revisiones de algunos de los mayores riesgos en el código?	<input checked="" type="checkbox"/> <b>CR 1</b>
♦ ¿Pueden la mayoría de los equipos de proyecto acceder a herramientas automatizadas de análisis de código para encontrar problemas de seguridad?	<input checked="" type="checkbox"/> <b>CR 2</b>
♦ ¿La mayoría de los interesados requieren y revisan constantemente los resultados de las revisiones de código?	<input checked="" type="checkbox"/> <b>CR 3</b>
♦ ¿La mayoría de los equipos de proyecto utilizan automatización para comprobar código contra los estándares de programación específicos de la aplicación?	<input checked="" type="checkbox"/> <b>CR 3</b>
♦ ¿Las auditorías de rutina del proyecto necesitan lineamientos para los resultados de la revisión de código antes de la liberación?	<input checked="" type="checkbox"/> <b>CR 3</b>



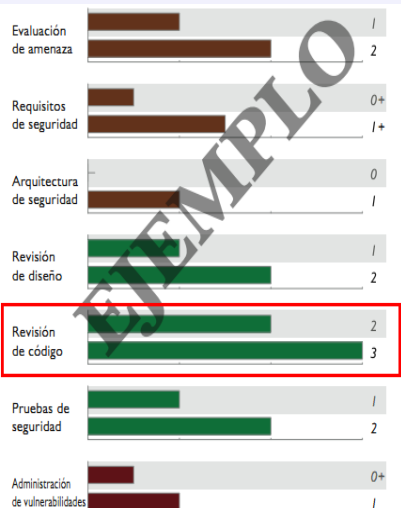
**OWASP**  
 The Open Web Application Security Project

**Ejemplo aplicado**  
**Evaluar situación**  
**actual**


➤ Realizar Evaluación (GAP análisis)

➤ SAMM aporta documentos de evaluación para cada “Práctica de Seguridad”.

**\*\* Recuerde adaptarlos a su realidad\*\***



Práctica de Seguridad	Calificación
Evaluación de amenaza	1
Requisitos de seguridad	0+
Arquitectura de seguridad	1
Revisión de diseño	2
Revisión de código	3
Pruebas de seguridad	2
Administración de vulnerabilidades	0+



**OWASP**  
The Open Web Application Security Project

## Ejemplo aplicado

### Objetivos detallados por nivel madurez

Por cada Nivel madurez, SAMM define...

- Objetivo
- Actividades
- Resultados
- Umbrales de satisfacción
- Costos
- Personal
- Niveles relacionados

#### Revisión de código

	✓ CR 1	✓ CR 2	✓ CR 3
<b>Objetivo</b>	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
<b>Actividades</b>	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 predicciones específicas de la aplicación B. Establecer puntos de control para la liberación de las revisiones de código
<b>Evaluación</b>	• ¿La mayoría de los equipos de proyecto tienen listas de verificación basadas en los problemas más comunes? • ¿Los equipos de proyecto ¿Constantemente realizan revisiones de algunos de los mayores riesgos en el código?	• ¿Pueden la mayoría de los equipos de proyecto acceder a herramientas automatizadas de análisis de código para encontrar problemas de seguridad? • ¿La mayoría de los interesados requieren y reciben constantemente los resultados de las revisiones de código?	• ¿La mayoría de los equipos de proyecto utilizan automatización para comprobar código contra los estándares de programación específicos de la aplicación? • ¿Las autoridades de rutina del proyecto necesitan herramientas para los resultados de la revisión de código antes de la liberación?
<b>Resultados</b>	• Inspección de las vulnerabilidades de código comunes que conducen a un probable deterioro o ataque • Revisión ligera de errores de codificación que conducen a encontrar impactos severos a la seguridad • Diligencia básica a nivel de código para el aseguramiento de la seguridad	• El desarrollo permite constantemente auto-verificar las vulnerabilidades de seguridad a nivel de código • Resultados de análisis de rutina para cumplir decenas históricos de hábitos de programación segura por equipo • Los interesados están conscientes de las vulnerabilidades no mitigadas para aplicar un mejor análisis de negociación	• Incrementar la confianza en la precisión y aplicabilidad de los resultados del análisis de código • Lineamientos organizacionales para las expectativas de programación segura • Equipos de proyecto con un objetivo a adoptar para lograr la seguridad a nivel de código



**OWASP**  
The Open Web Application Security Project

## Ejemplo aplicado

### Plantillas de roadmap por tipo de Industria

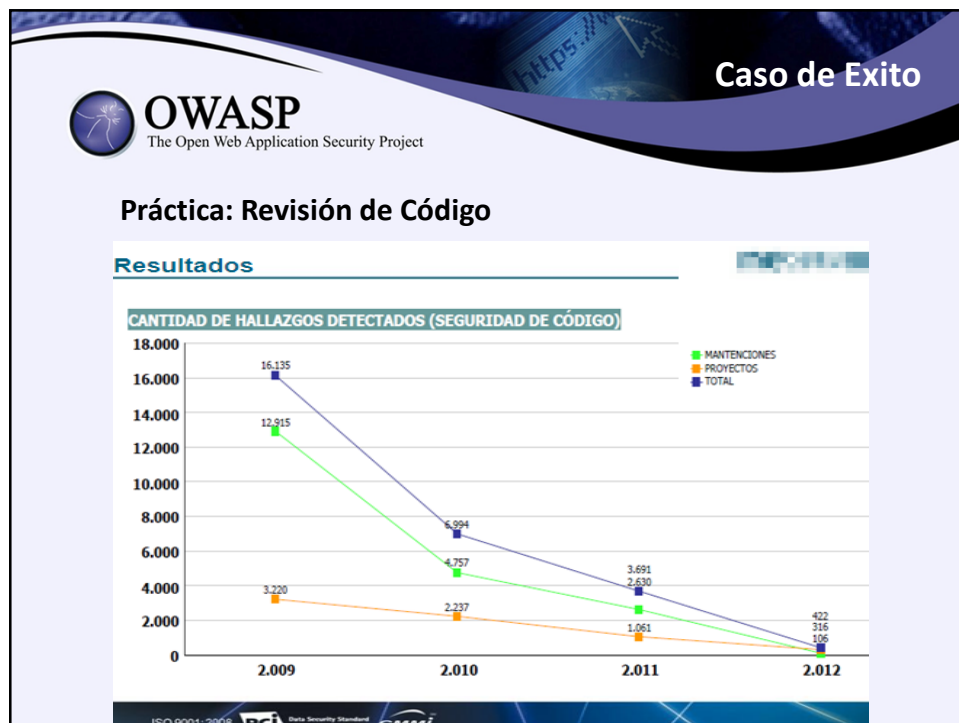
## Plantillas de Planes de Mejora (Roadmap)

- 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

**Caso de Exito**



**OWASP**  
The Open Web Application Security Project

**Práctica: Revisión de Código**

- **3,5 años**
- **2,3 millones de líneas de código**
- **96% Mejora, por reducir Hallazgos de Seguridad**

AÑO >>	año-1	año-2	año-3	año-4	
KLOCs	970	897	357	130	2.354
Security Findings	16.135	6.994	3.691	723	27.543
% Tasa de Mejora	0%	57%	77%	96%	
% Hallazgo Residual	100%	43%	23%	4%	

**Caso de Exito**




**OWASP**  
The Open Web Application Security Project

- 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**      **Mejorar mi trabajo!**

**¿Y esto cómo me ayuda a ~~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](mailto:carlos.allendes@owasp.org)