OWASP LatamTour
Rep.Dominicana 2016

BIENVENIDOS AL VI

OWASP LATAMTOUR

Carlos Allendes

Presidente Owasp Chile

OWASP
The Open Web Application Security Project

OWASP LATAM 2016 LATIN AMERICA TOUR

OWASP LatamTour
Honduras 2016

OWASP
The Open Web Application Security Project

Desarrollo Seguro

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

OWASP LATAM 2016 LATIN AMERICA TOUR

Antecedentes del Expositor

OWASP The Open Web Application Security Project

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

- Ingeniero Civil en Informática, USACH
- Presidente capítulo chileno OWASP
- Co-fundador capítulo OWASP Rep.Dominicana

- Socio en www.datactiva.cl (callendes@datactiva.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.

Agenda

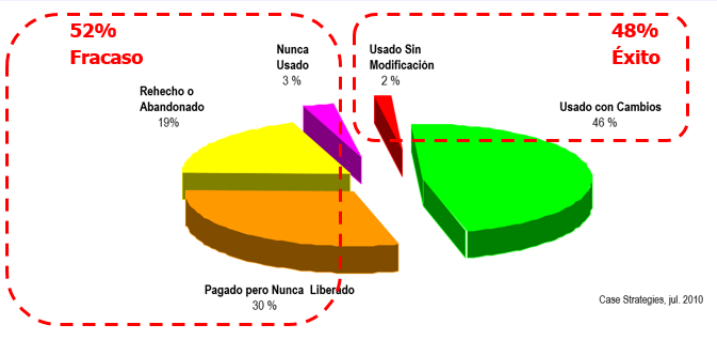
OWASP The Open Web Application Security Project

- 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

"Deuda Técnica" es una expresión conceptual, aplicada al impacto económico debido a la mala calidad del software (re-trabajo, atrasos, mayor uso de recursos).



La deuda técnica (el problema)

OWASP
The Open Web Application Security Project

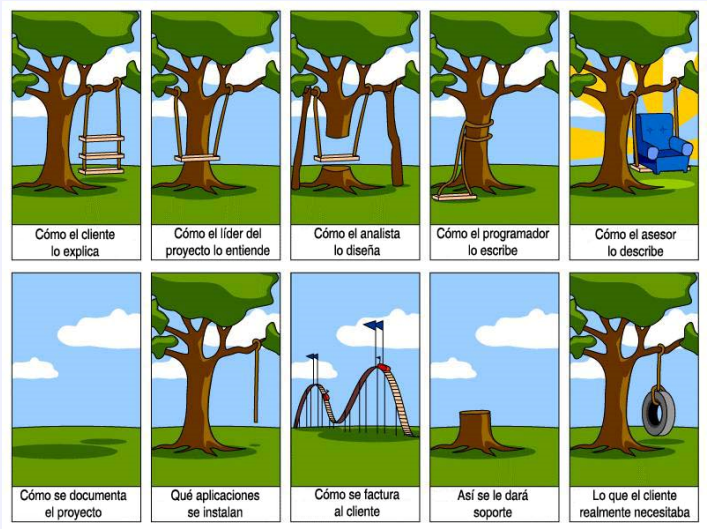
El Desarrollo de Software es una ARTESANIA...

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

Y en Desarrollo de Software abundan los artistas…

La deuda técnica (el problema)

OWASP
The Open Web Application Security Project



La deuda técnica (el problema)

OWASP
The Open Web Application Security Project

Otras industrias lograron estandarizarse…

Que necesita la industria del software?

Agenda

OWASP
The Open Web Application Security Project

- 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

Ingeniería de Software (la solución)

OWASP
The Open Web Application Security Project

La ingeniería de Software.

"Aplicación de un enfoque sistemático, disciplinado y medible al desarrollo, operación y mantenimiento del software".

[IEEE, 1993]

Ingeniería de Software (la solución)

OWASP The Open Web Application Security Project

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

CMMI

ISO/IEC 14598

ISO 9000-3

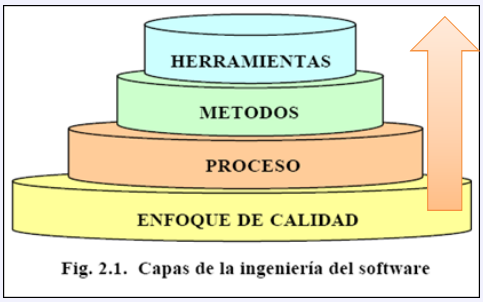


Fig. 2.1. Capas de la ingeniería del software

Agenda

OWASP The Open Web Application Security Project

- 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

El modelo CMMi

OWASP
The Open Web Application Security Project

El modelo SAMM

OWASP
The Open Web Application Security Project

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

Agenda

OWASP
The Open Web Application Security Project

- 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

El modelo SAMM

OWASP
The Open Web Application Security Project

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 ambiguedades 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

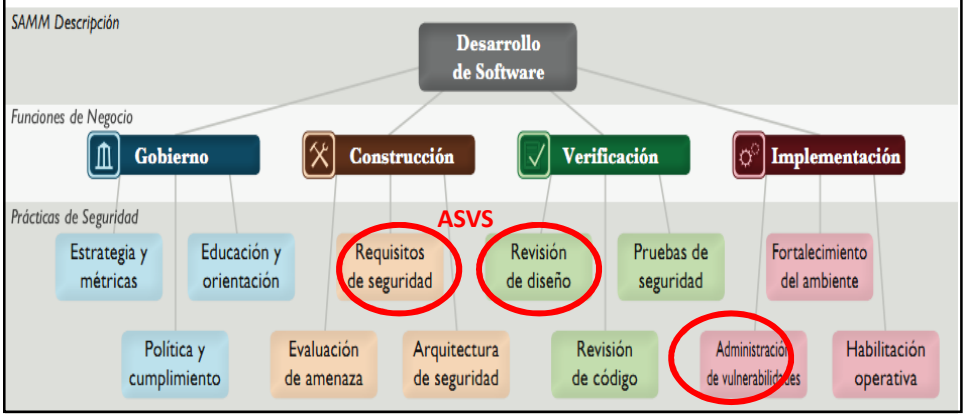
Utilidad de SAMM

- 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.

El modelo SAMM

OWASP
The Open Web Application Security Project

- 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



El modelo SAMM

OWASP
The Open Web Application Security Project

Niveles de Madurez de las Prácticas

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

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

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	Sí/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?		CR 1
✦ ¿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 revisan constantemente los resultados de las revisiones de código?		CR 2
✦ ¿La mayoría de los equipos de proyecto utilizan automatización para comprobar código contra los estándares de programación específicos de la aplicación?		
✦ ¿Las auditorías de rutina del proyecto necesitan lineamientos para los resultados de la revisión de código antes de la liberación?		CR 3

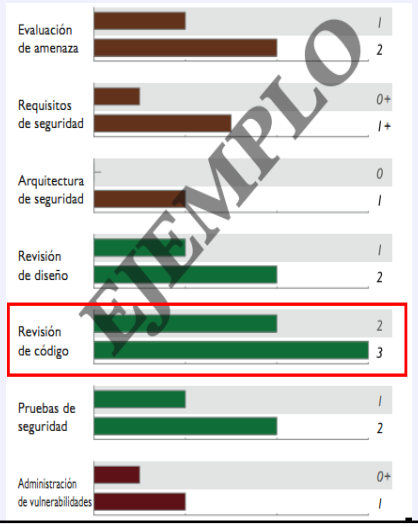
Ejemplo aplicado Evaluar situación actual

OWASP The Open Web Application Security Project

➢Realizar Evaluación
(GAP análisis)

➢SAMM aporta documentos de evaluación para cada "Práctica de Seguridad".

** Recuerde adaptarlos a su realidad**



Ejemplo aplicado Objetivos detallados por nivel madurez

OWASP The Open Web Application Security Project

Por cada Nivel madurez, SAMM define...

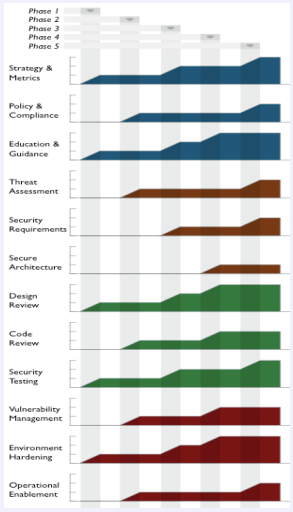
- Objetivo
- Actividades
- Resultados
- Umbrales de satisfacción
- Costos
- Personal
- Niveles relacionados

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

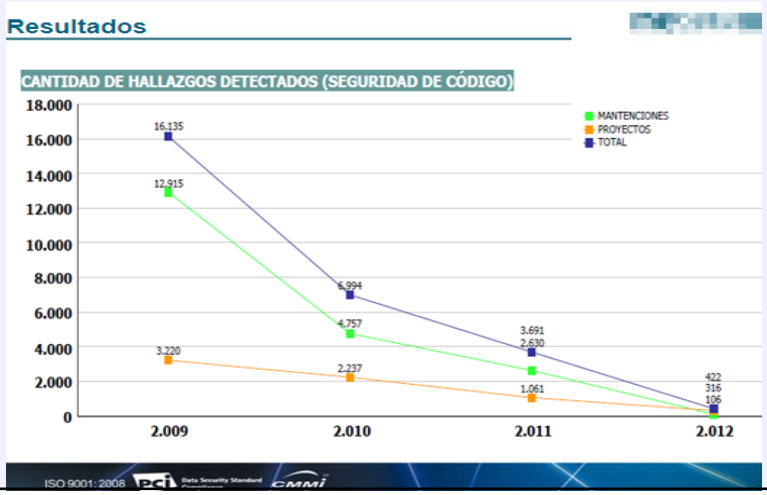
Caso de Exito

CASOS DE EXITO

Caso de Exito

OWASP
The Open Web Application Security Project

Práctica: Revisión de Código



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:

Repaso…

OWASP
The Open Web Application Security Project

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