



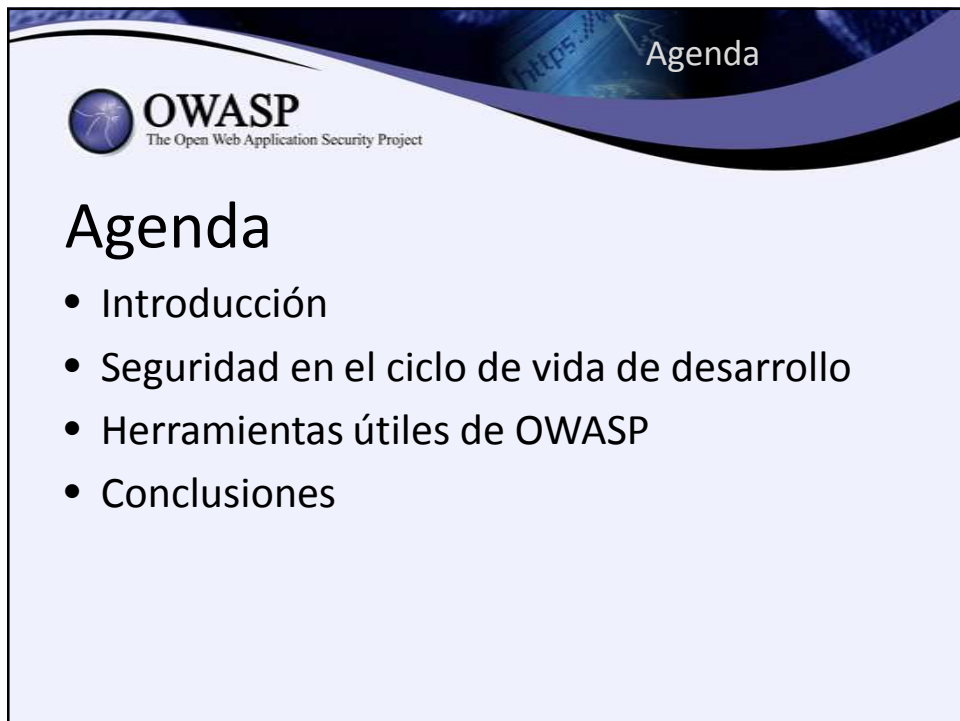
**OWASP Latam Tour
Chile 2013**

Seguridad en el desarrollo

Mateo Martínez, CISSP
mateo.martinez@owasp.org
OWASP Uruguay
Comité Global de Industrias de OWASP

 **OWASP**
The Open Web Application Security Project


 **OWASP**
LATAM TOUR 2013



OWASP
The Open Web Application Security Project

Agenda

- Introducción
- Seguridad en el ciclo de vida de desarrollo
- Herramientas útiles de OWASP
- Conclusiones



OWASP
The Open Web Application Security Project


Una cuestión de prioridades

Prioridades para los programadores:

- Funcionalidades
- Performance
- Usabilidad
- Uptime
- Mantenimiento
- Seguridad

Seguridad == nivel 6 de prioridad

<http://appsandsecurity.blogspot.com/2011/02/security-people-vs-developers.html>
Encuesta realizada a +200 programadores por John Wilander



OWASP
The Open Web Application Security Project

Excusas

Excusas para no implementar seguridad en los desarrollos:

- El cliente no especificó requerimientos de seguridad
- No hay presupuesto asignado para seguridad en el desarrollo
- Tenemos un proceso de auditoría fuerte que encuentra fallas
- El fin del proyecto está cerca y no podemos modificar el código
- El equipo de Testing verifica todo antes de realizar las entregas
- Nuestro software está basado en un framework Open Source
- Tenemos un Firewall y utilizamos SSL.
- Los atacantes solo están interesados en aplicaciones financieras

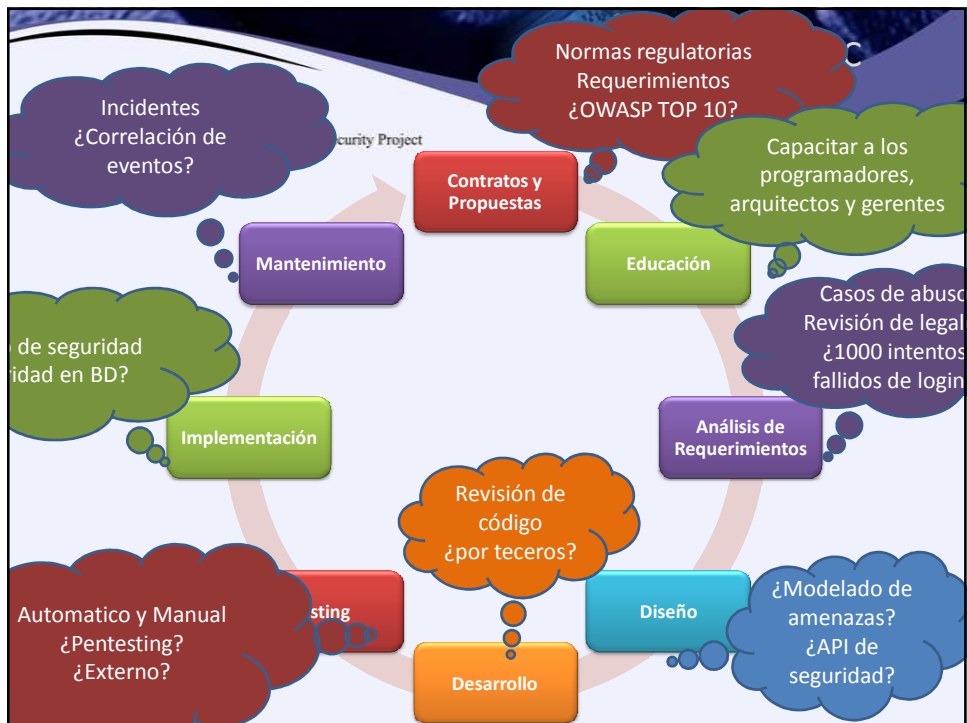
Requerimientos regulatorios




Ejemplo:
PCI DSS – Payment Card Industry Data Security Standard

SDLC

6.3 Desarrollar las aplicaciones (internas y externas incluyendo web) en cumplimiento con PCI DSS y basado en las buenas prácticas de la industria.
Incorporar seguridad de la información en el ciclo de vida del desarrollo de software (SDLC)




Lecciones aprendidas



OWASP
The Open Web Application Security Project

- **Microsoft SDL**
 - Muy pesado, bueno para grandes fábricas independientes
- **Touchpoints**
 - De alto nivel, no es lo suficientemente detallado desde un punto de vista operativo
- **CLASP**
 - Amplia colección de actividades, pero sin asignación de prioridades
- **TODOS:** Buenos para que expertos puedan usarlos como referencia, pero complicado para que gente sin conocimientos de seguridad lo usen como guía




OWASP
The Open Web Application Security Project

**OWASP Secure Coding Practices
Quick Reference Guide
(Ahora en Español! :D)**

https://www.owasp.org/index.php/OWASP_Secure_Coding_Practices_-_Quick_Reference_Guide

Quick Reference Guide



OWASP
The Open Web Application Security Project

Lista de Verificación de Prácticas de Codificación Segura

- Validación de entradas
- Codificación de salidas
- Administración de autenticación y contraseñas
- Administración de sesiones
- Control de Acceso
- Prácticas Critpográficas
- Manejo de errores y Logs
- Protección de datos
- Seguridad en las comunicaciones
- Configuración de los sistemas
- Seguridad de Base de Datos
- Manejo de Archivos
- Manejo de Memoria
- Practicas Generales para la Codificación

Seguridad en el SDLC



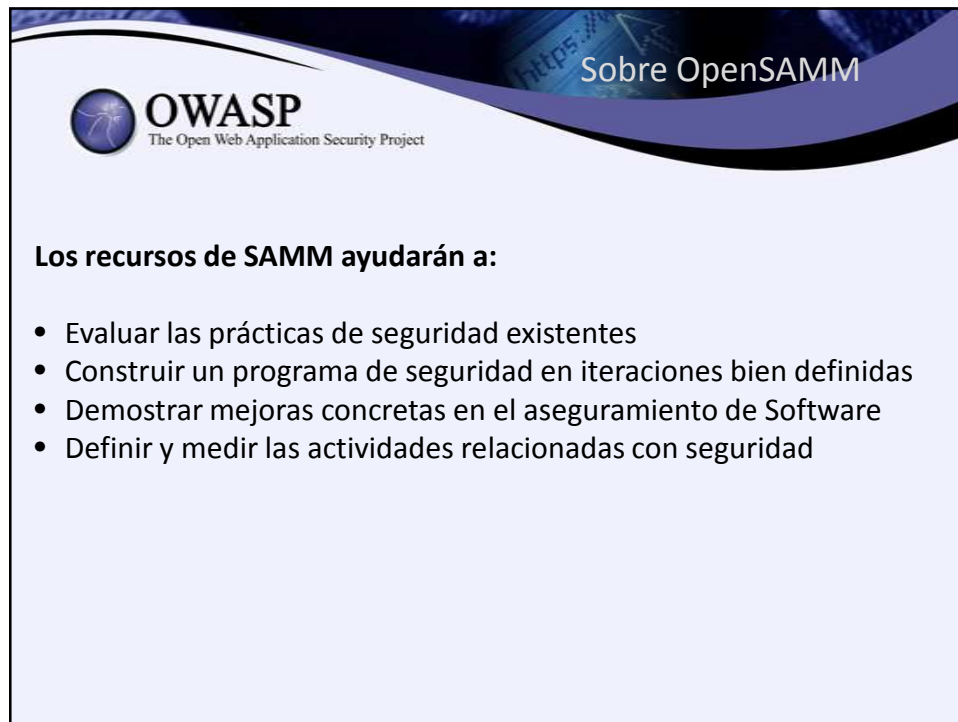
OWASP

SAMM


Software Assurance Maturity Model

OWASP

	Code Crawler	ZAP		
	ESAPI	WebScarab		
OWASP			ESAPI WAF	
Controles	Riesgo	Código	Seguridad	Firewalls
SDLC	Plan	Construir	Test	Implementar
Controles	Política	Concientización	Entrenamiento	
OWASP	ASVS	T10	WebGoat	Swingset

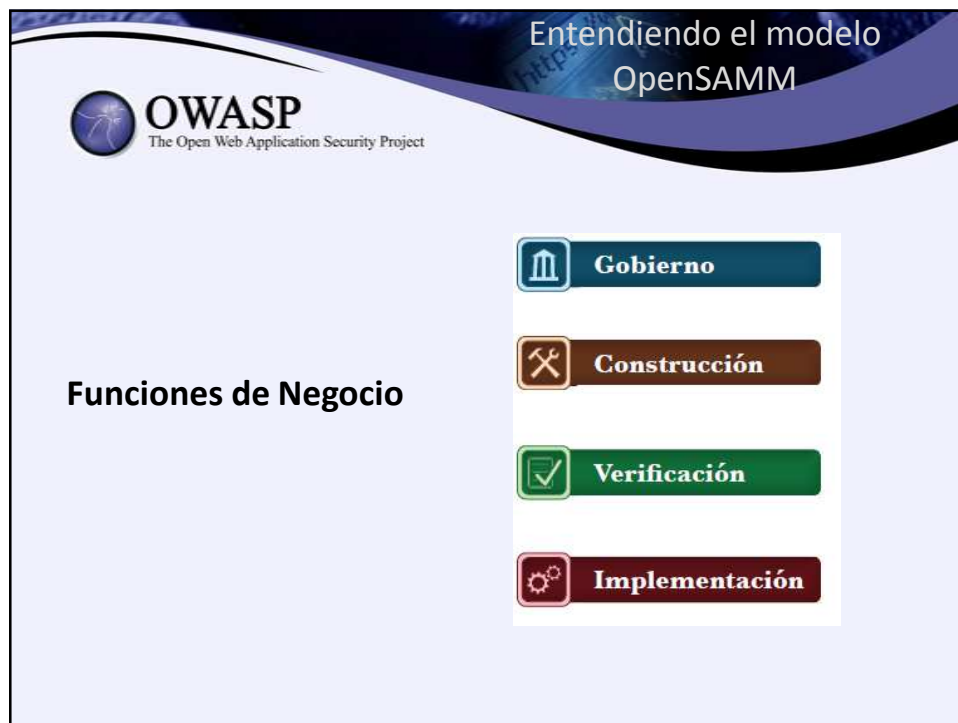


Sobre OpenSAMM


 **OWASP**
The Open Web Application Security Project

Los recursos de SAMM ayudarán a:





- Evaluar las prácticas de seguridad existentes
- Construir un programa de seguridad en iteraciones bien definidas
- Demostrar mejoras concretas en el aseguramiento de Software
- Definir y medir las actividades relacionadas con seguridad



Entendiendo el modelo OpenSAMM

 **OWASP**
The Open Web Application Security Project

Funciones de Negocio

-  **Gobierno**
-  **Construcción**
-  **Verificación**
-  **Implementación**




Ejemplo de SAMM

OWASP
The Open Web Application Security Project

Arquitectura de seguridad

	SA 1	SA 2	SA 3
OBJETIVOS	Insertar consideraciones para lineamientos proactivos de seguridad en el proceso de diseño de software	Dirija el proceso de diseño de software hacia servicios seguros conocidos y diseños seguros desde la concepción	Controlar formalmente el proceso de diseño de software y validar la utilización de componentes de seguridad
ACTIVIDADES	<ul style="list-style-type: none"> A. Mantener una lista de los marcos de trabajo de software recomendados B. Aplicar explícitamente los principios de seguridad para el diseño 	<ul style="list-style-type: none"> A. Identificar y promover los servicios de seguridad e infraestructura B. Identificar los patrones de diseño de seguridad desde la arquitectura 	<ul style="list-style-type: none"> A. Establecer arquitecturas y plataformas formales de referencia B. Validar el uso de marcos de trabajo, patrones, y plataformas
EVALUACIÓN	<ul style="list-style-type: none"> ¿Cuentan los equipos de proyectos con una lista de los componentes de terceros recomendados? ¿Están la mayoría de los equipos de proyecto conscientes de los principios de diseño seguro y su aplicación? 	<ul style="list-style-type: none"> ¿Hace publicidad de los servicios compartidos de seguridad como guía para equipos de proyectos? ¿Están los equipos de proyectos previstos con los patrones de diseño prescriptivo basado en su arquitectura de aplicación? 	<ul style="list-style-type: none"> ¿Están los equipos de proyecto construyendo software a partir de plataformas y marcos de trabajo controlados? ¿Están los equipos de proyecto siendo auditados para el uso de componentes

Entendiendo el modelo OpenSAMM



OWASP
The Open Web Application Security Project

Por cada nivel SAMM define:

- Objetivos
- Actividades
- Resultados
- Umbrales de satisfacción
- Coste
- Personal
- Niveles relacionados

EVALUACIÓN

- ◆ ¿Cuentan los equipos de proyectos con una lista de los componentes de terceros recomendados?
- ◆ ¿Están la mayoría de los equipos de proyecto conscientes de los principios de diseño seguro y su aplicación?

RESULTADOS

- ◆ Prevención ad hoc de las dependencias inesperadas
- ◆ Las partes interesadas son conscientes del incremento de los riesgos de proyecto debido a las bibliotecas y los marcos de trabajo elegidos
- ◆ Se establece un protocolo dentro del desarrollo para la aplicación proactiva de mecanismos de seguridad en el diseño

MÉTRICAS DE ÉXITO

- ◆ >80% del personal de desarrollo informado sobre las recomendaciones de los marcos de trabajo de software durante el pasado año
- ◆ >50% de los proyectos de presentando proactivamente la aplicación de los principios de seguridad para el diseño

Estándares de desarrollo basados en ASVS




OWASP
The Open Web Application Security Project

(OWASP Application Security Verification Standard (ASVS) Project)



ASVS

- Security Architecture Documentation
- Authentication
- Session Management
- Access Control
- Input/Output validation
- Cryptography
- Error Handling & Logging
- Data Protection
- HTTP Security
- Security Configuration



Estándares de desarrollo basados en ASVS


OWASP
The Open Web Application Security Project

Los requerimientos de ASVS fueron desarrollados con los siguientes objetivos en mente:

*Utilizar como una **métrica** – Provee a los desarrolladores y gerentes de aplicaciones con una métrica para determinar el nivel de confianza de las mismas.*

*Utilizar como una **guía** – Provee a los desarrolladores de controles de seguridad con indicaciones en que funcionalidades incluir para cumplimentar con los requerimientos de seguridad.*

*Utilizar **durante adquisiciones** – Provee una base para especificar los requerimientos de seguridad en aplicaciones adquiridas a terceros.*



Codificación Segura ESAPI

OWASP
The Open Web Application Security Project

- OWASP ESAPI (Enterprise Security API) apunta a proveer a los desarrolladores con todos los controles de seguridad necesarios:
 - Estandarizados
 - Centralizados
 - Organizados
 - Integrados
 - Intuitivos
 - Testeados


Codificación Segura ESAPI



OWASP
The Open Web Application Security Project

- Los Toolkits de OWASP Enterprise Security API ayudan a los desarrolladores de software a protegerse de problemas de seguridad relacionados con el diseño o implementación de una aplicación.
- Colección de clases que encapsulan los controles de seguridad mas importantes para una aplicación.
- Existen versiones de Java EE, .Net, Javascript, Classic ASP ColdFusion/CFML, PHP y Python.
- La version de ESAPI para JAVA EE incluye un Web Application Firewall (WAF) que puede ser utilizado mientras los equipos de desarrollo se focalizan en remediar los problemas.
- Todas las versiones de ESAPI se encuentran bajo una licencia BSD de software libre.
- Usted puede modificar o utilizar ESAPI como le parezca. Incluso puede incluirlo en productos comerciales de manera totalmente gratuita.

Codificación Segura – Áreas cubiertas por ESAPI



OWASP
The Open Web Application Security Project

Custom Enterprise Web Application


Enterprise Security API

Authenticator	User	AccessController	AccessReferenceMap	Validator	Encoder	HTTPUtilities	Encryptor	EncryptedProperties	Randomizer	Exception Handling	Logger	IntrusionDetector	SecurityConfiguration
---------------	------	------------------	--------------------	-----------	---------	---------------	-----------	---------------------	------------	--------------------	--------	-------------------	-----------------------

Existing Enterprise Security Services/Libraries

Existen mas de 120 métodos disponibles

Conclusiones



OWASP
The Open Web Application Security Project

- Una Guía inicial con la **“Quick Reference Guide”**
- Implementar seguridad en el SDLC
 - **OWASP CLASP Project**
 - **OpenSAMM**
- Estándar de desarrollo seguro → **OWASP Development Guide Project**
- Utilizar librerías de seguridad → **OWASP Enterprise Security API (ESAPI)**
- Verificar los controles → **OWASP Application Security Verification Standard (ASVS)**
- RFPs y Contratos → **OWASP Legal Project**

Preguntas



OWASP
The Open Web Application Security Project



Mateo Martínez
mateo.martinez@owasp.org