Desarrollo Seguro: Principios y Buenas Prácticas

Por Cesar R. Cuenca Díaz

@ccuencad

OWASP

The Open Web Application Security Project

OWASP
The Open Web Application Security Project

Acerca del Expositor…

Licenciado en Informática – UMSA, ACE – AccessData Examiner, CISO – Certified Information Security Officer.

Experiencia en Desarrollo, Testing, Pentesting, Ethical Hacking, Test de Penetración, ISO27001, PCI-DSS y COBIT.

Capacitaciones en Desarrollo Seguro dictadas a entidades financieras: Banco Ganadero y Banco Unión.

Actualmente: Administrador de Seguridad Informática Senior, Banco Central de Bolivia.

OWASP
The Open Web Application Security Project

DESARROLLO INSEGURO?, ¿A QUIEN CULPAMOS?

PROGRAMADOR?

HACKER?

ALTA GERENCIA

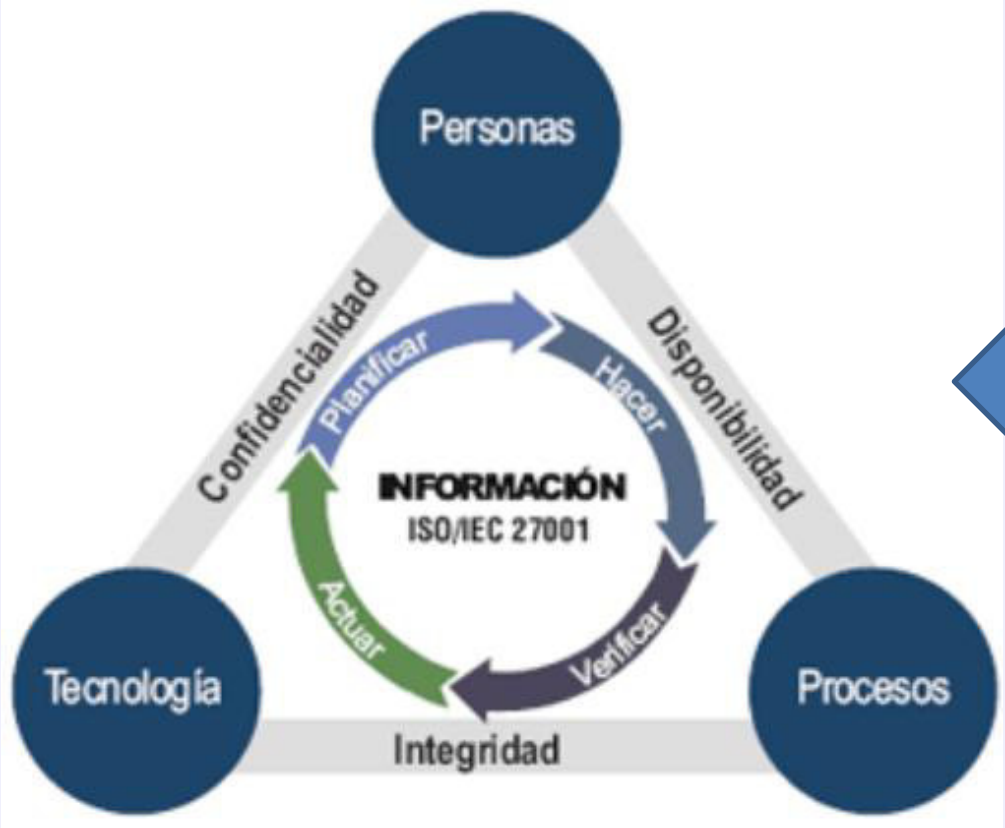
USUARIO FINAL?

OWASP
The Open Web Application Security Project

IDENTIFICANDO AL ENEMIGO

OWASP
The Open Web Application Security Project

COMO ASEGURAMOS LAS APLICACIONES?



"Bien hecho, Chang. La muralla ya no es tan grandiosa si olvidas cerrar la puerta."

OWASP
The Open Web Application Security Project

QUE ES SEGURIDAD EN APLICACIONES?

Seguridad en Aplicaciones, es el uso de principios y/o buenas practicas de SEGURIDAD durante el ciclo de vida del software (SDLC), pudiendo ser este adquirido o desarrollado.

OWASP
The Open Web Application Security Project

CICLO DE VIDA DE DESARROLLO DE SOFTWARE

Se debe tener en cuenta que mientras los nombres de las varias fases pueden cambiar dependiendo del modelo SDLC usado, cada fase conceptual del arquetipo SDLC será usada para desarrollar la aplicación (es decir, definir, diseñar, desarrollar, implementar, mantener).

OWASP
The Open Web Application Security Project

SI ES TAN SENCILLO PORQUE HAY APLICACIONES INSEGURAS?

Seguridad **VS** Funcionalidad

¿¿¿¿ Calidad != Seguridad ????

OWASP
The Open Web Application Security Project

MUY BIEN, Y CUAL ES EL PRIMER PASO?

El primer paso es, establecer requerimientos y controles de seguridad para el CICLO DE VIDA DE DESARROLLO DE SOFTWARE, los cuales deben ser medibles.

OWASP
The Open Web Application Security Project

FASE DE REQUERIMIENTOS

REQUISITOS
R1. Control de Autenticación
R2. Control de Roles y Privilegios(*)
R3. Requerimientos Orientados al Riesgo
R4. Aprobación de Privilegios

CONTROL DE ROLES Y PRIVILEGIOS(*)

MODULOS DE APLICACIÓN		
ID	MODULO	Descripción
M1	Administración de usuarios	Permite la adición, modificación y eliminación de usuarios.
M2	…..	……
M3	Modulo de Contabilidad	Permite efectuar cierres, balances, libro diario, libro mayor…..
M4	Visor de Pistas de Auditoria	…….

CONTROL DE ROLES Y PRIVILEGIOS(*)

L: Lectura A:Alta B:Baja M:Modificación

MATRIZ DE ROLES																
ID	ROL	M1				M2				M3				M4		
		L	A	B	M	L	A	B	M	L	A	B	M	L	A	B	M
1	Administrador	S	S	S	S	S	S	S	S	N	N	N	N	N	N	N	N
2	Operador									S	S	S	S				
3	Auditor	N	N	N	N	N	N	N	N	N	N	N	N	S	S	S	S
4	Cajero									S	S	N	S				
5	.....																

OWASP
The Open Web Application Security Project

FASE DE ANÁLISIS Y DISEÑO

REQUISITOS
R5. Acceso a Componentes y Administración del sistema.
R6. Pistas de Auditoría
R7. Gestión de Sesiones
R8. Datos Históricos.
R9. Manejo Apropiado de Errores
R10. Separación de Funciones (Segregación)

OWASP
The Open Web Application Security Project

FASE DE IMPLEMENTACIÓN Y CODIFICACIÓN.

REQUISITOS
R12. Aseguramiento del Ambiente de Desarrollo
R13. Elaboración de Documentación Técnica
R14. Codificación Segura (*)
R15. Seguridad en las comunicaciones
R16. Seguridad en promoción a ambientes de producción

OWASP
The Open Web Application Security Project

CODIFICACIÓN SEGURA.

BUENAS PRACTICAS

- Validación de entradas
- Codificación de Salidas.
- Estilo de Programación
- Manejo de Log de Cambios.
- Prácticas Criptográficas
- Manejo de errores y Logs
- Manejo de Archivos.
- Manejo de Memoria.
- Estandarización Y Reutilización de Funciones de Seguridad

OWASP
The Open Web Application Security Project

CODIFICACIÓN SEGURA.

	Validación de Entradas	Validacion de Salidas	Controles Criptograficos	Manejo de Archivos	Manejo de Memoria
Interfaz 1	Aplica	Aplica	Aplica	-	No Aplica
Interfaz 2	-	-	-	Aplica	-
Interfaz 3					

OWASP
The Open Web Application Security Project

FASE DE PRUEBAS.

REQUISITOS
R17 Control de calidad en Controles de Seguridad
R18. Inspección de Código por Fases
R19. Comprobación De Gestión De Configuraciones.
R20. Caja Negra (TOP TEN DE OWASP, Guía de Pruebas)

OWASP
The Open Web Application Security Project

FASE DE MANTENIMIENTO.

REQUISITOS
R20. Aseguramiento basado en RIESGOS.
R21. Pruebas de Seguridad (Caja Blanca y Caja Negra) después de los cambios.

OWASP
The Open Web Application Security Project

CONCLUSIONES.

- El alcance del Desarrollo Seguro incluye al SDLC.

- Se debe estandarizar los controles y requisitos, mediante guías y formularios.

OWASP
The Open Web Application Security Project

CONCLUSIONES.

- La seguridad no es un producto, es una sumatoria de personas, procesos y tecnología.

- Suele ser mas costoso aplicar la seguridad al final y no durante el proceso.


DUDAS O
PREGUNTAS?

OWASP
The Open Web Application Security Project

MUCHAS GRACIAS