OWASP

Open Web Application Security Project

Iniciando en Desarrollo Seguro

¿Por dónde Empezar?

Presentador:

Gabriel Robalino

CPTE, CSWAE

Acerca de mi

- Ingeniero de Software
- 5 años de experiencia en desarrollo
- C/C++, C#, Java, Python
- 3 años en seguridad
- Evaluaciones de Seguridad
- Automatización de procesos

OWASP
Open Web Application Security Project

¿Por qué esta charla?

¡No más lágrimas!

OWASP
Open Web Application Security Project

Situación Actual

INTRODUCCIÓN

Anhelo

"Aplicaciones Seguras ejecutándose sobre Sistemas Seguros en Redes Seguras"

Desafíos

- Las tres restricciones tradicionales
- Ausencia de conocimientos de seguridad
- La seguridad como reflexión tardía
- Controles Técnicos sobre Administrativos
- Seguridad vs “Usabilidad”

¿Cómo enfrentarlo?

Acceso

Riesgo

Integridad

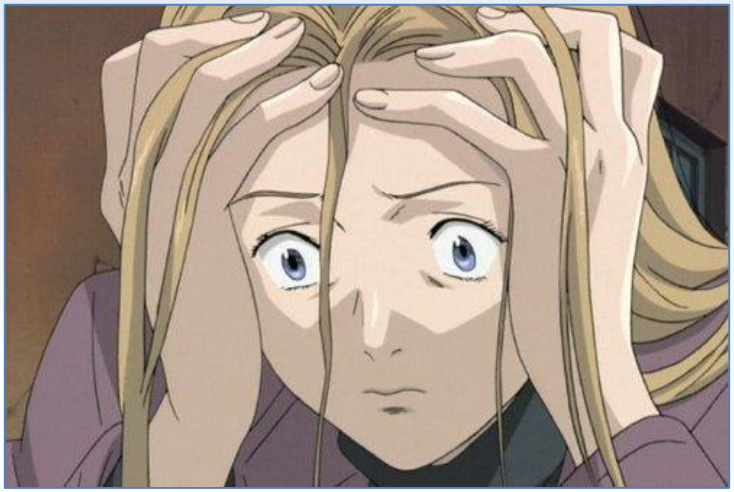
Regulaciones

Alcance

Estándares

SEGURIDAD

Privacidad



Diseño

Metodologías

Amenaza

Cumplimiento

Código Seguro

Vulnerabilidades

Innovación

OWASP
Open Web Application Security Project

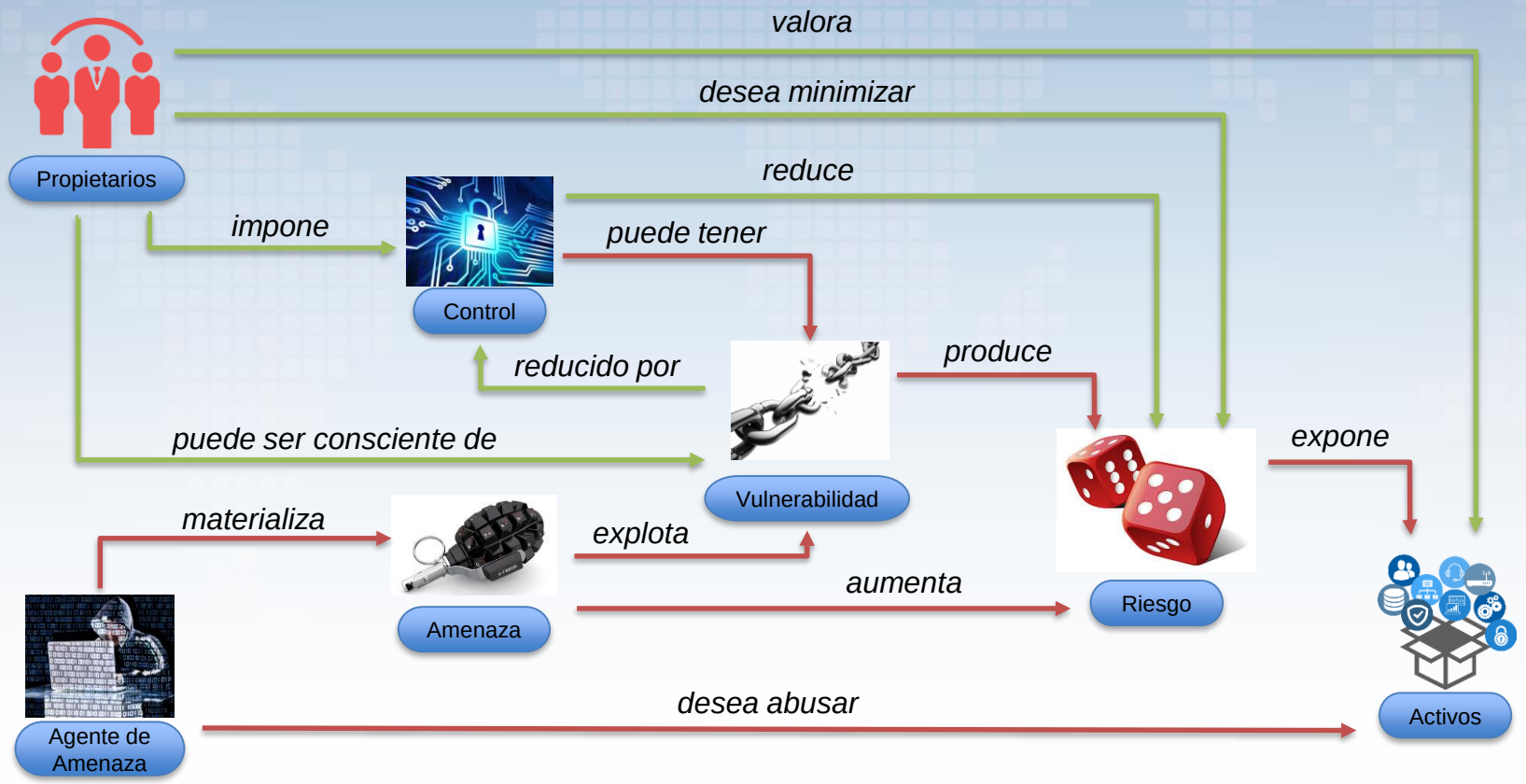
¿Sabemos de seguridad?

ALINEANDO CONCEPTOS

Conceptos de Seguridad

Core	Confidentiality	Integrity	Availability
	Authentication	Authorization	Accountability
Design	Least Privilege	Separation of Duties	Defense in Depth
	Fail Secure	Economy of Mechanisms	Complete Mediation
	Open Design	Least Common Mechanisms	Psychological Acceptability
	Weakest Link	Leveraging Existing Components	

Gestión de Riesgo



ESTÁNDARES DE SEGURIDAD

Estándar NIST

- Desarrolla tecnologías, métodos de medición y normas.
- Mejora calidad y capacidades
- Promueve la innovación
- Documentación
  - Special Publications (SP 800-XX)
  - Federal Information Processing Standards (FIPS)

NIST National Institute of Standards and Technology U.S. Department of Commerce

OWASP Open Web Application Security Project

Estándares ISO

- Estándar Internacional
- Norma productos y servicios
- Aplica a cualquier organización
- Algunas a considerar
  - ISO/IEC 15408 – Common Criteria
  - ISO/IEC 21827 – SSE-CMM
  - ISO/IEC 15504 – SPICE

PCI Standard

- Estándar de Industria
- Protección de datos del tarjetahabiente
  - Almacenar
  - Procesar
  - Transmitir
- Documentación
  - PCI DSS v3.2
  - PA DSS v3.2

METODOLOGÍAS DE ASEGURAMIENTO DE SOFTWARE

Metodologías Tradicionales

Desarrollo Tradicional

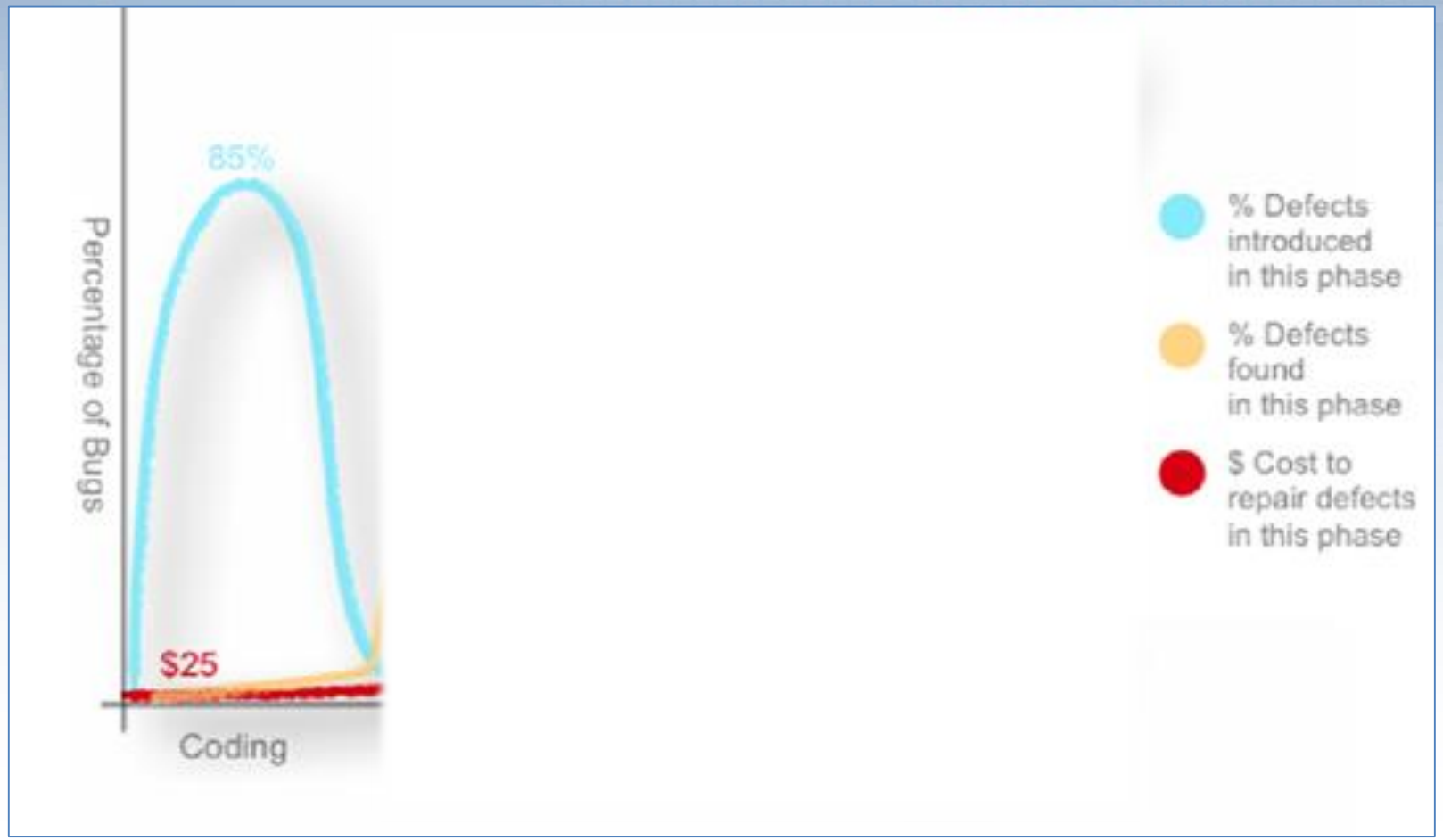
- Modelo Cascada
- Iterativo/Prototipo
- Espiral/Evolutivo

Desarrollo Ágil

- Programación Extrema (XP)
- SCRUM
- Desarrollo Adaptativo

¿Seguridad?

Hitos decisivos



Six Sigma (6σ)

- Estrategia de gestión de negocios
- Mejorar = Eliminación de Defectos
- Defectos son desviaciones de las especificaciones.
- DMAIC (Define, Measure, Analyze, Improve and Control)
- DMADV (Define, Measure, Analyze, Designe and Verify)

NOTA: *Sigue siendo inseguro si no se incluyen requerimientos de seguridad*

Capability Maturity Model Integration (CMMI)

- Mejora de los procesos
- Tres áreas: Development, Delivery and Adquisition
- Cinco niveles de madures:
  - Nivel 1 – Inicial
  - Nivel 2 – Administrado o Repetible
  - Nivel 3 – Definido
  - Nivel 4 – Administrado Cuantitativamente
  - Nivel 5 - Optimizado

Operationally Critical Threat Asset and Vulnerabiliy Evaluation (OCTAVE®)

Otras Metodologías

STRIDE

- Modelamiento de Amenaza
  - **S**poofing
  - **T**ampering
  - **R**epudiation
  - **I**nformation Disclosure
  - **D**enial of Service
  - **E**levation of Privilege

DREAD

- Clasificación de Riesgo
  - **D**amage potencial
  - **R**eproducibility
  - **E**xploitability
  - **A**ffected users
  - **D**iscoverability

Open Web Application Security Project (OWASP)

BUENAS PRÁCTICAS

Open Web Application Security Proyect (OWASP)

OWASP Top 10 - us)	O – 2017 (New)
A1 – Injection	A1 –
A2 – Broken Authentication and S	and Session Management
A3 – Cross-Site Scripting (XSS)	g (XSS)
A4 – Insecure Direct Object References - Me	ss Control (Original category in 2003/2004)
A5 – Security Misconfiguration	Misconfiguration
A6 – Sensitive Data Exposure	Exposure
A7 – Missing Function Level Access C	rotection (NEW)
A8 – Cross-Site Request Forgery	ry (CSRF)
A9 – Using Components wi	A9 – n Vulnerabilities
A10 – Unvalidated Redirects an ed	A10 – Unde W)

Open Web Application Security Proyect (OWASP)

- OWASP Testing Guide
- OWASP Development Guide
- OWASP Code Review Guide
- Estándar de verificación de seguridad (ASVS)
- APIs de Seguridad
- Analizadores de vulnerabilidades
- Laboratorio de Entrenamiento
- Talleres de Seguridad
- OWASP TOP 10 (Web and Mobile)

En resumen

- Conocer conceptos claves de seguridad
- Contar con una metodología de aseguramiento*
- Requerimientos de Seguridad y Negocio unificados
- Adoptar buenas prácticas
- Aprovechar las herramientas públicas
  - OWASP
  - SAMM
  - BSIMM

GRACIAS…