Métricas para la Seguridad de las Aplicaciones

MAI. Andrés Casas

CISSP - CISA - CISM - CRISC - ITIL - COBIT

Deloitte & Touche, S.A.

OWASP

The Open Web Application Security Project

Expositor

OWASP
The Open Web Application Security Project

MAI. Andrés Casas, Director de Gestión de Riesgo de Deloitte,

Dirige la Implementación de Gobierno de Tecnología, Aseguramiento y Seguridad de la Información para Costa Rica, Nicaragua, Honduras y República Dominicana.

Certificaciones

CISSP, CISA, CISM, CRISC, ITIL, COBIT, ISO 27001, MAI

Experiencia

Más de ocho años en Servicios de Análisis de Riesgos a las Empresas, Aseguramiento de Controles, Diseño de Sistemas de Control Interno, Auditoría Interna de tecnología de la información, Seguridad y Privacidad

Deloitte.

Agenda

- ¿Qué es esto?
- ¿De qué me sirve?
- ¿Qué proceso de administración implemento?
- ¿Cuáles métricas existen?

¿Qué es esto?

OWASP
The Open Web Application Security Project

- Medidas

- Métricas

- KPI

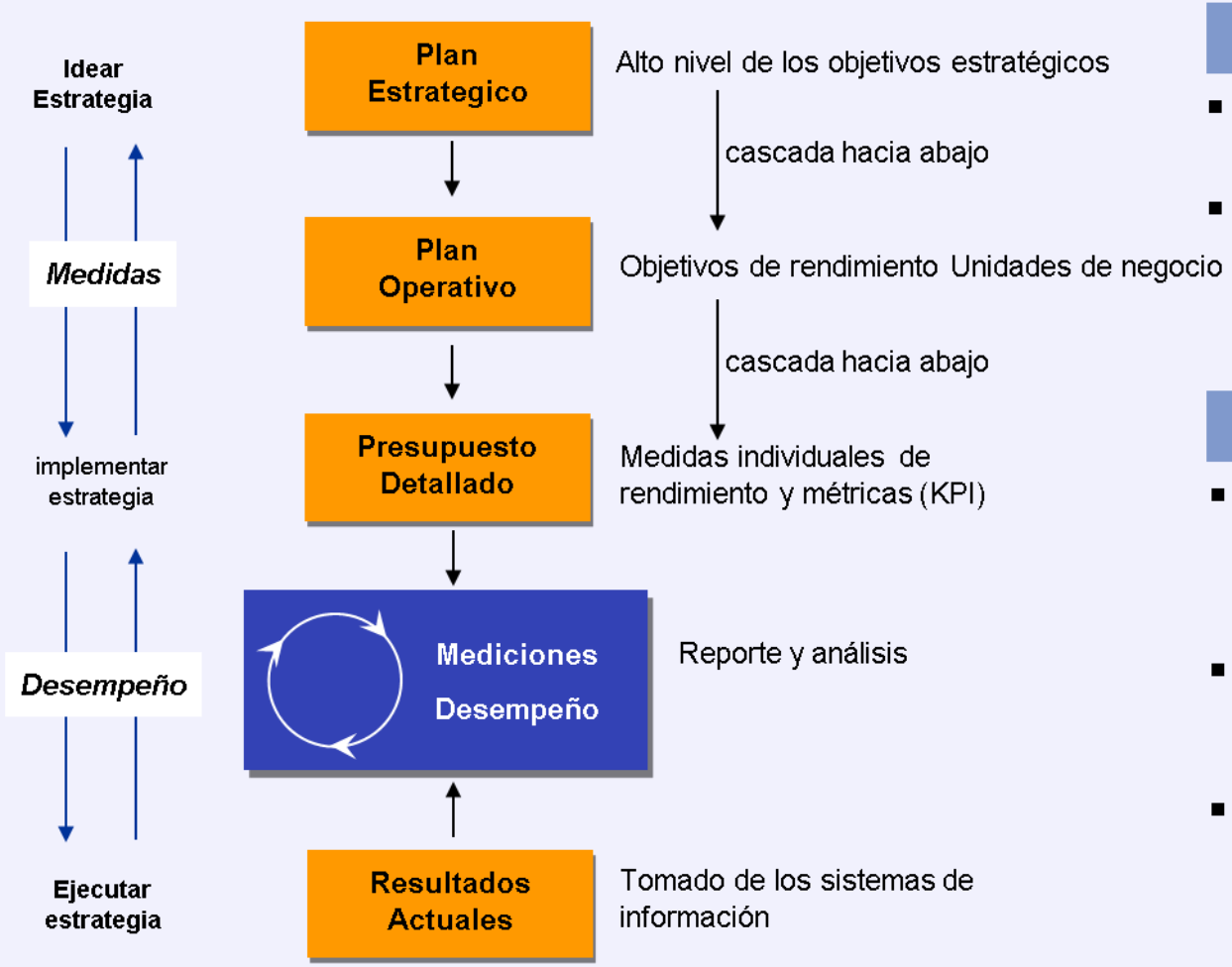
¿De qué me sirve?

- Incrementar la rendición de cuentas
  - Activos frente a la responsabilidad
- Mejorar la efectividad de la seguridad de la información
- Demostrar cumplimiento
  - Leyes
  - Buenas prácticas
- Proporcionar insumos cuantificables para las decisiones

¿Qué proceso de administración implemento?

OWASP
The Open Web Application Security Project

Metrics Framework



Enfoque

- Enfoque en cascada global a individual
- Definir indicadores clave de rendimiento (KPI) para medir el éxito en la ejecución de la estrategia

Factores Críticos de Éxito

- Identificar medidas que promuevan un enfoque en la estrategia de las empresas y los conductores de valor.
- La definición y despliegue de las medidas para construir un modelo de gestión del rendimiento.
- La alineación de los sistemas de información, incentivos y el modelo de gestión del rendimiento.

¿Qué proceso de administración implemento?

OWASP
The Open Web Application Security Project

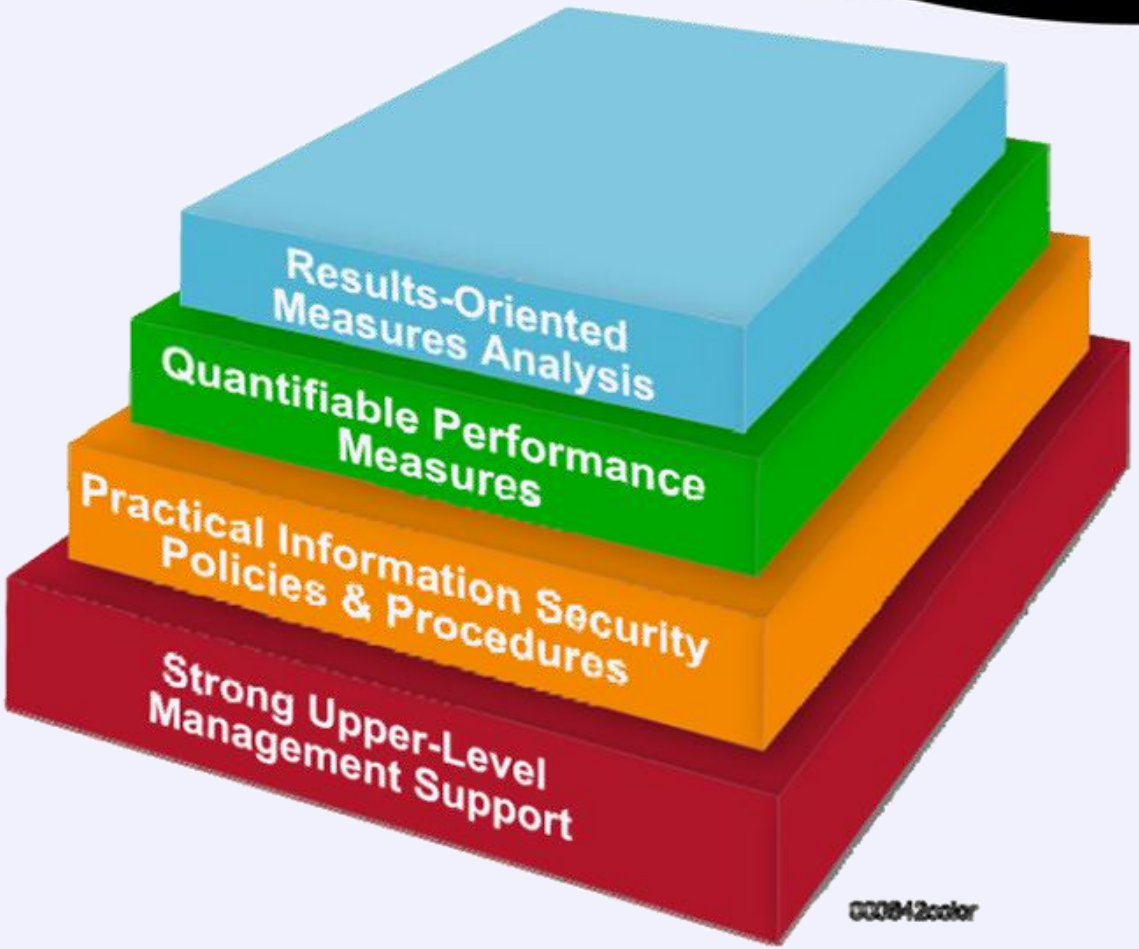
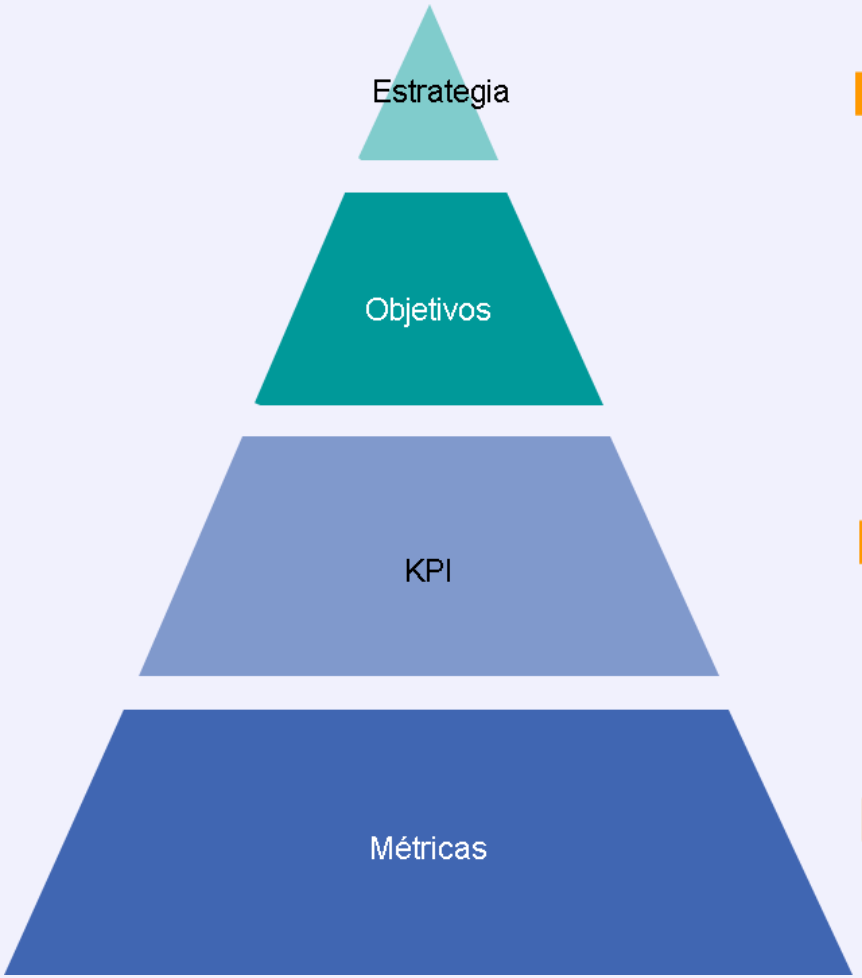


Figure 1-1. Information Security Measurement Program Structure

¿Qué proceso de administración implemento?



- El conjunto de iniciativas y actividades, guiado por la visión de la organización y los valores, que tiene como objetivo proporcionar a la empresa una ventaja competitiva

- Un conjunto de objetivos derivados de la estrategia general, que pueden ser seguidos y controlados a través de indicadores clave de rendimiento

- Una "vara de medir" que proporciona una evaluación de los resultados de un proceso
- Consta de las medidas pertinentes y métricas, y deben estar vinculados a los factores necesarios para el éxito (es decir, los objetivos)

- El rendimiento real medida por los datos cuantitativos

Qué proceso de administración implemento?

Las métricas son más valiosos cuando se cumplen ciertos criterios.

Dependiente del proceso	▪ Las métricas deben ser derivadas del resultado de procesos específicos para garantizar que sean relevantes y se pueden obtener fácilmente y repetir
Confiable	▪ Los datos utilizados en las mediciones no deben ser "arbitrarios" , deben reflejar la información precisa y verificable
Cuantificable	▪ Las métricas deben ser concretas en oposición a conceptuales, deben ser medibles y fácilmente expresadas unidades relevantes.
En curso y comparable	▪ Deben proporcionar información que sea comparable y relevante a través de períodos, en lugar de ser indicadores de rendimiento "una vez"
Relacionado a los objetivos	▪ Deben proporcionar información que pueda estar relacionada con y que apoyen los objetivos adecuados de la empresa

Qué proceso de administración implemento?

Las métricas son más valiosos cuando se cumplen ciertos criterios.

S	Específicas
M	Medibles
A	Acordadas
R	Realistas
T	Con límite de tiempo

Qué proceso de administración implemento?

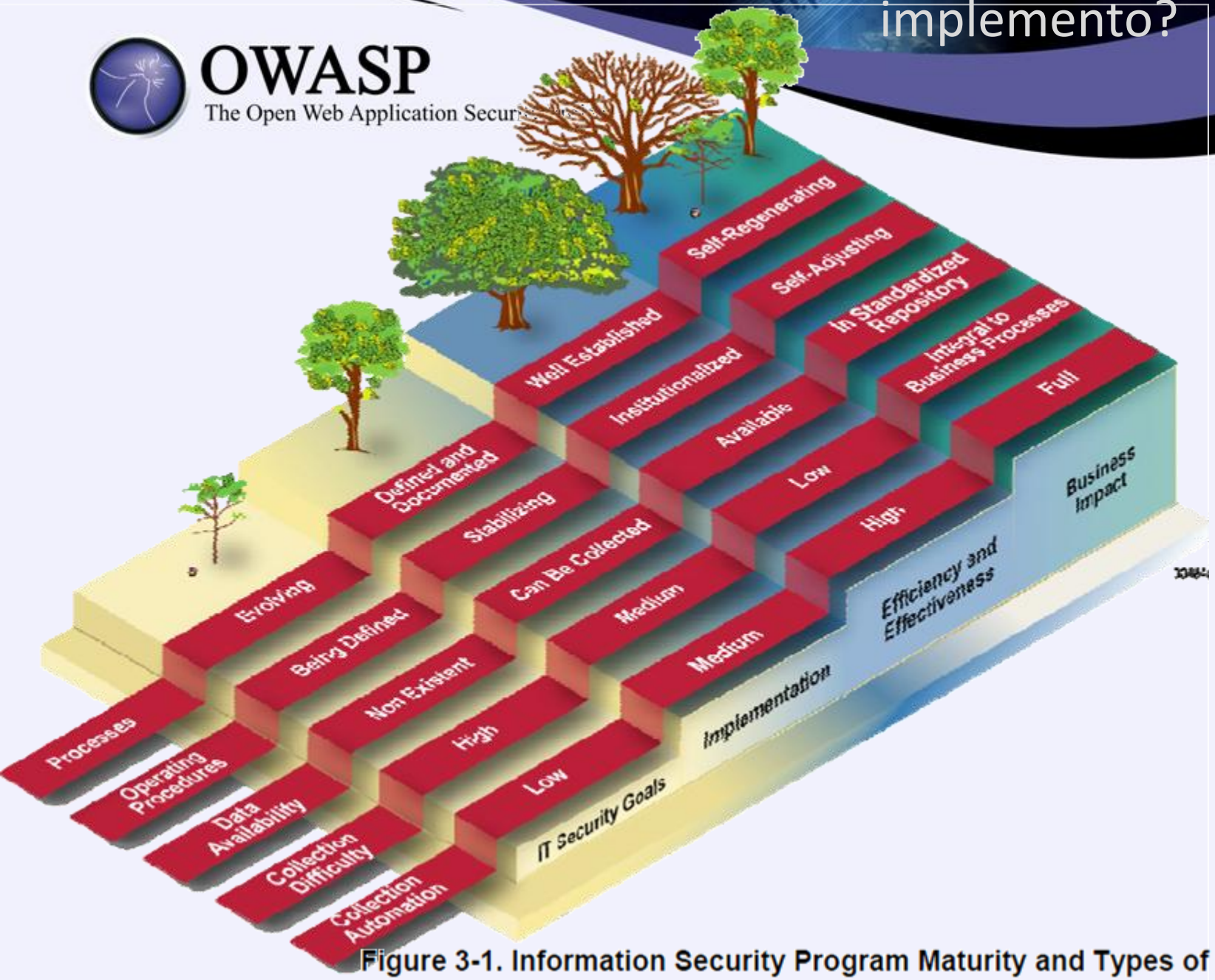


Figure 3-1. Information Security Program Maturity and Types of Measurement

Qué proceso de administración implemento?

1. Alcance	2. Reunir & Evaluar	3. Analizar & Construir	4. Validar & Revisar	5. Finalizar & Aprovar
Key Activities				
▪ Definir y acordar el alcance ▪ Desarrollar un plan detallado del proyecto ▪ Definir las partes interesadas ▪ Invitar a las partes interesadas a los talleres ▪ Reúna la documentación de las actuales estrategias de las empresas, las iniciativas y la información actual ▪ Desarrollar cuestionarios y otras plantillas de proyecto pertinentes	▪ Recopilar las mejores prácticas externas de expertos en la materia ▪ Crear estado actual de la métrica y la estrategia ▪ Llevar a cabo taller para desarrollar basado en el cliente mapa valor ▪ Evaluar las métricas existentes contra el mapa de valor e identificar las lagunas	▪ Analizar los GAPs existentes con los parámetros recogidos benchmarks ▪ Filtrar principios rectores para el desarrollo de métricas ▪ Construir borrador con la participación de los SME y los principales interesados del negocio ▪ Desarrollar diccionario (definición detallada y cálculos) de métricas	▪ Validar métricas preliminares contra diversos elementos de equilibrio ▪ Asegúrese que las métricas preliminares están alineados con las estrategias empresariales ▪ Acotar la tarjeta de puntuación preliminar ▪ Desarrollar una estrategia integrada de gestión del rendimiento y la hoja de ruta	▪ Obtener la aprobación para las métricas finales en el nivel de las partes interesadas clave ▪ Obtener la aprobación de las normas de datos y hoja de ruta tecnológica ▪ Desarrollar caso de negocio para la implementación
Entregables				
▪ Alcance definido ▪ Lista de interesados ▪ Plan de proyecto detallado ▪ Las plantillas de proyecto	▪ Análisis del estado actual de las métricas ▪ Mapas estratégicos ▪ Sistemas de información actuales	▪ Métricas preliminares ▪ Análisis Gap ▪ Diccionario de métricas	▪ Métricas revisadas ▪ Hoja de ruta	▪ Paquete final de métricasEstrategia de implementación

¿Qué proceso de administración implemento?

OWASP
The Open Web Application Security Project

Qué proceso de administración implemento?

OWASP
The Open Web Application Security Project

Holistic IT Security Management Framework

[EC] Enablers and controlling

- [EC1] Strategy, governance and organization
- [EC2] Policies, standards and compliance
- [EC3] Training and awareness
- [EC4] HR security
- [EC5] Physical security
- [EC6] Effectiveness metrics and reporting

[IM] IT management and supporting processes

- [IM1] IT risk management
- [IM2] Security architecture
- [IM3] Secure engineering
- [IM4] Secure operation
- [IM5] Information and asset management
- [IM6] IT continuity management
- [IM7] Vulnerability management
- [IM8] Extended enterprise security management

[IA] Identity and access management

- [IA1] Identification and authentication
- [IA2] Authorization

[AS] Application security

- [AS1] Secure software development
- [AS2] Application functions and controls

[IS] Infrastructure security

- [IS1] Servers and middleware
- [IS2] User devices
- [IS3] Network and communication

[DS] Data security

- [DS1] Data loss prevention
- [DS2] Media security

¿Qué proceso de administración implemento?

Aplicaciones	Planillas	Segx	Producción	Ventas
Herramienta de Desarrollo	Oracle Forms		Power Builder 8.0	Visual Basic .NET
Software Base Clientes	Windows 2008 Server	Windows NT4 Server		Windows 2003 Server
Bases de Datos	Oracle 11i		SQL Server 8	
Software Base de Servidores	Windows 2008 Server	Windows 2003		Windows 2000 Server
Servidores	SERVER 2008			

¿Qué proceso de administración implemento?

OWASP
The Open Web Application Security Project

Tipos de métricas:

- Métricas en procesos de seguridad
- Métricas de red
- Métricas de software
- Métricas de seguridad del personal

¿Qué proceso de administración implemento?

OWASP
The Open Web Application Security Project

Métricas en procesos de seguridad:

- Medición de los procesos y procedimientos Implica alta utilidad de la seguridad políticas y procesos
- Relación entre indicadores y nivel de seguridad no está claramente definido
- Cumplimiento / Gobierno impulsado generalmente apoya una mayor seguridad
- Impacto real difícil de definir

¿Qué proceso de administración implemento?

Métricas de red:

- Impulsado por productos (firewalls, IDS, etc)
- Disponible
- Ampliamente utilizado
- Brinda una sensación de control
- Gráficos agradables
- Puede ser engañoso

¿Qué proceso de administración implemento?

OWASP
The Open Web Application Security Project

Métricas de software:

- Medidas de software están problemáticos (LOC, FPS, Complejidad etc)
- Dependen del contexto y sensible al entorno
- Dependiente Arquitectura

¿Qué proceso de administración implemento?

Las organizaciones deben documentar su métricas en un formato estándar para asegurar la aplicación del modelo, adaptación, recopilación y presentación de informes.

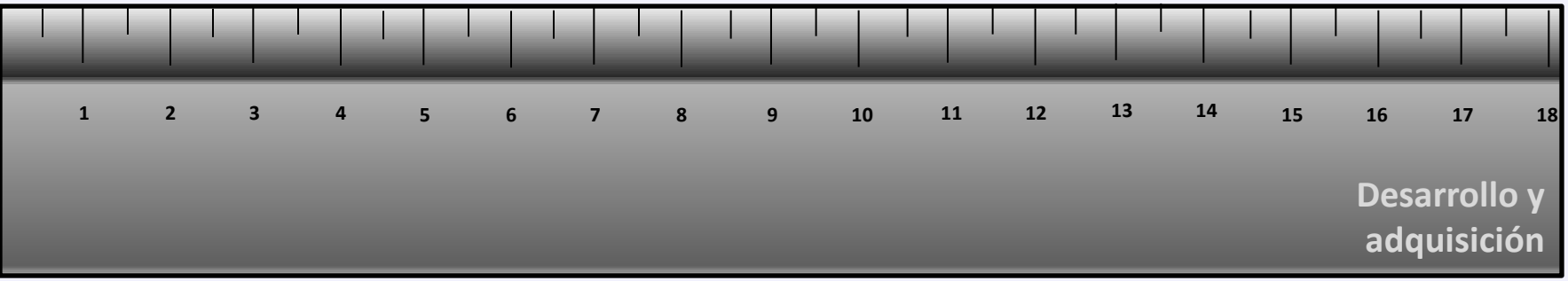
INDICADOR	**PREVENCION CODIGO MALICIOSO**	
OBJETIVO	Mide el nivel de efectividad del proceso de prevención de código malicioso.	
ALCANCE	Todos los intentos de infección detectados durante el período.	
COMENTARIOS, EJEMPLOS Y TIPOS DE MEDICION		
DATOS		
Logs antivirus	Se informa la cantidad de intentos de infección detectados durante el periodo analizado.	
	Responsable: Juanito Perez	Origen: DEFINIR ORIGEN DE DATOS
	Frecuencia: Mensual	
METODO DE CALCULO		**META**
Infecciones no detenidas por el antivirus / Todos los intentos de infección registrados		Normal >90% Seguimiento <=90%

Métricas SDLC

% defectos que impactan seguridad

% requerimientos de seguridad mapeados

desviaciones entre diseño, código y requerimientos



puntos de entrada para cada módulo

vulnerabilidades de software conocidas

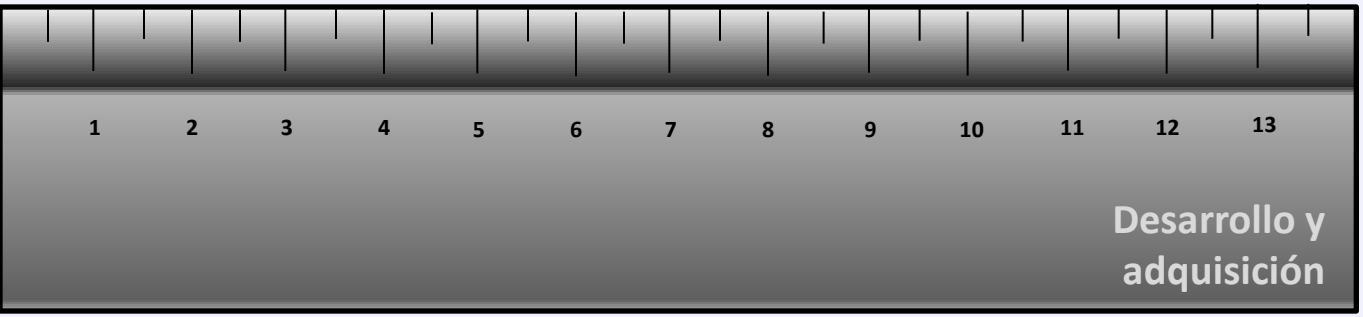
Métricas SDLC

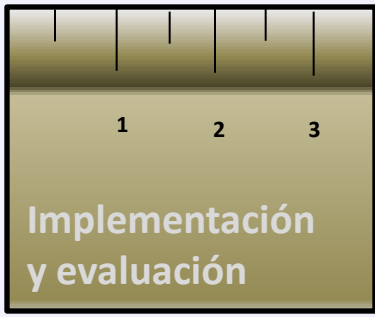
OWASP
The Open Web Application Security Project

defectos en código según su componente

% variación de costo o presupuesto en actividades de seguridad

% controles de seguridad fallidos





% vulnerabilidades que han sido mitigadas

% módulos que contienen vulnerabilidades

Métricas de calidad

Correctitud

Grado de operación del programa respecto los requerimientos

- Defectos KLOC
- Horas por interrupción del programa

Mantenibilidad

Grado que un programa puede cambiar

- Costo de corregir
- Tiempo para realizar cambios

Integridad

Grado de resistencia ante pérdida de información

- Tolerancia de fallos
- Ataques registrados contra el programa

Usabilidad

Grado de facilidad de uso

- Tiempo de entrenamiento
- Conocimientos necesarios para operar el programa

¿Qué proceso de administración implemento?

OWASP
The Open Web Application Security Project

Software Facts

Expected Number of Users 15
Typical Roles per Instance 4

Amount Per Serving

Modules 155 Modules from Libraries 120

	% Vulnerability*
Cross Site Scripting 22	**65%**
Reflected 12	**15%**
Stored 10	
SQL Injection 2	**10%**
Buffer Overflow 5	**95%**
Total Security Mechanisms 3	**10%**
Modularity .035	**0%**
Cyclomatic Complexity 323	
Encryption 3	
Authentication 15	4%
Access Control 3	2%
Input Validation 233	20%
Logging 33	4%

* % Vulnerability values are based on typical use scenarios for this product. Your Vulnerability Values may be higher or lower depending on your software security needs:

	Usage	Intranet	Internet
Cross Site Scripting	Less Than	10	5
Reflected	Less Than	10	5
Stored	Less Than	10	5
SQL Injection	Less Than	20	2
Buffer Overflow	Less Than	20	2
Security Mechanisms		10	14
Encryption		3	15

OWASP
The Open Web Application Security Project

¿PREGUNTAS?