Seguridad y Competencias Profesionales
Tema 10: Metolodogías de verificación
Curso 2012–2013

Ingeniería en Informática (2° ciclo)

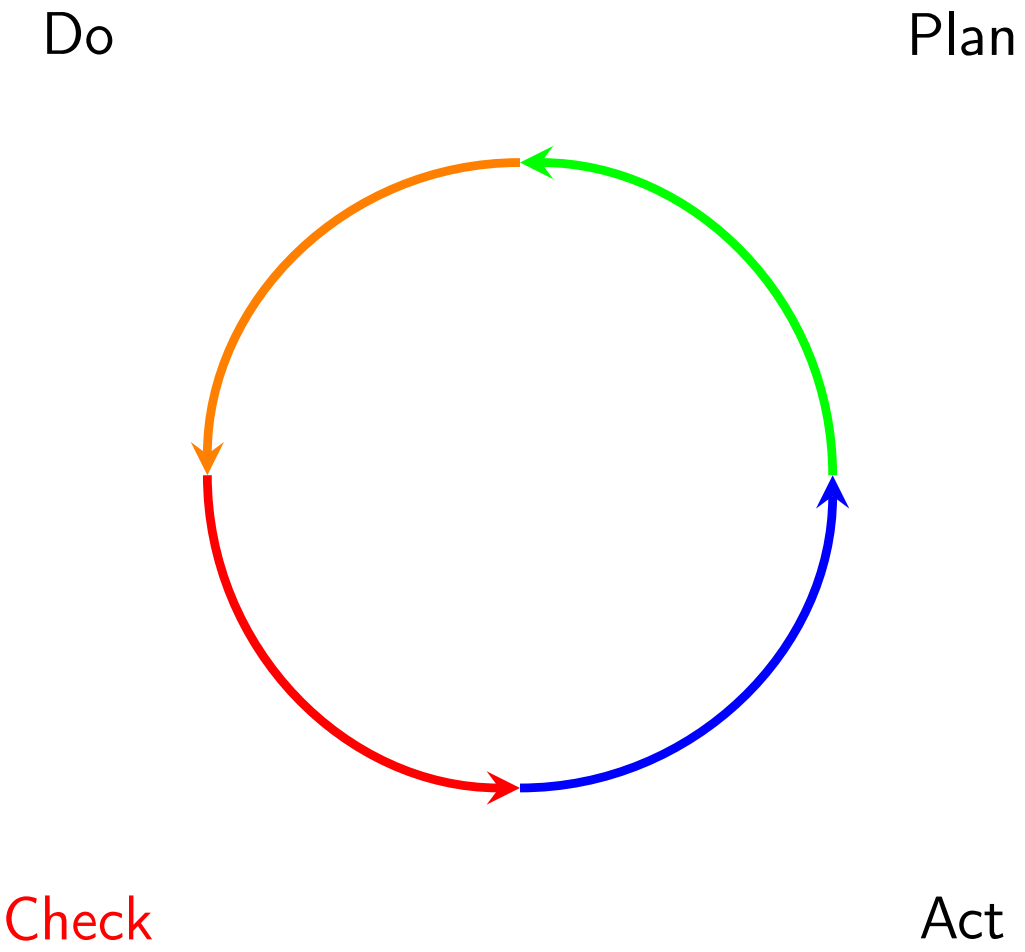
Departamento de Ingeniería Informática
Universidad de Cádiz

Cádiz, 14 enero 2013

Índice

Índice

Repaso del ciclo PDCA



Situaciones para verificación

Sobre organizaciones completas: OSSTMM

- Dentro de la misma organización puede haber presiones y malos hábitos que impiden darse cuenta de problemas
- Lo ideal es llamar a una entidad externa neutral que ayude a identificar los problemas $\rightarrow$ una auditoría
- La auditoría solo dice *qué* hay que revisar

Sobre programas desarrollados: OWASP

- El hecho de encontrar problemas de seguridad y parchearlos no nos asegura que vayamos a tener seguridad («seguridad es un proceso, no un producto»)
- La seguridad se tiene que garantizar, integrándose como otra prueba más del proceso de desarrollo de software

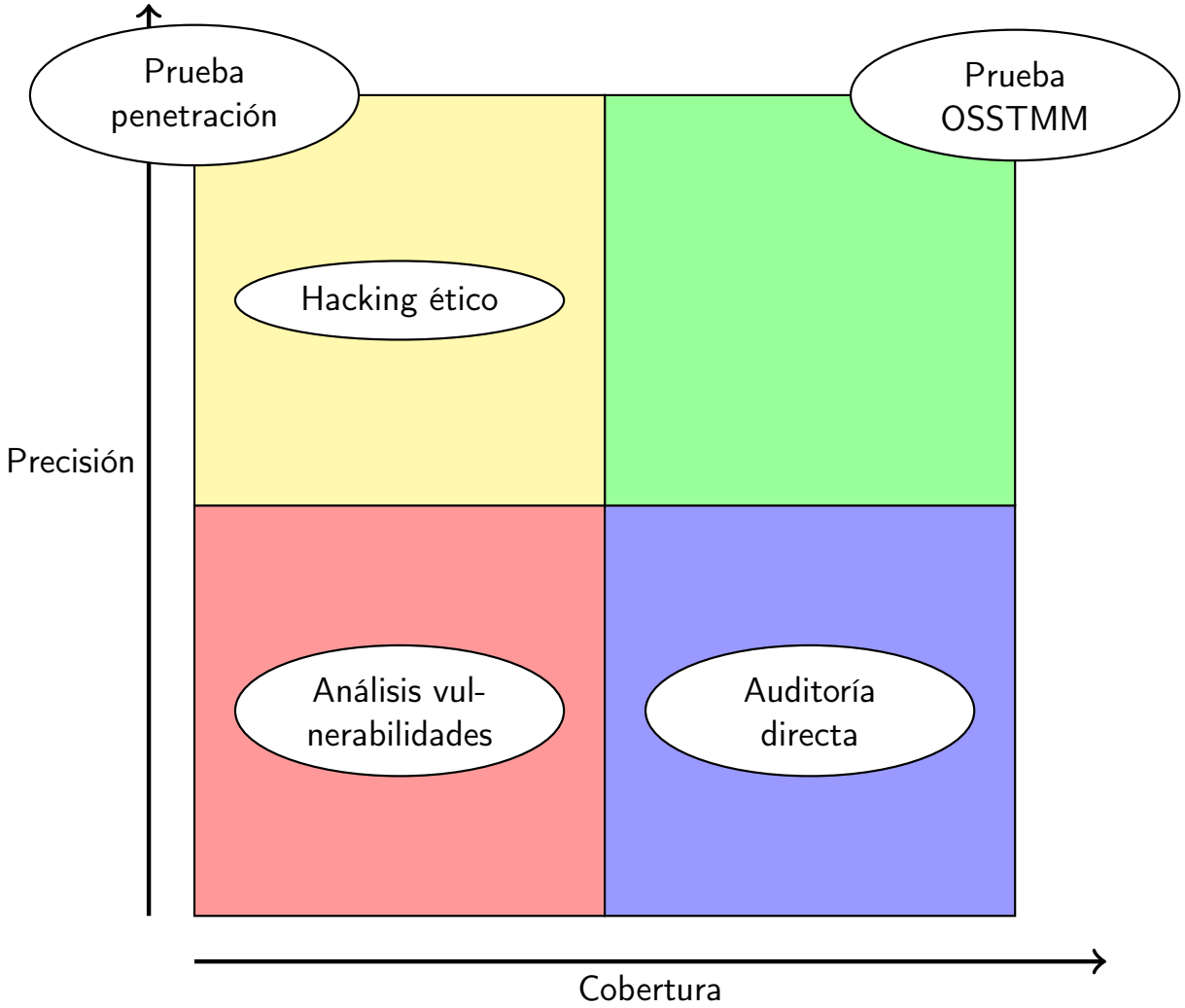
Índice

¿Qué es OSSTMM?

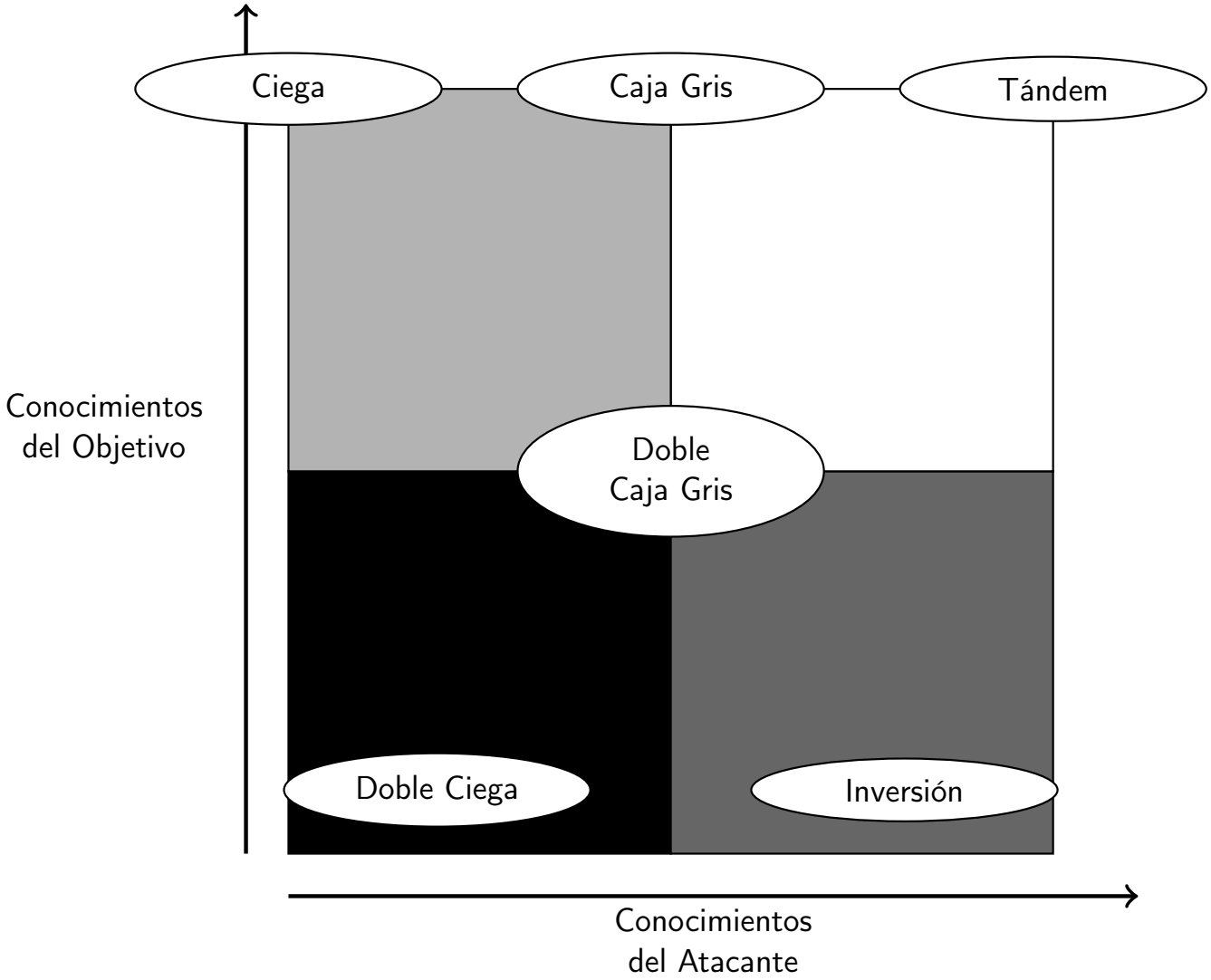
Open Source Security Testing Methodology

- Es una metodología abierta de testeo de seguridad de los sistemas
- Se ha convertido en una referencia estándar en la realización de pruebas técnicas, abarcando un conjunto exhaustivo de tests aplicables a todas las áreas de seguridad lógica de la información
- Su objetivo es auditar un sistema
- Es de alto nivel: indica las tareas, pero no exactamente cómo hacerlas, para ser más longeva (ISSAF puede complementar este aspecto, junto con otras bases de datos)

Tipos de auditorías



Tipos de pruebas de seguridad



Objetivos

- El resultado de aplicar la metodología OSSTM es obtener una plantilla de datos de test de seguridad firmadas por los testeadores, acompañado de todos los informes finales con objeto de obtener una certificación OSSTM.
- Esta plantilla mostrará lo que ha sido testeado de forma completa y lo que no lo ha sido con su justificación.
- Esta plantilla permitirá otorgar a la empresa obtener una certificación OSSTM.

Características

Atributos deseados

- Profundidad completa
- Se incluyen todos los canales
- La realización de las pruebas cumple la ley
- Los resultados son medibles y cuantificables
- Los resultados son consistentes y repetibles
- Los resultados sólo contienen hechos derivados de las pruebas

Estructura

Conceptos

- Entorno de cualquier interacción con cualquiera de los recursos listados en el índice
- Un recurso es algo de valor para el dueño, sea tangible o intangible: oro, información, una banda de frecuencias, etc.
- Cada medio de interacción es un canal, cuya seguridad se evalúa en una o más secciones, que se divide en 17 módulos

Canales y secciones

PHYSSEC	Seguridad humana y física
COMSEC	Seguridad de las redes y telecomunicaciones
SPECSEC	Seguridad del espectro