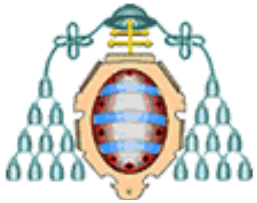
Calidad y testing del software. Aspectos esenciales para la seguridad

ISO/IEC/IEEE 29119 Software Testing

Javier Tuya (giis.uniovi.es)

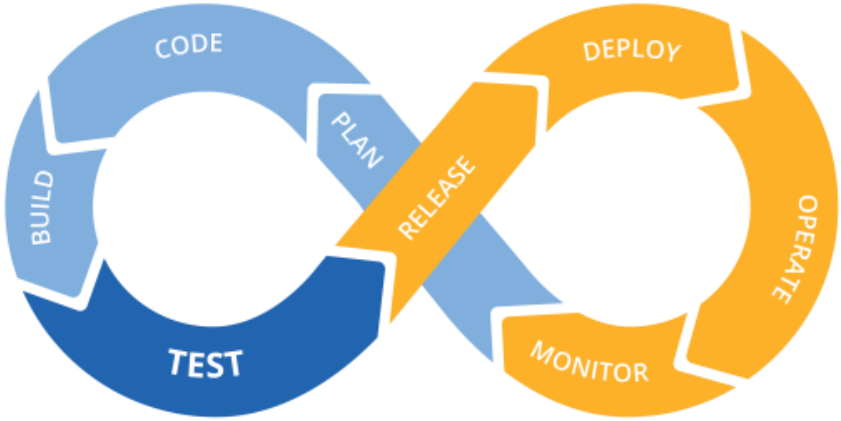
Grupo de Investigacion en Ingeniería del Software, Universidad de Oviedo



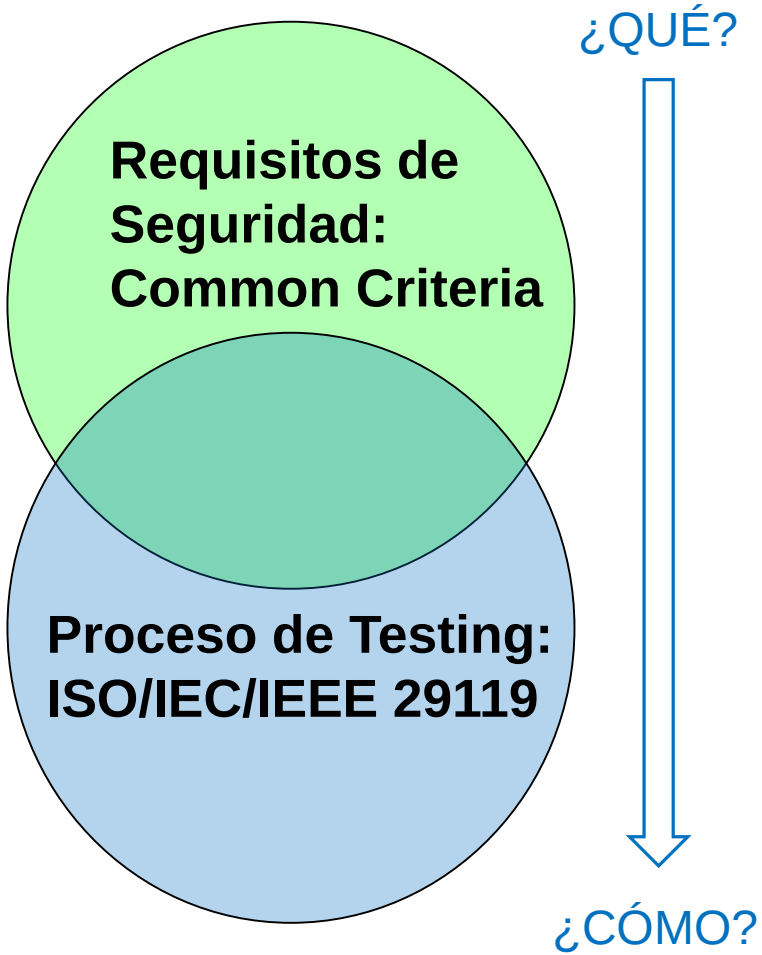
AEN/CTN 71/SC7/GT26 – Ingeniería del Software y Sistemas de Información – Pruebas del Software

Jornada de Ciberseguridad Corporativa, Gijón, 16 de Marzo de 2017

Agenda



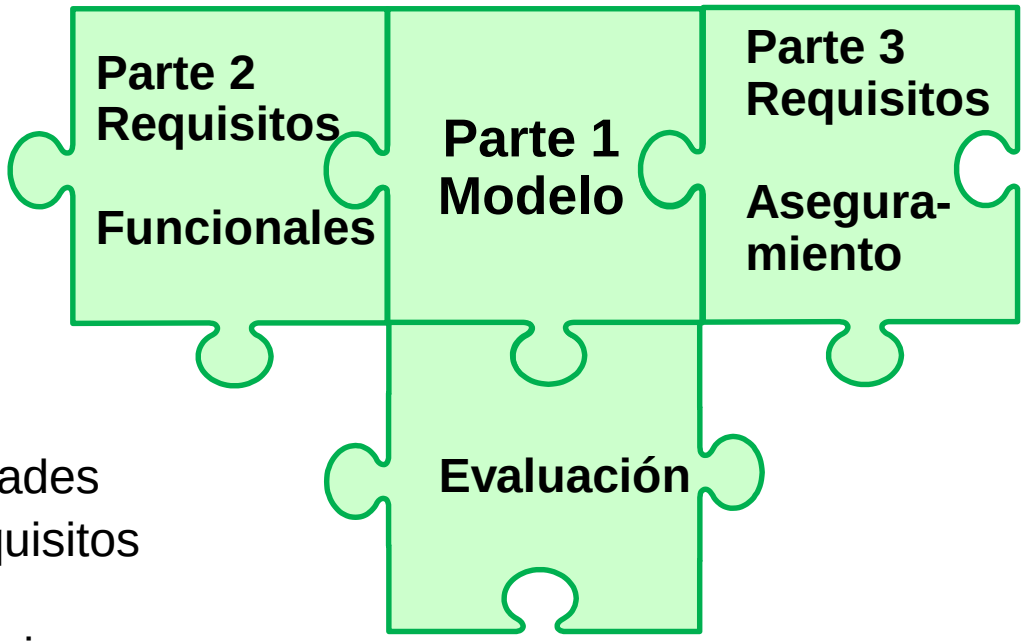
“In Vitro” “In Vivo”



THE CARTOON TESTER ON HIS WAY TO EXPOQA

A CONVERSATION WITH A FELLOW PASSANGER TURNS TO TESTING EVEN BEFORE THE PLANE HAS SET OFF!

Common Criteria
for Information Technology Security Evaluation



- Objetivo:
  - Establecer nivel de confianza
  - Compatibilidad entre resultados de evaluaciones independientes de seguridad
- Para:
  - Consumidores: definir necesidades
  - Desarrolladores: identificar requisitos y preparar/asistir evaluaciones
  - Evaluadores: Establecer un juicio sobre la conformidad
- CC Recognition Agreement
  - 17 Authorizing Members. ES: Centro Criptológico Nacional

CC: Requisitos Funcionales

Functional class

FAU: Security Audit
FCO: Communication
FCS: Cryptographic Support
FDP: User Data Protection
FIA: Identification and Authentication
FMT: Security Management
FPR: Privacy
FPT: Protection of the TSF
FRU: Resource Utilisation
FTA: TOE Access
FTP: Trusted Path/Channels

Family – Component – Requirement

FAU_GEN Security audit data generation
FAU_GEN.1 Audit data generation
1.1. *The TSF shall be able to generate an audit record of the following auditable events:*
…
1.2. …
FAU_GEN.2 User identity association
…
FAU_SAA Security Audit Analysis
…

CC: Requisitos de Aseguramiento

Assurance Level

EAL1: functionally tested
EAL2: structurally tested
EAL3: metodically tested and checked
EAL4: metodically designed, tested and reviewed
EAL5: semiformally designed and tested
EAL6 semiformally verified design and tested
EAL7: formally verified design and tested

X

Class – Family – Component

Development …
Guidance documents …
Life-cycle support …
Security target evaluation …
Tests
ATE_COV: **Coverage**
1, 2, 3
ATE_DPT: **Depth** …
ATE_FUN: **Functional tests** …
ATE_IND: **Independent testing**…
Vulnerability assessment …

CC: Componentes por Nivel de Aseguramiento

Assur. Class	Assur. Family	Assur. Comp. by Eval. Assur. Lev						
		1	2	3	4	5	6	7
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
V. A.	AVA_VAN		2	2		4	5	5

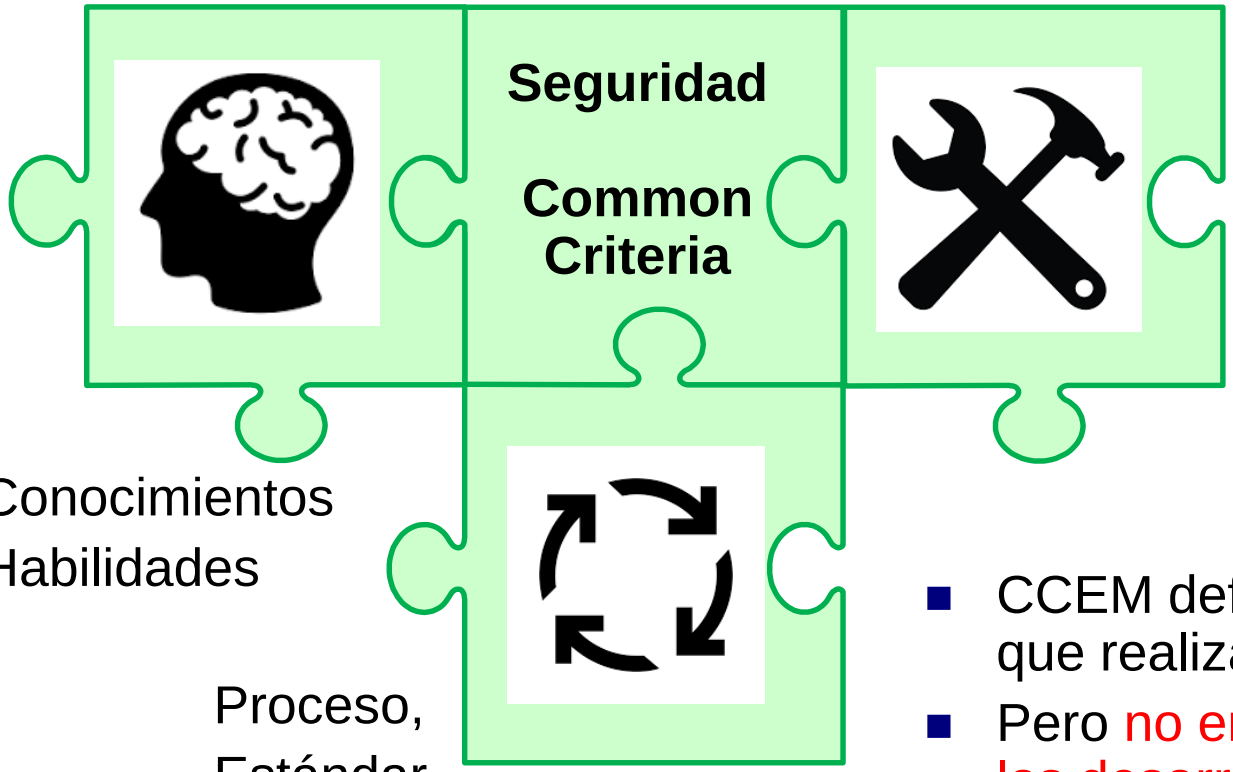
ATE_COV.1.1C *The **evidence of the test coverage** shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification*

ATE_FUN.1.1C *The test documentation shall consist of **test plans, expected test results and actual test results**. ATE_FUN.1.2C The test plans shall **identify the tests** to be performed and **describe the scenarios**…*

ATE_IND.1.2E *The evaluator shall **test a subset** of the TSF to confirm that the TSF operates as specified*

ATE_IND.2.2E *The evaluator shall **execute a sample** of tests in the **test documentation** to verify the developer test results*

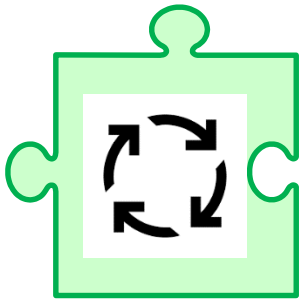
Cómo realizar las pruebas



- CCEM define actividades y tareas que realiza el evaluador
- Pero no entra en detalle de cómo los desarrolladores realizan las actividades de testing y obtienen las evidencias requeridas

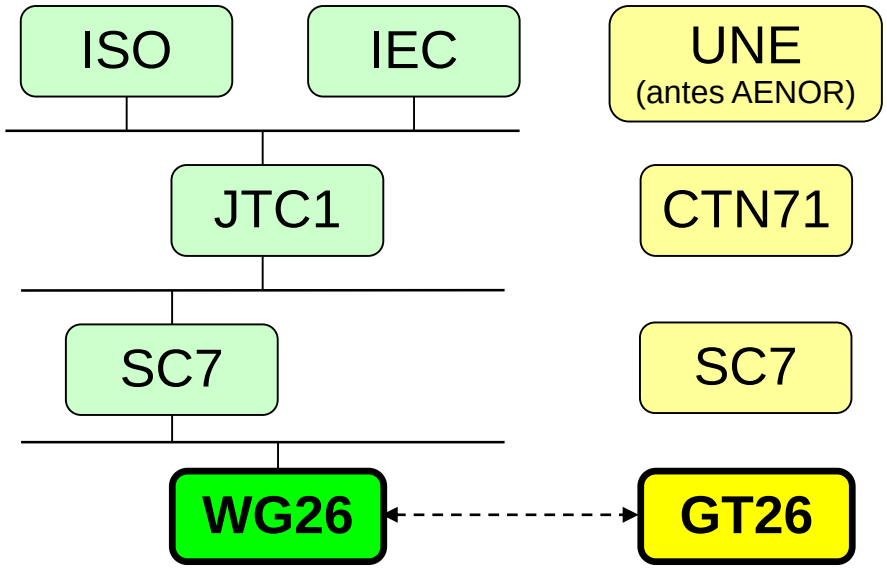
Qué Estándares utilizar

- BS 7925-1, SW Testing: Part 1-Vocabulary
- BS 7925-2, SW Testing: Part 2-Software Comp. Testing
- IEEE Std 829, Software Test Documentation
- IEEE Std 1008, Software Unit Testing
- Estándares generales: ISO/IEC 12207, 15289
- Estándares sectoriales



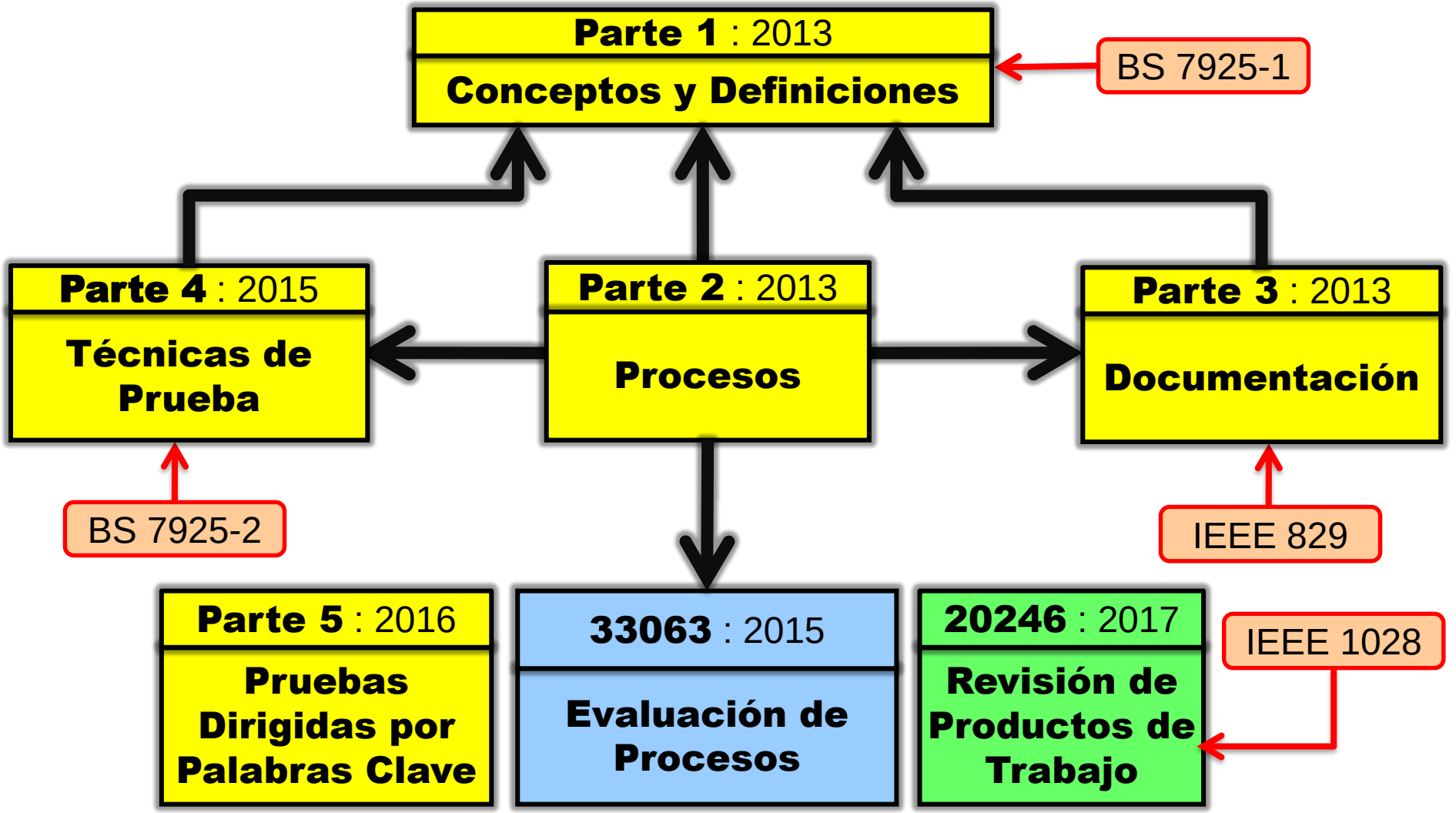
- Aspectos clave sin cubrir en los anteriores:
  - Pruebas no unitarias (integración, sistema, aceptación)
  - Modelo de procesos explíctio
  - Aspectos organizativos y gestión del proyecto. Riesgos
  - Visión más completa de técnicas de prueba
- Definiciones en conflicto, procesos y procedimientos

ISO/IEC/IEEE 29119 Software Testing



- *Propósito: to unify and integrate the currently fragmented corpus of normative literature regarding testing that is currently offered by three distinct standards-makers: BSI, IEEE, and ISO/IEC JTC1/SC7. The result of the project will be a consistent, unified treatment adopted by all three organizations*"
- GT26: Pruebas del Software
  - **http://in2test.lsi.uniovi.es/gt26/**

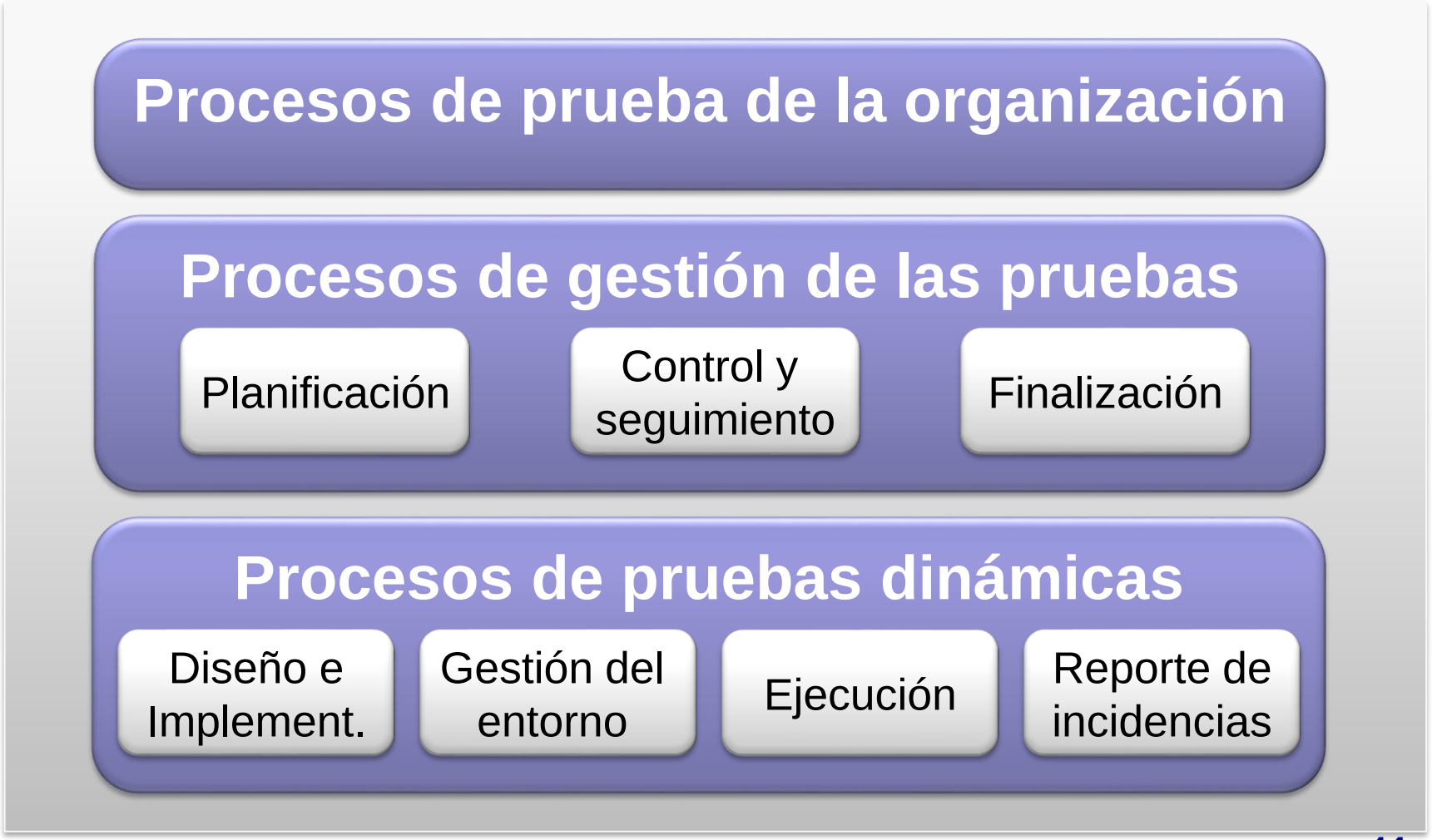
ISO/IEC/IEEE 29119 Software Testing - Estructura



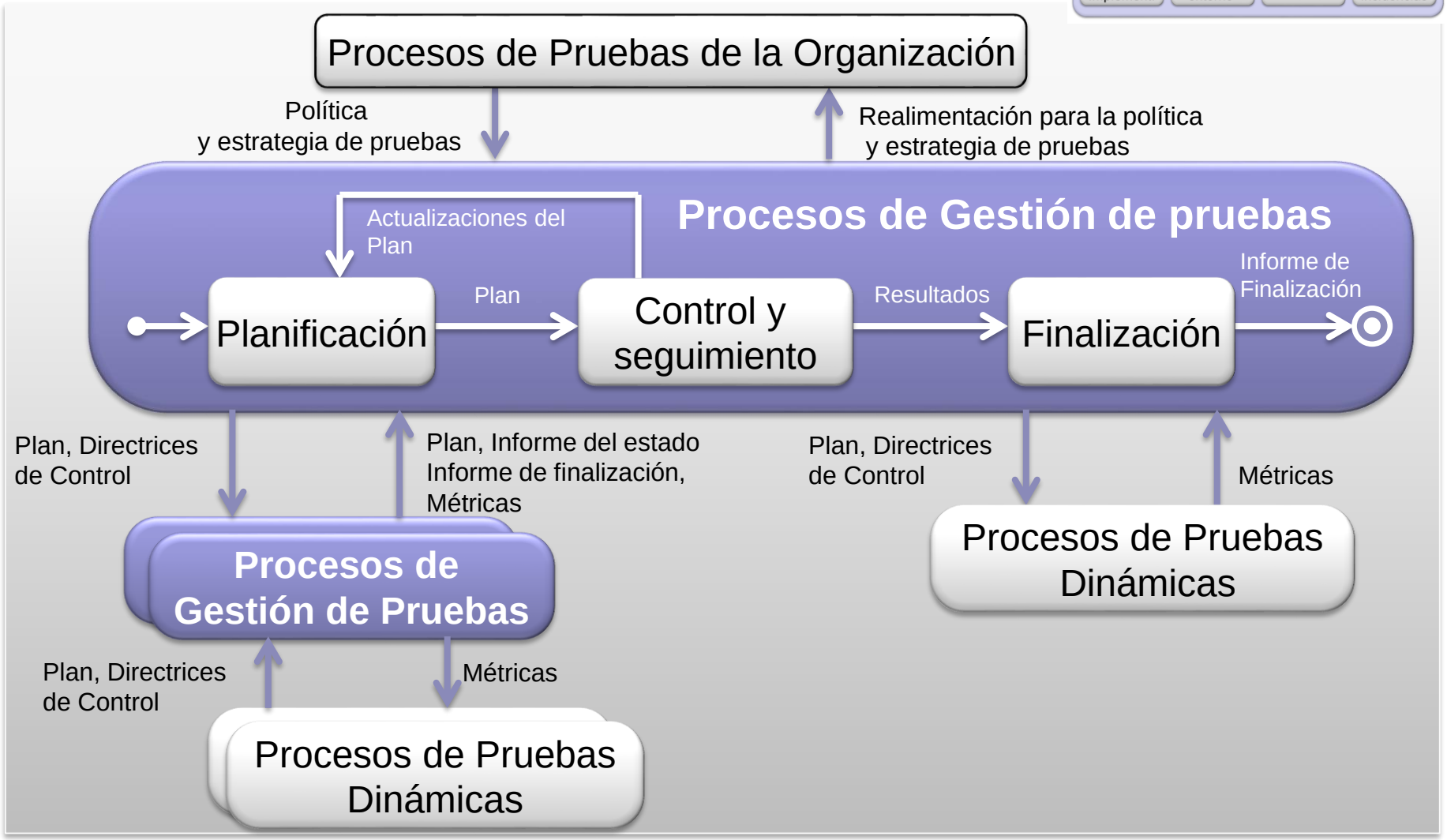
Parte 1 – Conceptos y Definiciones

- Testing
  - "Set of activities conducted to facilitate discovery and/or evaluation of properties of one or more test items"
    - Static testing: without code being executed
    - Dynamic testing: requires the execution of the test item
  - Including: planning, preparation, execution, reporting, and management activities
- Conceptos sobre pruebas de software:
  - Pruebas basadas en riesgos. Estrategias de prueba
  - Diferentes modelos de ciclo de vida
  - Automatización de las pruebas. Métricas
  - Roles y responsabilidades. Problemas en la gestión
  - …

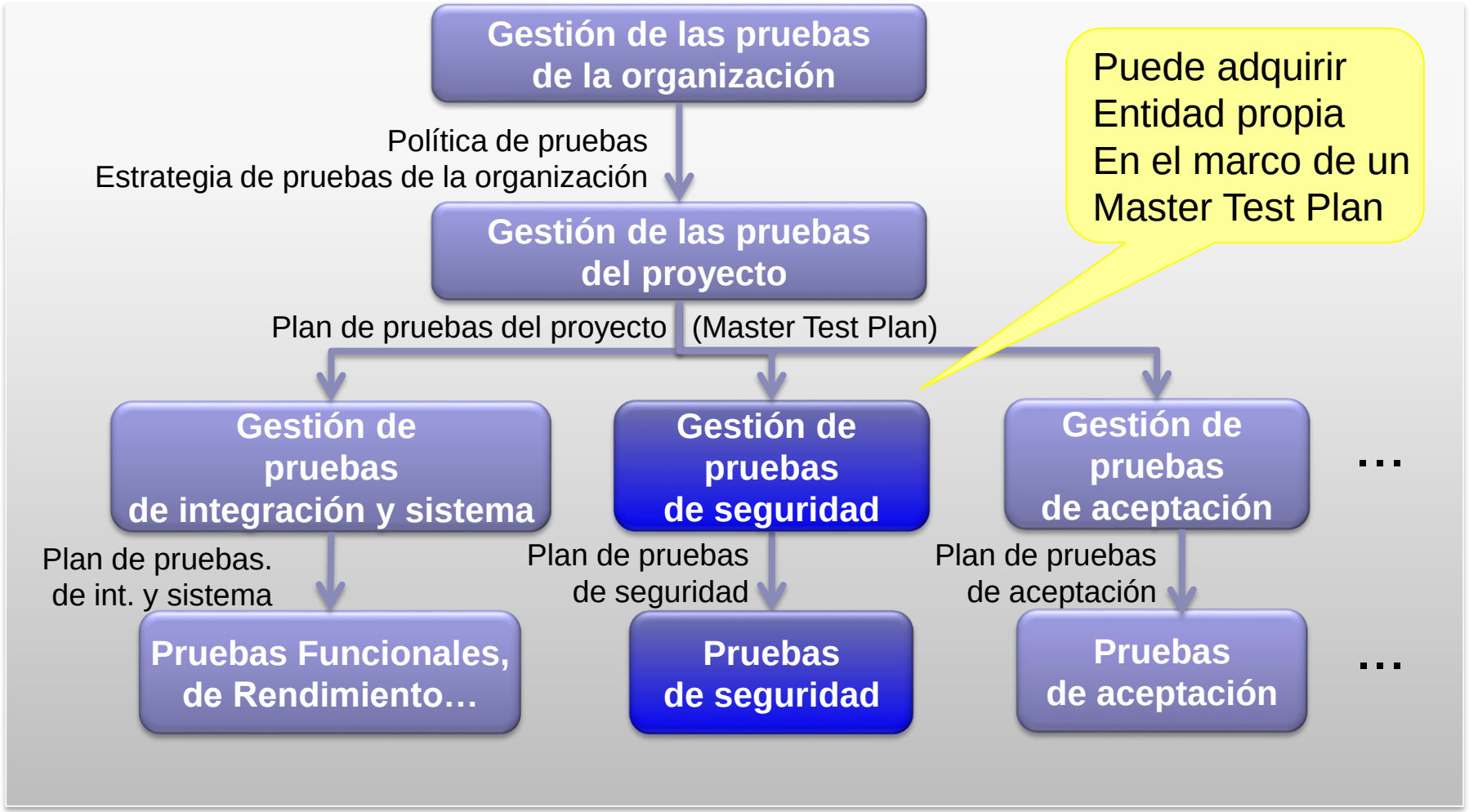
Parte 2 - Modelo de Procesos de pruebas



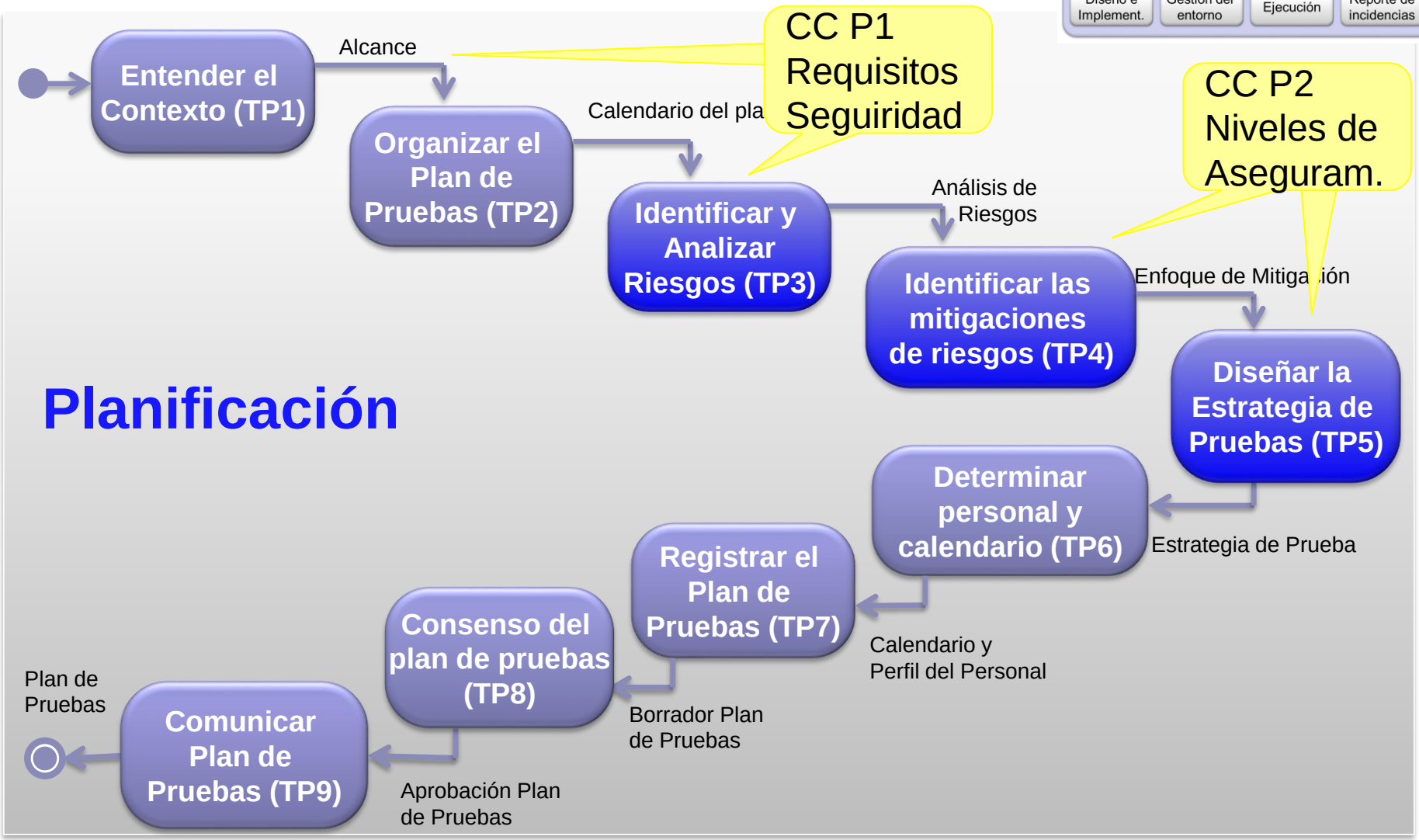
P2 Procesos de Gestión



P2 Aplicación recursiva de procesos - Ejemplo

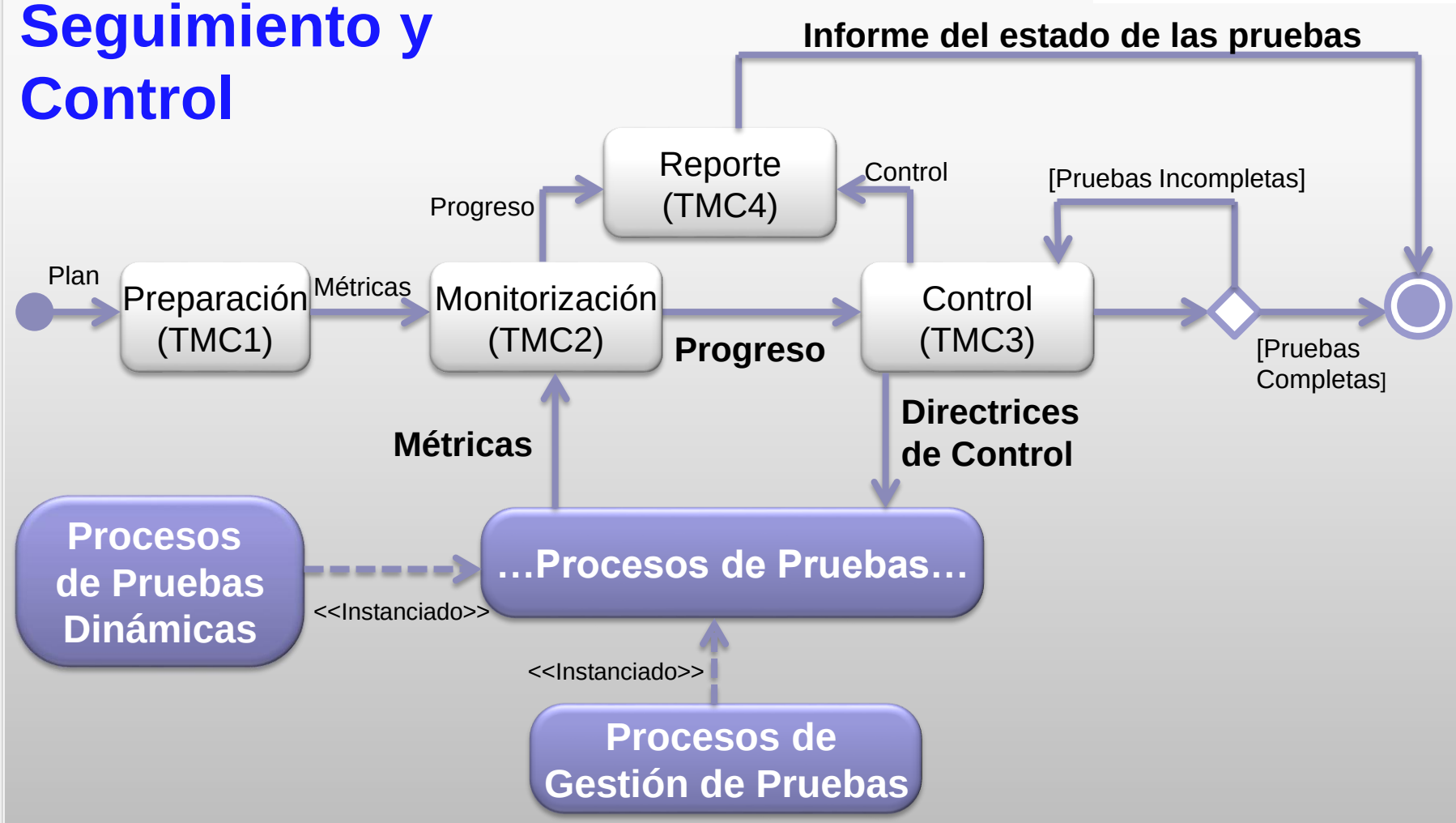


P2 Procesos de Gestión

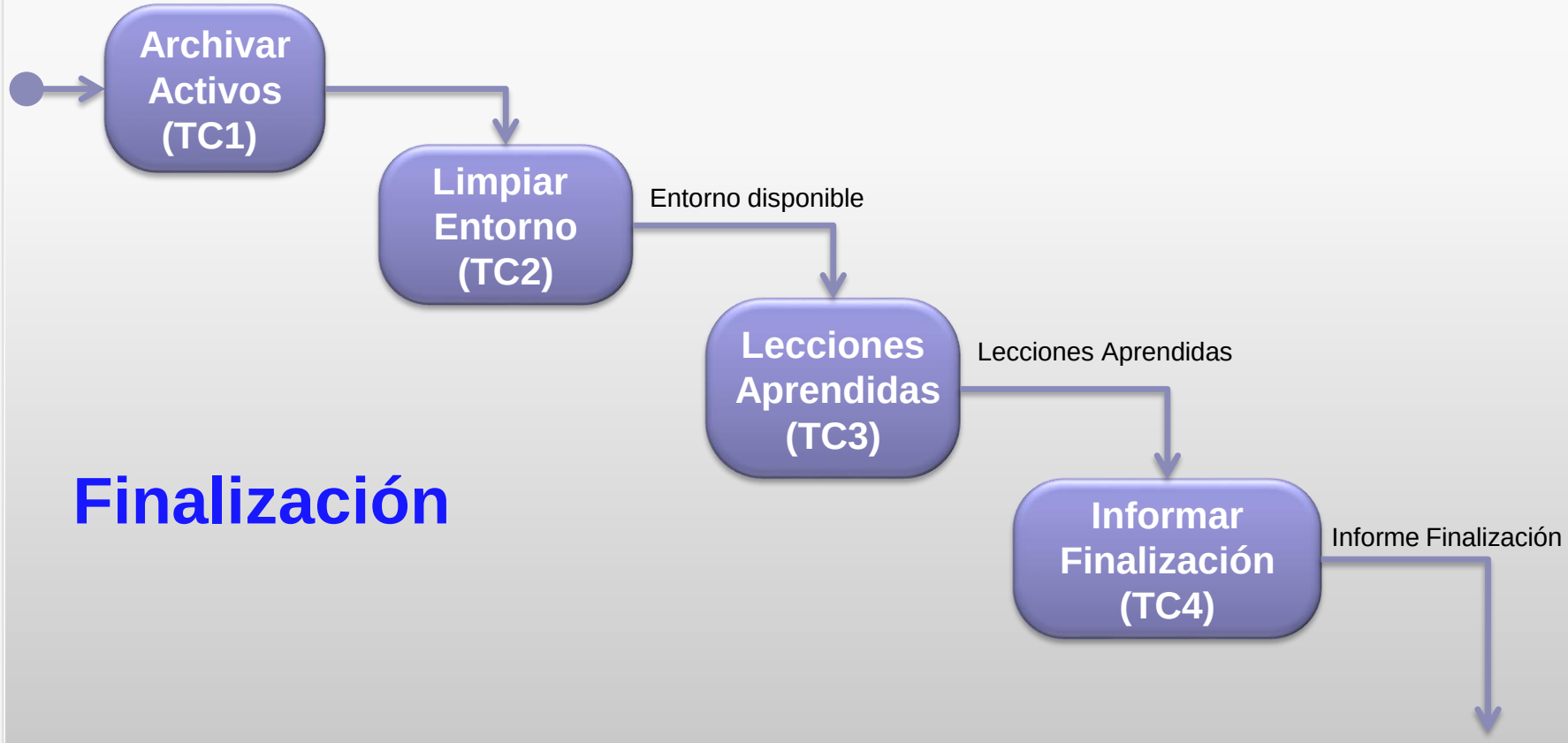


P2 Procesos de Gestión

Seguimiento y Control



P2 Procesos de Gestión

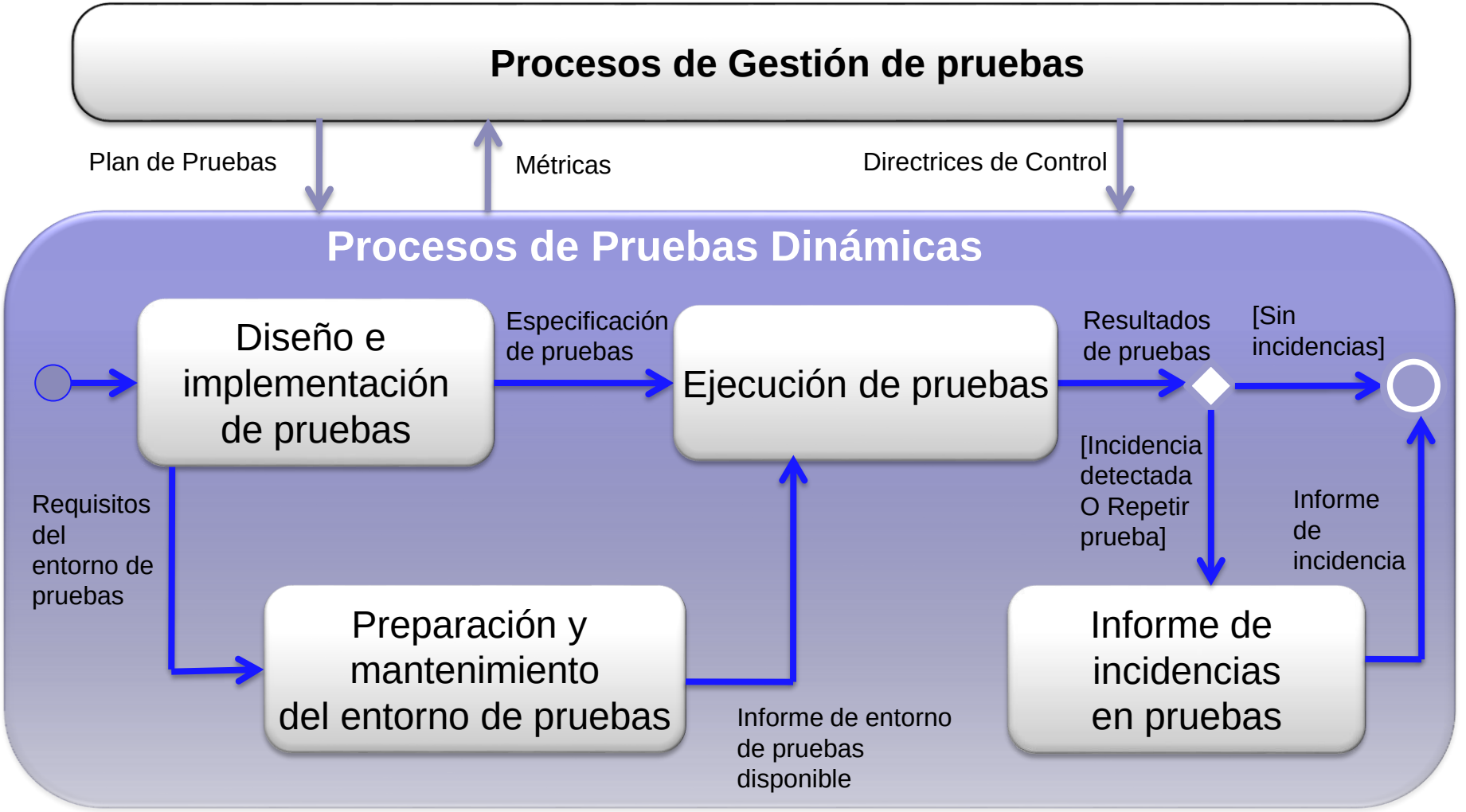


P2 Procesos de Pruebas Dinámicas

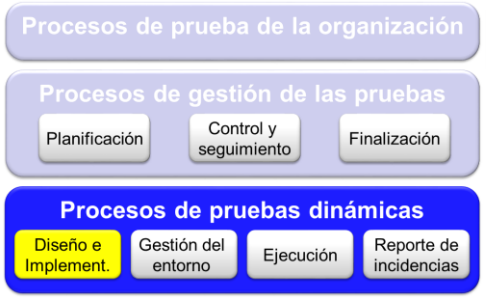
Procesos de prueba de la organización

Procesos de gestión de las pruebas: Planificación | Control y seguimiento | Finalización

Procesos de pruebas dinámicas: Diseño e Implement. | Gestión del entorno | Ejecución | Reporte de incidencias



P2 Procesos de Pruebas Dinámicas



Diseño e Implementación

Identificar juegos de características (TD1)

Juegos de características

Derivar condiciones de prueba (TD2)

Condiciones de prueba (test conditions)

CC P2
ATE_COV
ATE_DPT

Derivar elementos de cobertura de prueba (TD3)

Situaciones que deben cubrir las pruebas (test coverage ítems)

CC P2
ATE_FUN
ATE_IND

Derivar casos de prueba (TD4)

Casos de prueba

Ensamblar conjuntos de pruebas (TD5)

Conjuntos de pruebas

Derivar procedimientos de prueba (TD6)

Procedimientos y scripts de prueba

Base de pruebas (Test basis)

CC P1
Requisitos
Seguridad

Trazabilidad

Parte 3 – Documentación

- Define plantillas que pueden ser utilizadas para generar documentación (information items) producto de los procesos de la parte 2
  - Diferentes formas: registro electrónico, dividido, combinado
  - Conformidad adaptada: según procesos de P2 o según necesidades de proyecto/organización.
- Ejemplos (Anexos C a S). Versiones diferentes para proyectos ágiles y tradicionales, p.e.
  - Políticas y estrategias de la organización
  - Plan de pruebas e informes de estado
  - Especificaciones de pruebas, entorno y datos …
- Mapeo a otros estándares (Anexo T):
  - IEEE 829:2008, BS 7925-2 1998
  - ISO/IEC 15289, ISO/IEC 25051:2006

Parte 4 –Técnicas para el diseño de las pruebas

- Conformidad
  - Total: Subconjunto elegido de técnicas
  - Adaptada: Subconjunto de requisitos. Nuevas Técnicas
- Técnicas para el diseño de las pruebas
  - Basadas en las especificaciones
  - Basadas en la estructura
  - Basada en la experiencia
- Medidas de cobertura
- **Anexos**
  - Anexo A. Características de calidad
  - Anexo B, C y D. Guías y ejemplos de aplicación de las diferentes técnicas de diseño
  - Anexo E. Efectividad en el cálculo de la cobertura

Resumen/Conclusión

- Common Criteria:
  - Establecer un nivel de confianza en un producto
  - Requisitos de seguridad y diferentes niveles de aseguramiento
  - Directrices para definir qué evaluar en relación a la seguridad
- ISO/IEC/IEEE 29119 Software Testing
  - Directrices para la realización de las pruebas cubriendo todos los aspectos del ciclo de vida (definiciones, procesos, técnicas)
  - Soluciona dispersión y huecos no cubiertos por estándares anteriores
  - Adoptado por los comités de normalización nacionales: IEEE y BSI
  - Actualmente representado por 26 naciones, revisado por profesionales de las pruebas de software en todo el mundo
  - Paso adelante hacia la profesionalización de esta industria.
- Más información y contacto:
  - Grupo de trabajo GT26 (**http://in2test.lsi.uniovi.es/gt26/**)
  - Coordinador GT: Javier Tuya (**http://giis.uniov.es/**)