Seguridad en Sistemas Informáticos (SSI)

Visión general de la seguridad informática

Carlos Pérez Conde

Departament d'Informàtica

Escola Técnica Superior d'Enginyeria

Universitat de València

Guión

- **El proceso de la seguridad**
- **Riesgos y vulnerabilidades**
- **La política de seguridad**
- **Tratamiento de incidentes**

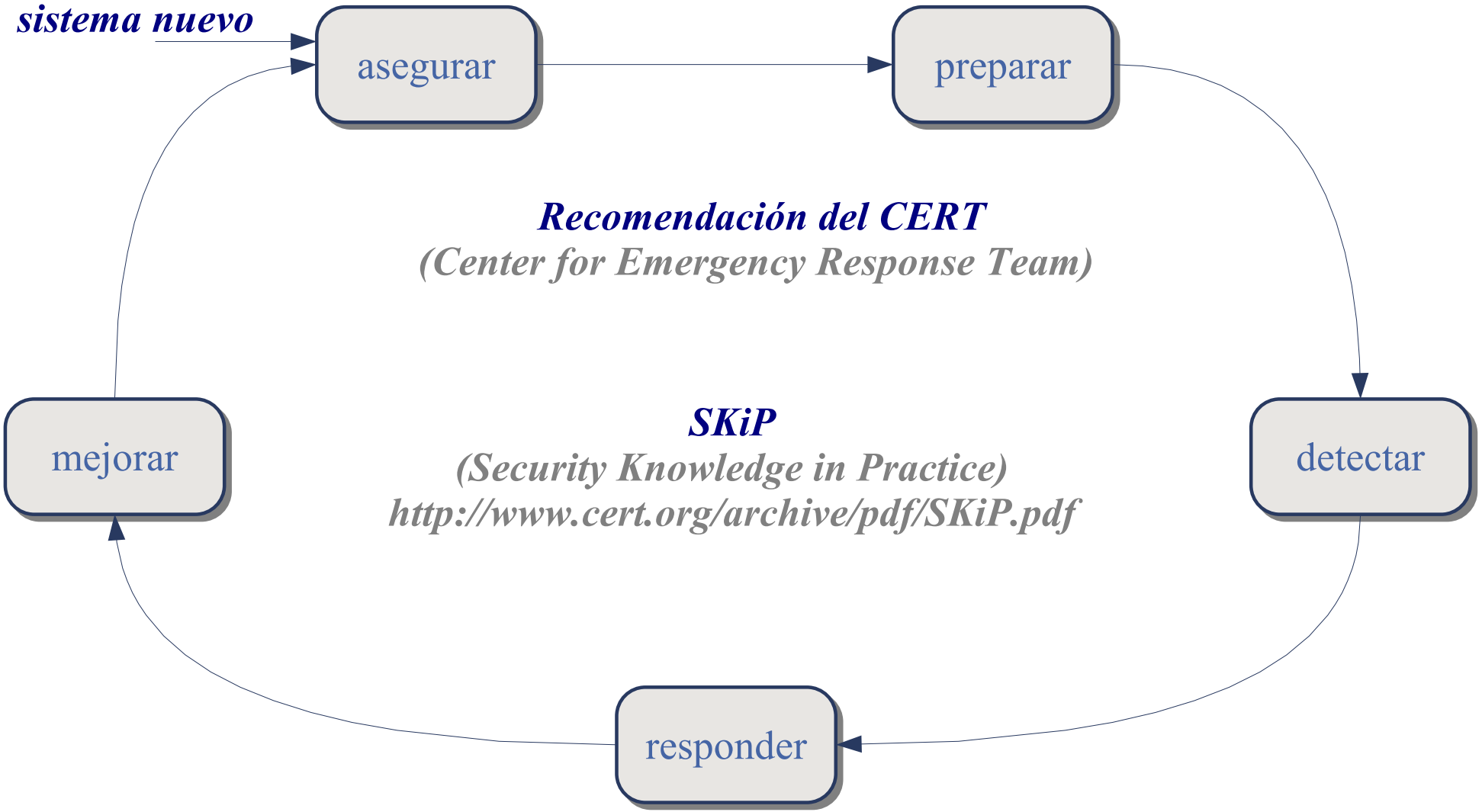
¿Qué significa seguridad?

- **"Un sistema informático (SI) es seguro si se puede depender de que se comporte tal y como de él se espera." [GS96, p. 6]**
- **Cualquier SI puede ser comprometido:**
  - errores sw/hw
  - accidentes y causas naturales
  - ataque con suficientes recursos y conocimientos
- **Compromiso: ¿cuántos recursos destinar?**
  - Política de seguridad
    - ¿Cómo debe comportarse el sistema?
    - ¿Cuánto esforzarse en garantizar que se cumple?
  - Estrategia de seguridad
    - ¿cómo conseguirlo?

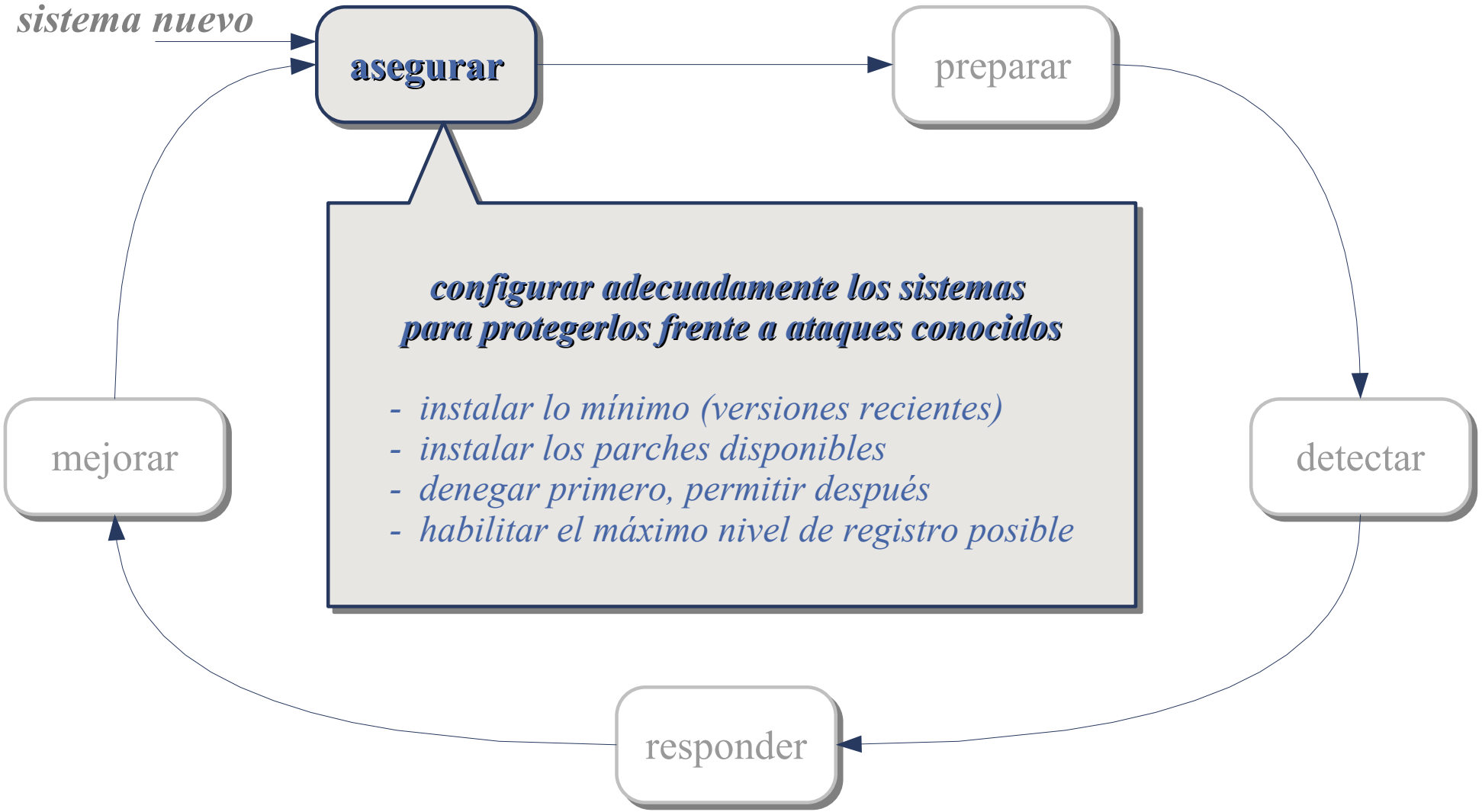
Concepto de seguridad

- **Papel del profesional de seguridad:**
  - ayudar en el establecimiento de la política de seguridad
  - diseñar e implantar la estrategia de seguridad
  - comprobar que se cumple la política de seguridad
- **La seguridad es un proceso**
  - prevención
  - detección
  - reacción
- **Requiere participación universal**

El proceso de la seguridad

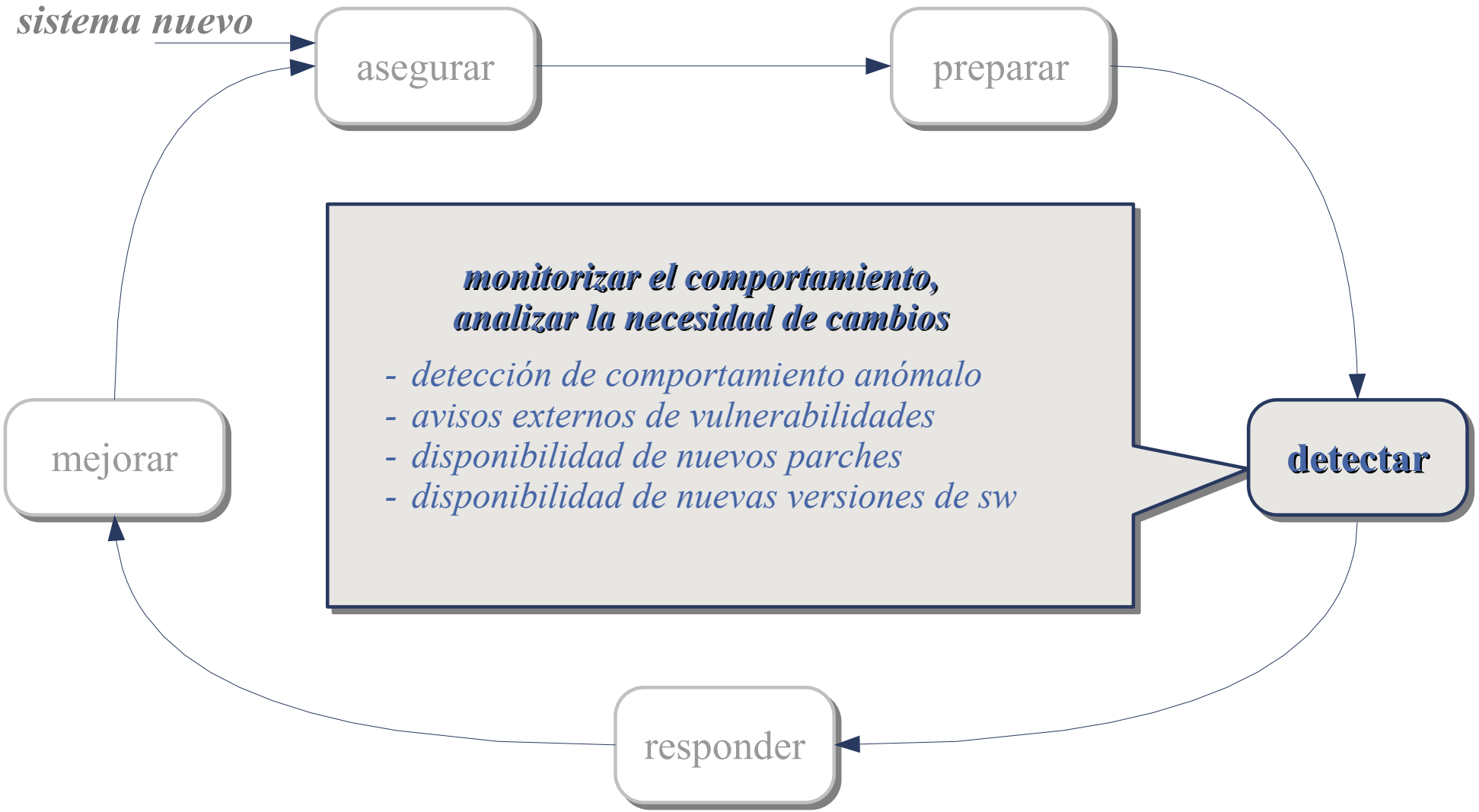


El proceso de la seguridad

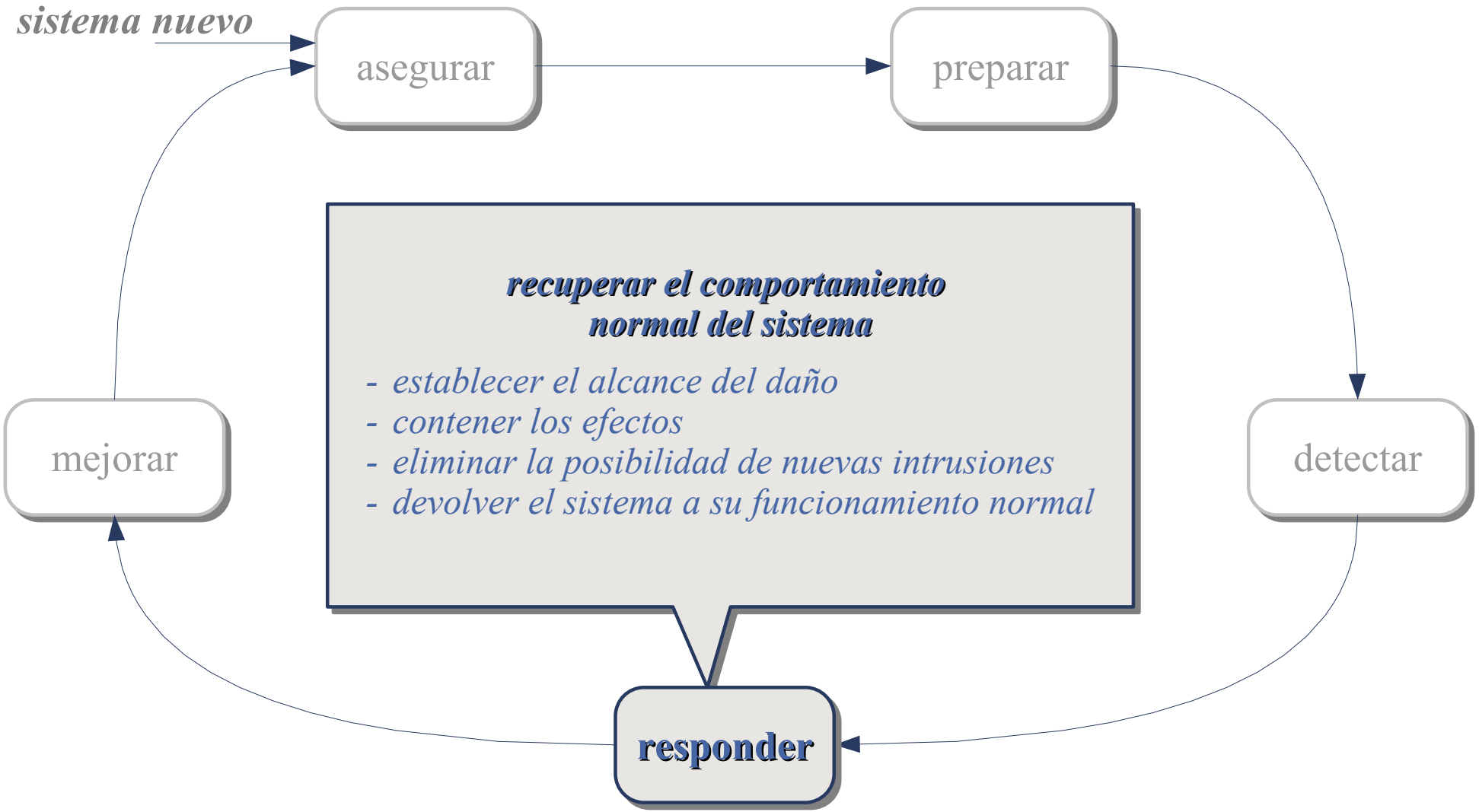


El proceso de la seguridad

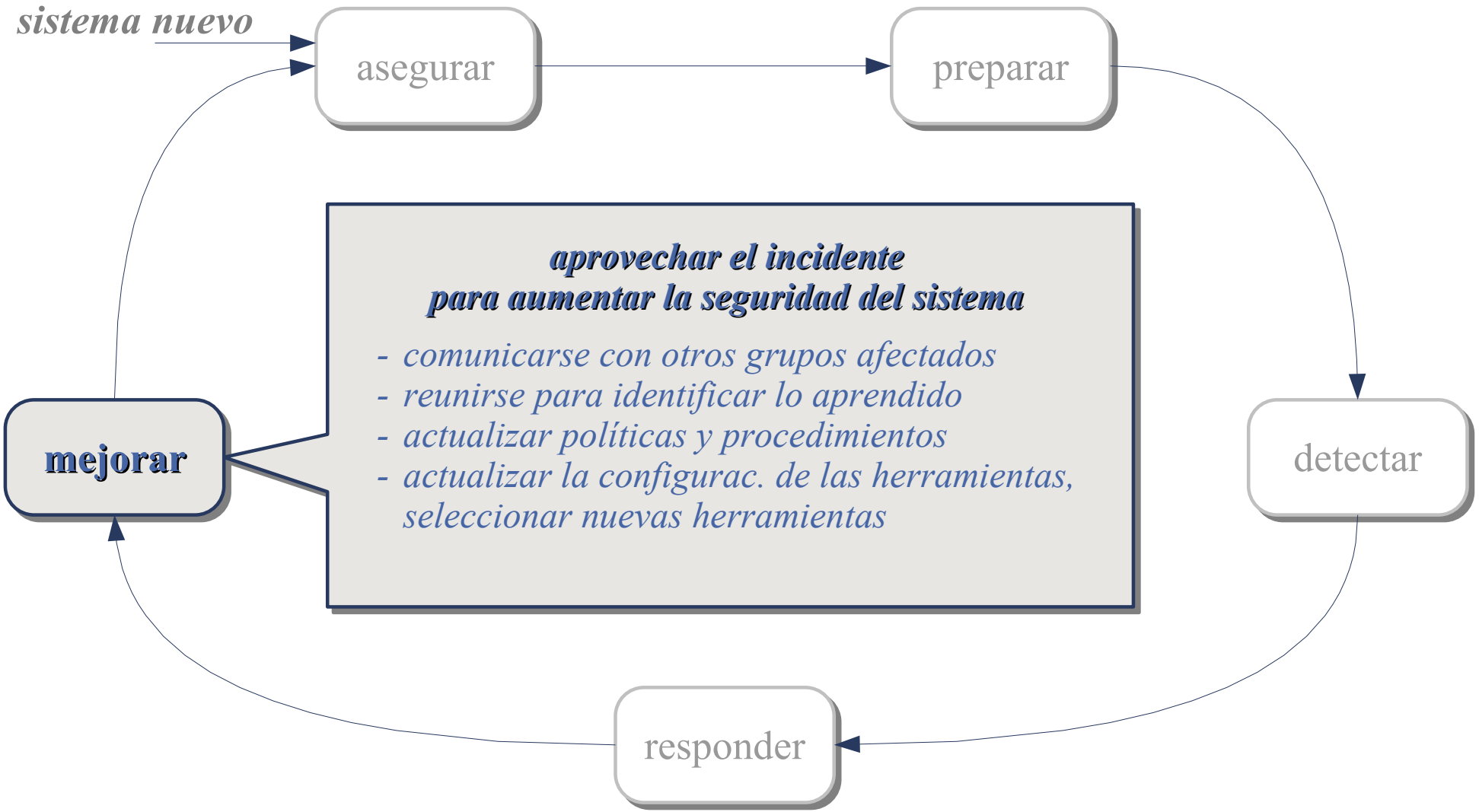
El proceso de la seguridad



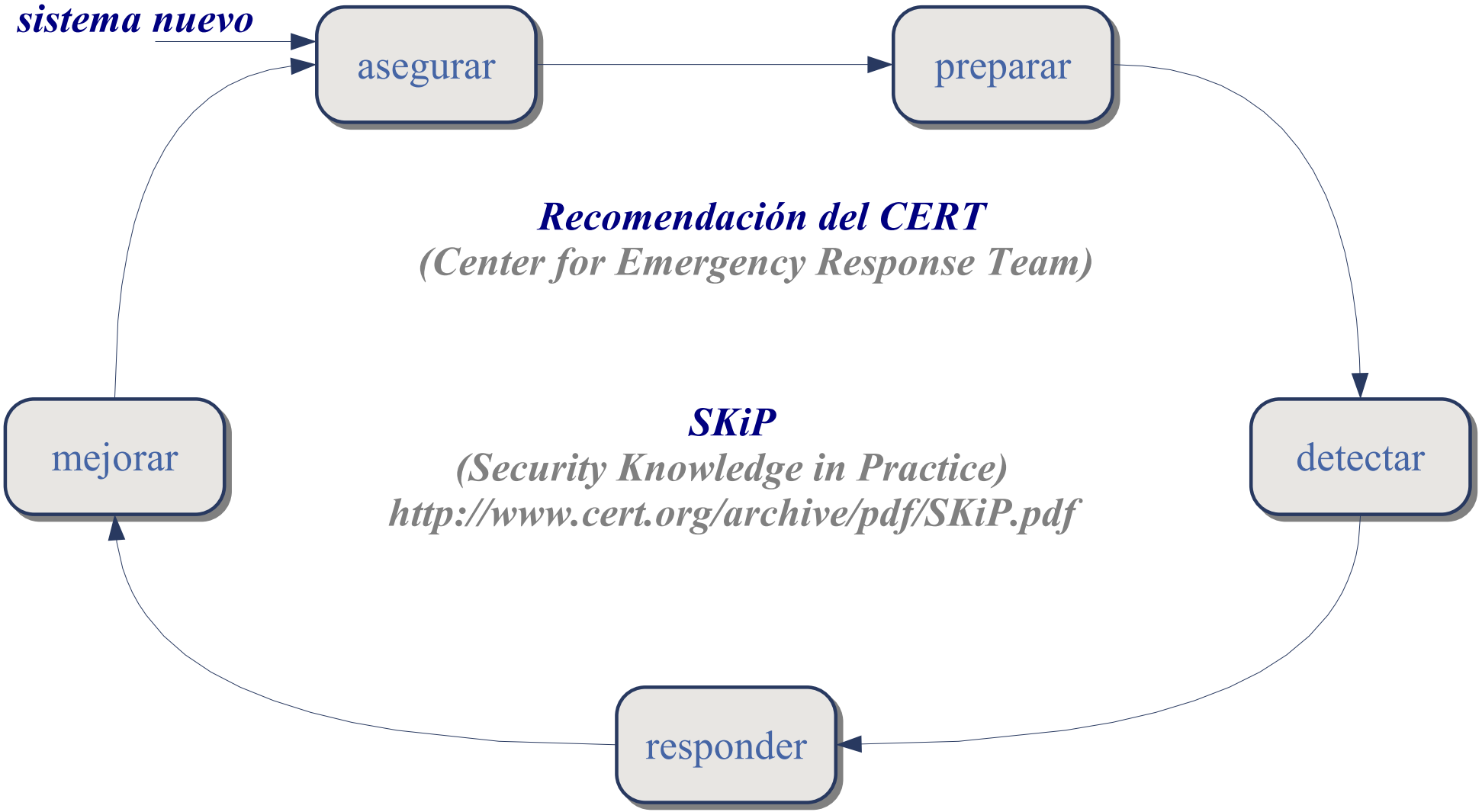
El proceso de la seguridad



El proceso de la seguridad



El proceso de la seguridad



Guión

- El proceso de la seguridad
- **Riesgos y vulnerabilidades**
- La política de seguridad
- Tratamiento de incidentes

Requisitos de seguridad

- **Secreto o confidencialidad**
  - lectura
  - conocimiento de existencia
  - Ejemplo: empresas e instituciones (patentes industriales, secretos de estado...)
- **Integridad**
  - consistencia de la información
  - modificación de los datos
  - Ejemplo: modificación de un saldo
- **Disponibilidad**
  - disponibilidad para los usuarios autorizados
  - evitar el uso no autorizado
  - Ejemplo: el gusano de Internet

Amenazas a los componentes del sistema

- **Soporte físico**
  - disponibilidad: el equipo puede ser dañado
  - medidas físicas y administrativas
- **Soporte lógico (sw)**
  - confidencialidad: copias no autorizadas
  - integridad: modificación del sw
  - disponibilidad: borrado o dañado del sw
  - medidas: administración cuidadosa del sistema
- **Datos**
  - confidencialidad: lectura, copia, información indirecta
  - disponibilidad: eliminación, modificación del control de acceso
  - integridad: modificación, creación
  - medidas: administración + colaboración de los usuarios

Principios de diseño

- **Principio del menor privilegio**
  - cada acción realizada con los privilegios estrictamente necesarios
- **Economía de mecanismos**
  - sencillez para verificación
  - parte integral del diseño del sistema
- **Aceptabilidad**
  - completos, pero sin interferencias innecesarias
  - sencillos de utilizar
- **Intervención completa**
  - todos los accesos deben ser controlados
- **Diseño abierto**
  - los mecanismos de seguridad no deben ser secretos

Guión

- El proceso de la seguridad
- Riesgos y vulnerabilidades
- **La política de seguridad**
- Tratamiento de incidentes

Políticas de seguridad

- **Análisis previos:**
  - análisis de las necesidades de seguridad
  - análisis de riesgos
  - análisis de costes y beneficios
- **La política de seguridad establece:**
  - qué se protege y por qué
  - quién es responsable de esa protección
  - cómo resolver problemas derivados de su aplicación
- **La política de seguridad del sistema:**
  - debe ser impulsada por la administración de la empresa/institución
  - debe ser conocida y comprendida por todos los usuarios

Creación de la política de seguridad

- **Usos y costumbres de los usuarios**
- **Reglas (escritas y no escritas) y la cultura de la organización**
- **Redacción del documento**
  - específico
  - claro
  - conciso
  - realista
- **Política bien escrita → fácil generar una lista de comprobación de que se cumple**

Guión

- El proceso de la seguridad
- Riesgos y vulnerabilidades
- La política de seguridad
- **Tratamiento de incidentes**

Gestión de incidentes de seguridad

- **Preparación**
- **Detección e identificación**
- **Contención**
  - contener y limpiar versus observar y aprender
  - preparar futuros análisis mientras se limita el daño
- **Erradicación**
  - reforzar las medidas de prevención (eliminar las nuevas vulnerabilidades)
- **Recuperación**
  - necesidad de reforzar la vigilancia para comprobar la efectividad de los cambios
- **Lecciones aprendidas**

Caso de ejemplo: descripción de incidentes de seguridad

- **Ejemplo de incidente**
  - Sun Microsystems Java GIF image processing buffer overflow
    - US-CERT: http://www.kb.cert.org/vuls/id/388289
    - CVE: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-0243
  - Preguntas
    - ¿cómo funciona?
    - ¿qué riesgos supone?
    - ¿cómo se puede resolver el problema?
    - ¿cómo se puede resolver el problema en openSUSE 10.3?
- **¿Cómo informar de un incidente?**
  - http://www.cert.org/tech_tips/incident_reporting.html