El papel del Plan Director de Seguridad en las organizaciones

Antonio Villalón Huerta
Director Técnico de Explotación
S2 Grupo

Nuevos escenarios en Seguridad de la Información

ISO 27001 y Reglamento de Desarrollo de la LOPD

Introducción

- El Plan Director de Seguridad (PDS) es la herramienta que permite a una organización definir sus actividades en Seguridad de los Sistemas de Información a corto, medio y largo plazo.

- Determinando el estado de seguridad en que se encuentra mi organización y conociendo mi estado objetivo, puedo trazar una planificación que me permita alcanzar dicho objetivo.

Para empezar a trabajar…

- Antes de poder definir un Plan Director de Seguridad en la organización es necesario identificar los **objetivos** y las **necesidades** en materias de Seguridad de la Información:
  - Requisitos de seguridad en el negocio.
  - Criticidad de la información.
  - Legislación aplicable.
  - ...

- Decisión a nivel estratégico: la seguridad debe ser respaldada al más alto nivel directivo.

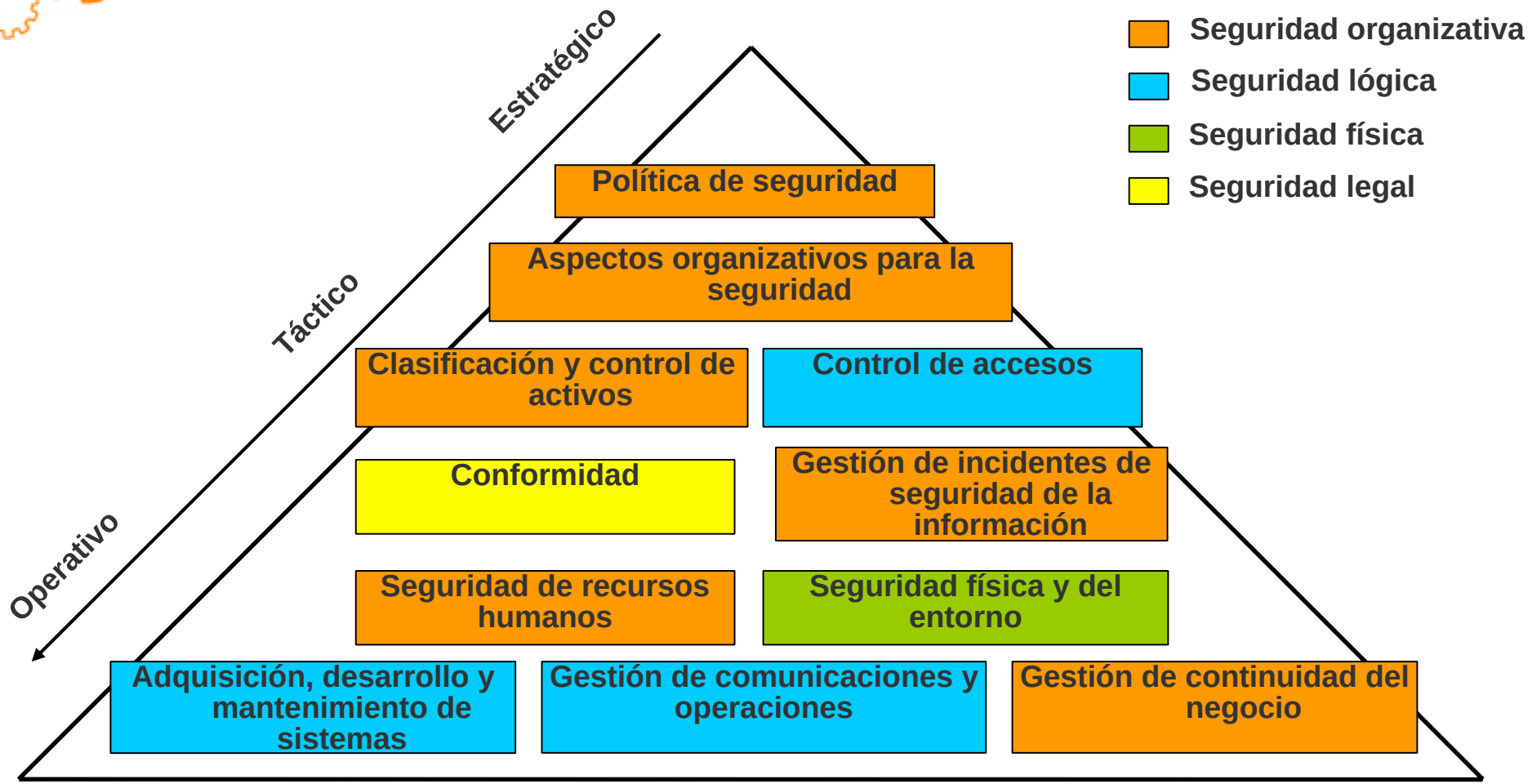
El primer problema

- ¿Cómo plasmo las directrices estratégicas en seguridad tangible?

- Debo hablar de 'seguridad' de una forma objetiva:
  - ISO 13335 / UNE 71501
  - ISO 15408
  - …
  - **UNE-ISO/IEC 17799:2002, ISO/IEC 17799:2005**

- La norma ISO 17799 me permite marcar un objetivo de cumplimiento **cuantitativo**, un objetivo *objetivo.*

UNE-ISO/IEC 17799:2005

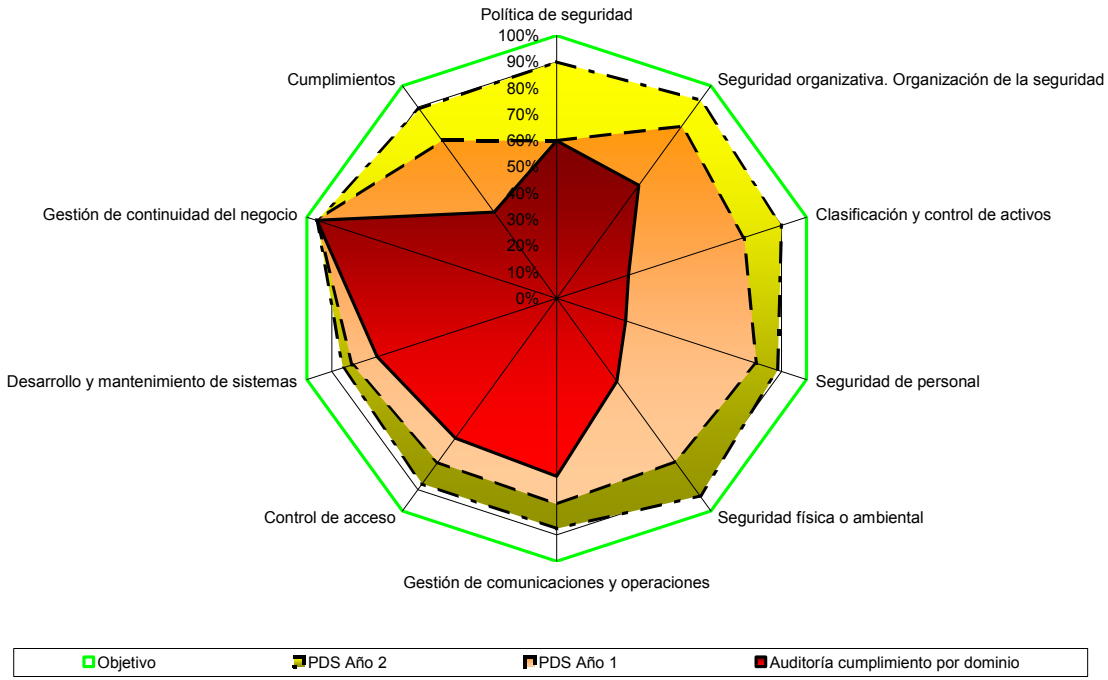


Y ahora, ¿qué?

- Conociendo cuantitativamente mis objetivos, debo identificar mi situación actual.
- Sé donde quiero estar: sabiendo donde estoy actualmente podré planificar el camino.
- ¿Cómo? Auditoría ISO 17799:2005. Mido objetivamente mi seguridad en todos sus ámbitos:
  - Físico.
  - Lógico.
  - Organizativo.
  - Legal.

Auditoría ISO17799

- Una auditoría ISO 17799 proporciona **información precisa** acerca del **nivel de cumplimiento** de la norma a diferentes niveles: global, por dominios, por objetivos y por controles.

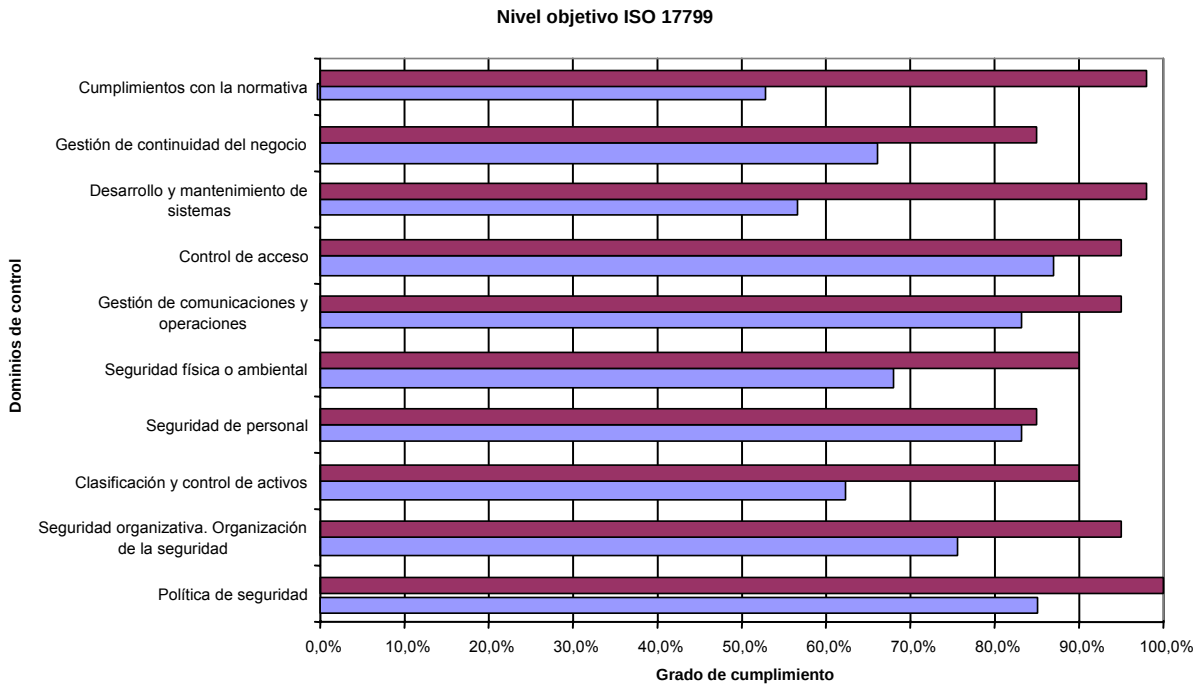


Auditoría ISO17799: un ejemplo

- Dominio: Control de acceso.
  - Objetivo: Prevenir el acceso no autorizado a los servicios de red.
    - Control: Restricción de las posibilidades de conexión a la red corporativa desde otras redes.
- Análisis:
  - Test de visibilidad.
  - Test de penetración.
  - Test de propagación.
  - Revisión reglas de cortafuegos.
  - Revisión registros NIDS.
  - …

Planificación

- Conozco cuantitativamente la situación actual y mi situación objetivo. Ya puedo planificar el camino a seguir: **Plan Director de Seguridad**.



El camino a seguir…

- Identificación de iniciativas y proyectos concretos, e implantación y seguimiento de los mismos:
  - Plazos.
  - Costes.
  - Asignación de recursos.
  - ...

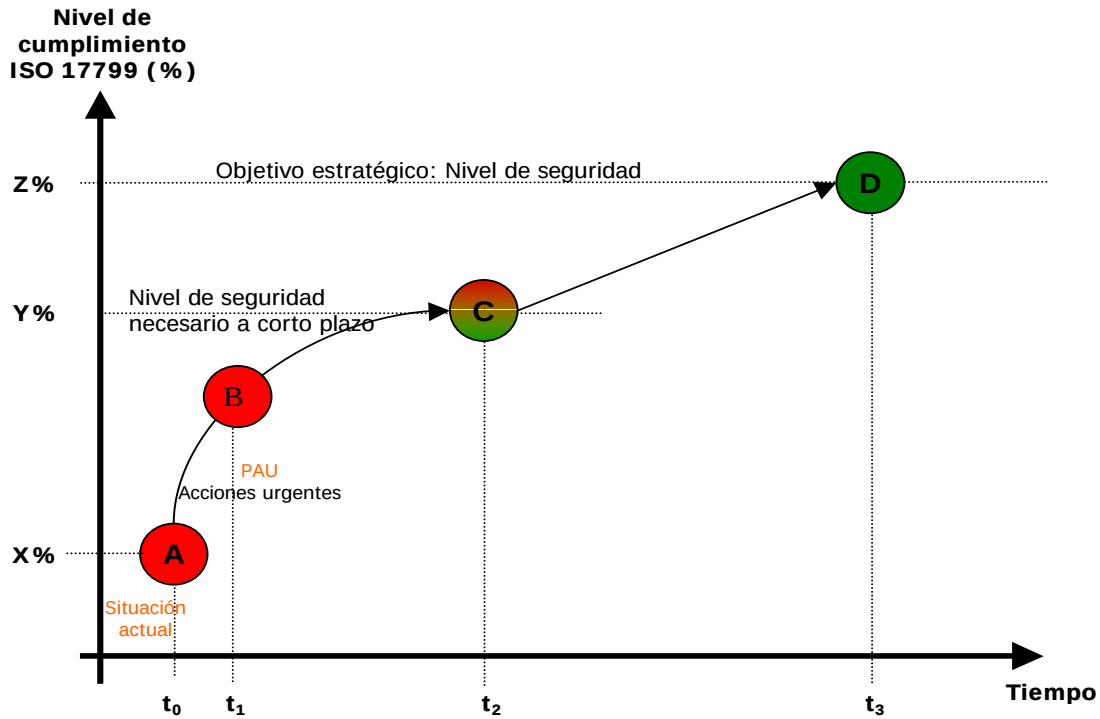
- Factor crítico de éxito: avance permanente.
  - '*Retroceder nunca,...*'

Un ejemplo

- Iniciativa para reforzar los controles de acceso a la información.
- Plazo estimado: 2 meses.
- Inversión: 8.000,00 euros.
- Tareas a desarrollar:
  - Implantación nuevo cortafuegos.
  - Configuración ACLs en routers.
  - Políticas de contraseñas robustas.
  - *Honeytokens*.
  - Procedimientos de autorización de acceso.
  - Definición de usuarios nominativos.
  - …
- Incremento dominio ISO 17799:2005: 43% → 78%

Plan de trabajo

- Hitos intermedios y auditorías de cumplimiento en el camino: control de la implantación.
- Hito más crítico: nivel **mínimo aceptable**. Hasta no superarlo, debo preocuparme seriamente.



Para acabar…

- El Plan Director de Seguridad tiene como primer gran objetivo el alcance de los niveles de seguridad estratégicamente aceptables.
- No sólo es importante el alcance, sino también el mantenimiento.
  - Debo mantener en el tiempo los niveles alcanzados.
  - No puedo permitirme ir hacia atrás.
    - Cambios en el entorno.
- Alcanzado un nivel aceptable, puedo plantearme la certificación UNE 71502 / ISO 27001.
  - El ‘nivel aceptable’ incluirá la definición de un SGSI.

Conclusiones

- Tres **pilares fundamentales** para el Plan Director de Seguridad:
  - Punto de partida.
  - Objetivo marcado.
  - Camino a recorrer entre ambos.

- No sólo es importante la definición del PDS: lo son más su **cumplimiento** y el avance permanente.

- Una vez he alcanzado mi objetivo debo mantenerlo a toda costa.

The End…

¡¡MUCHAS GRACIAS!!