Gestión de la seguridad de la información: UNE 71502, ISO 17799

Antonio Villalón Huerta
avillalon@s2grupo.com

Junio, 2004

Índice

- Introducción
- La norma UNE-ISO/IEC 17799
- La norma UNE 71502
- Gestión de la seguridad
- Certificación
- Conclusiones

Introducción: definiciones

- **ACTIVO:** Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.
- **AMENAZA:** Evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.
- **RIESGO:** Posibilidad de que una amenaza se materialice.
- **IMPACTO:** Consecuencia sobre un activo de la materialización de una amenaza.
- **CONTROL:** Práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

Introducción: ¿qué es seguridad?

- La norma UNE-ISO/IEC 17799 define la **seguridad de la información** como la preservación de...

  - ... su **confidencialidad**.
    - Sólo quienes estén autorizados pueden acceder a la información.

  - ... su **integridad**.
    - La información y sus métodos de proceso son exactos y completos.

  - ... su **disponibilidad**.
    - Los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

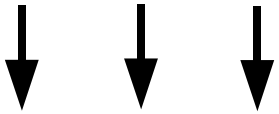
Introducción: ¿qué es gestionar?

- *Gestionar* es llevar a cabo las diligencias necesarias para lograr un determinado fin.
  - La gestión de la seguridad consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización.

- Algunas consideraciones...
  - Los problemas de seguridad no son únicamente de índole tecnológica.
  - Los riesgos no se eliminan... se gestionan.
  - La seguridad no es un producto, es un proceso.

Introducción: ¿por qué gestionar?

- Garantizar la confidencialidad, integridad y disponibilidad de sus activos es crítico para cualquier organización.
- Las nuevas tecnologías introducen nuevas amenazas.
- La dependencia creciente de los recursos de TI aumenta los impactos.
- No siempre se pueden eliminar los riesgos.
- ...



- Es necesario **gestionar** la seguridad de la información.

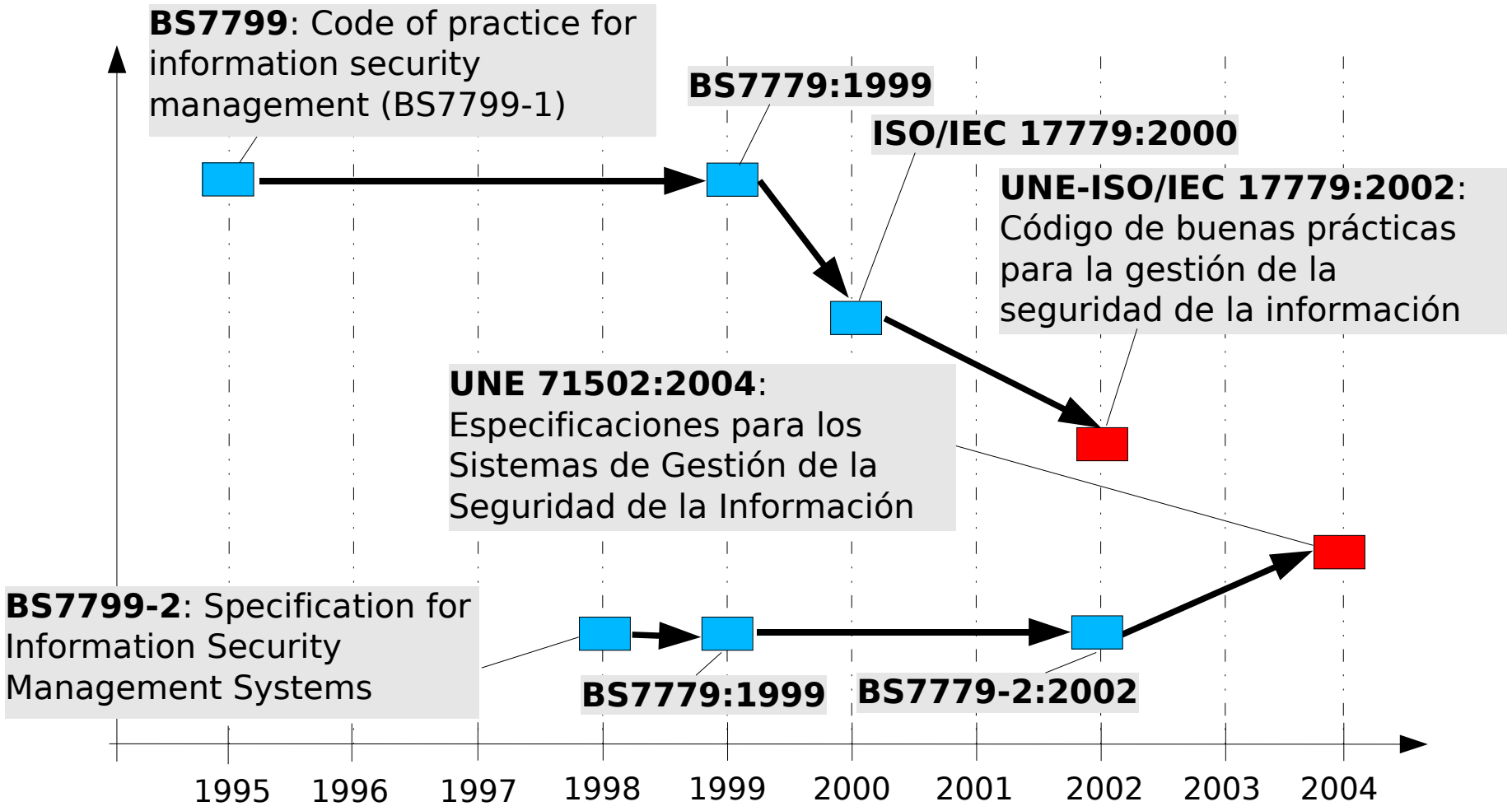
Introducción: ¿cómo gestionar?

- PROBLEMA: ¿Cómo establecer qué entendemos por '*Seguridad*'?
- Diferentes criterios de evaluación de la seguridad: internos a una organización, sectoriales, nacionales, internacionales...
- Multitud de estándares aplicables a diferentes niveles:
  - TCSEC (Trusted Computer Security, militar, US, 1985).
  - ITSEC (Information Technology Security, europeo, 1991).
  - Common Criteria (internacional, 1986-1988).
  - *7799 (británico + internacional, 2000).
  - ...

Introducción: *7799. Historia

- En 1995 el British Standard Institute publica la norma **BS7799**, un código de buenas prácticas para la gestión de la seguridad de la información.
- En 1998, también el BSI publica la norma **BS7799-2**, especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2002.
- Tras una revisión de ambas partes de BS7799 (1999), la primera es adoptada como norma ISO en 2000 y denominada **ISO/IEC 17799**.
- En 2002 la norma ISO se adopta como UNE sin apenas modificación (**UNE 17799**), y en 2004 se establece la norma **UNE 71502**, basada en BS7799-2 (no existe equivalente ISO).

Introducción: *7799. Gráficamente...



Norma UNE-ISO/IEC 17799

- Con origen en la norma británica BS7799-1, constituye un código de buenas prácticas para la Gestión de la Seguridad de la Información.
- Establece la base común para desarrollar normas de seguridad dentro de las organizaciones.
- Define diez dominios de control que cubren por completo la Gestión de la Seguridad de la Información.
- Norma técnica de seguridad de la información más reconocida a nivel internacional.
- 36 objetivos de control y 127 controles.
- NO CERTIFICABLE.

Norma UNE-ISO/IEC 17799: dominios

1. Política de seguridad
2. Aspectos organizativos para la seguridad
3. Clasificación y control de activos
4. Seguridad ligada al personal
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones
7. Control de accesos
8. Desarrollo y mantenimiento de sistemas
9. Gestión de continuidad del negocio
10. Conformidad

Norma UNE 71502

- Norma que contiene las especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI):
  - Establecimiento
  - Implantación
  - Documentación
  - Evaluación

- Basada en los controles y objetivos de control de la norma UNE-ISO/IEC 17799.

- Define la relación de procedimientos para establecer el SGSI: componente documental del sistema.

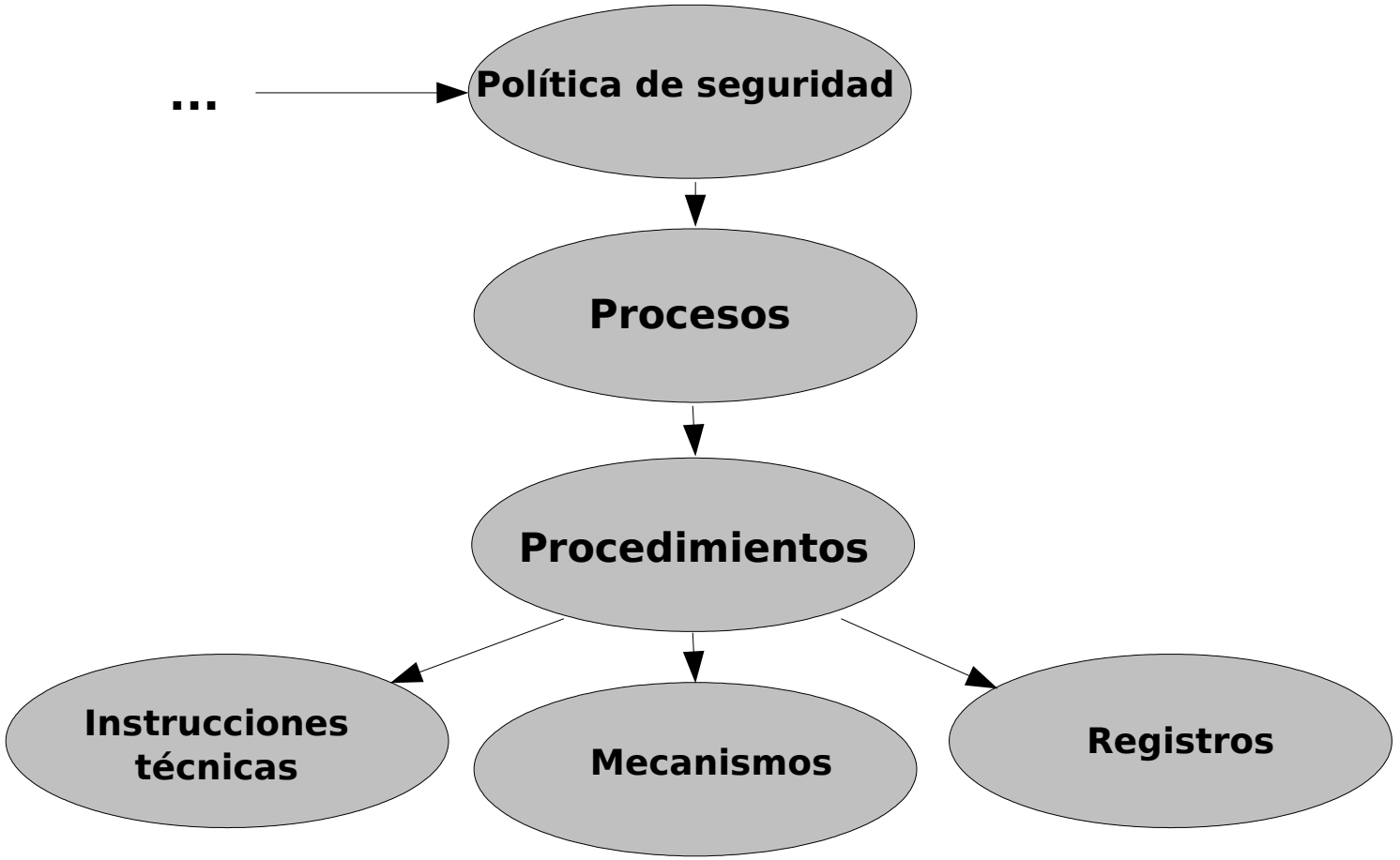
Norma UNE 71502

- Sistema equivalente a otros sistemas de gestión (ISO9000, ISO14000...) e integrable con ellos.
- Independiente del tipo, tamaño o área de actividad de la organización.
- CERTIFICABLE.
- Limitaciones: no tiene equivalente ISO.
  - Actualmente se está estudiando la unificación internacional de normas... a largo plazo.

Gestión de la seguridad: SGSI

- **Sistema de Gestión de la Seguridad de la Información (SGSI):** Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.
- Cubre aspectos organizativos, lógicos, físicos, legales...
- Independiente de plataformas tecnológicas y mecanismos concretos.
  - Aplicación en todo tipo de organizaciones.
- Fuerte contenido documental.

Gestión de la seguridad: estructura



Gestión de la seguridad: modelo

- Modelo PDCA (Plan – Do – Check – Act): Planificar, Hacer, Verificar y Actuar.

Gestión de la seguridad: planificar

- Tres preguntas clave:
  - ¿Cuál es el estado actual de nuestra seguridad?
  - ¿Cuál es el estado al que queremos llegar?
  - ¿Cómo queremos llegar a ese estado objetivo?
- Las respuestas a estas preguntas permiten definir el plan de actuación para conseguir los objetivos deseados.
- Piezas clave de esta fase:
  - Política de seguridad.
  - Análisis de riesgos.
  - Selección de controles.
- Aspecto crítico: implicación del más alto nivel directivo.

Gestión de la seguridad: hacer

- Dos grandes áreas: implantación del SGSI y explotación del mismo.

- Implantación del SGSI: ejecución del plan definido en la fase anterior.
  - Implantación de controles (tanto técnicos como no técnicos).
  - Control de controles: eficacia.

- Explotación del SGSI:
  - Operación de los sistemas implantados.
  - Respuesta ante incidentes.

Gestión de la seguridad: verificar

- Es necesario verificar la conveniencia, adecuación y eficacia del SGSI en la organización.
- Indicadores de rendimiento: valores objetivos (¿Mucho?, ¿Poco?, ¿A veces?, ¿Demasiado?...).
  - Eficacia: El SGSI cumple los objetivos de dirección.
  - Eficiencia: Lo hace con coste mínimo.
- Fase de **auditoría** del SGSI:
  - ¿Se ajusta a lo deseado?
  - ¿Ha sido implantado y se mantiene y ejecuta correctamente?
  - ¿Existen nuevos riesgos?
  - ¿Hay cambios que puedan afectar al SGSI?

Gestión de la seguridad: actuar

- La organización debe mejorar de manera contínua la eficacia del SGSI:
  - Revisión de objetivos de seguridad.
  - Indicadores de eficacia de los procesos.
  - Auditoría periódica y revisiones de seguridad.
  - ...
- Es necesario tomar acciones **correctivas** para eliminar la causa de las no conformidades en la implantación, operación y uso del SGSI.
- Es necesario determinar acciones **preventivas** para eliminar la causa de no conformidades potenciales, previniendo su ocurrencia.

Certificación

- Una entidad independiente y competente afirma que un sistema es correcto y compromete en ello su palabra... por escrito.
- Garantía de '*calidad de la seguridad*'.
- Aporta beneficios para...
  - ... la propia organización.
  - ... los inversores.
  - ... los clientes.
  - ... los empleados.
- Adaptarse a la norma no garantiza la inmunidad total de la organización frente a problemas de seguridad, pero reduce el riesgo y los costes asociados a tales problemas.

Certificación: proceso

- El proceso general de certificación consta de dos grandes etapas: consultoría y auditoría.

- En la primera de ellas, un equipo de consultores con experiencia en la norma ayuda a la organización a cumplir los requisitos de certificación: política de seguridad, procedimientos, controles...

- Cuando la organización – asesorada por los consultores – considera que cumple los requisitos de la norma, solicita la certificación a un organismo acreditado, como AENOR, que será el encargado de realizar la auditoría.

Certificación: proceso

- El proceso de auditoría consta a su vez de dos fases: una documental, en la que se revisan los procesos y procedimientos de gestión de la seguridad, y otra de revisión de la implantación de los controles seleccionados.

- La credibilidad y garantías de la certificación están sujetas a la confianza depositada en la entidad que certifica.

- La certificación no debe ser un OBJETIVO de seguridad, sino un **RECONOCIMIENTO** al trabajo bien hecho.

Conclusiones

- Los problemas de seguridad no son necesariamente técnicos.
- La seguridad no es un producto, es un **proceso**.
- Debemos **gestionar** nuestra seguridad.
- Un sistema de gestión debe contemplar la **mejora contínua** del sistema: todo evoluciona, especialmente la (in)seguridad.
- La **certificación** de seguridad es beneficiosa, pero ni garantiza inmunidad ni debe ser un objetivo.

¡La seguridad total no existe!

¡¡MUCHAS GRACIAS!!

Grupo S2
Vinalopó, 7 bajo
46021 Valencia
Tel: 963 110 300
Fax: 963 106 086

http://www.s2grupo.com/
info@s2grupo.com