El Sistema de Gestión de la Seguridad de la Información: Calidad de la Seguridad

Antonio Villalón Huerta
avillalon@s2grupo.com

Mayo, 2005

S2 grupo

Índice

- Problemática de la seguridad.
- Sistemas de gestión.
- Sistema de Gestión de la Seguridad de la Información.
  - Normativa.
  - Ciclo PDCA.
  - Proceso.
  - Algunas consideraciones.
- Certificación.
- Conclusiones.

Problemática de la seguridad

- ¿Problemas técnicos? Rara vez...

- Problemas de gestión: alineamiento de la tecnología y los objetivos de la organización:
  - *¿Qué entendemos por seguridad?*
  - *¿Cómo medimos la seguridad?*
  - *¿Quién se preocupa de la seguridad?*
  - *¿Cuánto dinero invertir en seguridad?*
  - *¿Dónde invertir ese dinero?*
  - ...

- Un **sistema de gestión** establece e implementa los procesos que permiten a una organización realizar un producto o servicio de manera conforme a unas especificaciones dadas:
  - UNE-EN ISO 9001:2000. Sistemas de Gestión de la Calidad: Requisitos.
  - UNE-EN ISO 14001:1996. Sistemas de Gestión Medioambiental: Especificaciones y directrices para su utilización.
  - OHSAS 18001:1999. Sistemas de Gestión de la Seguridad y Salud en el Trabajo.
  - UNE 71502:2004. Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI).
  - ...
- La seguridad/calidad/gestión medioambiental... es un proceso, no un producto.
  - Ciclo PDCA (mejora continua).

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

- **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.

- La **gestión de la seguridad** consiste en la realización de las tareas necesarias para garantizar los niveles de seguridad exigibles en una organización.

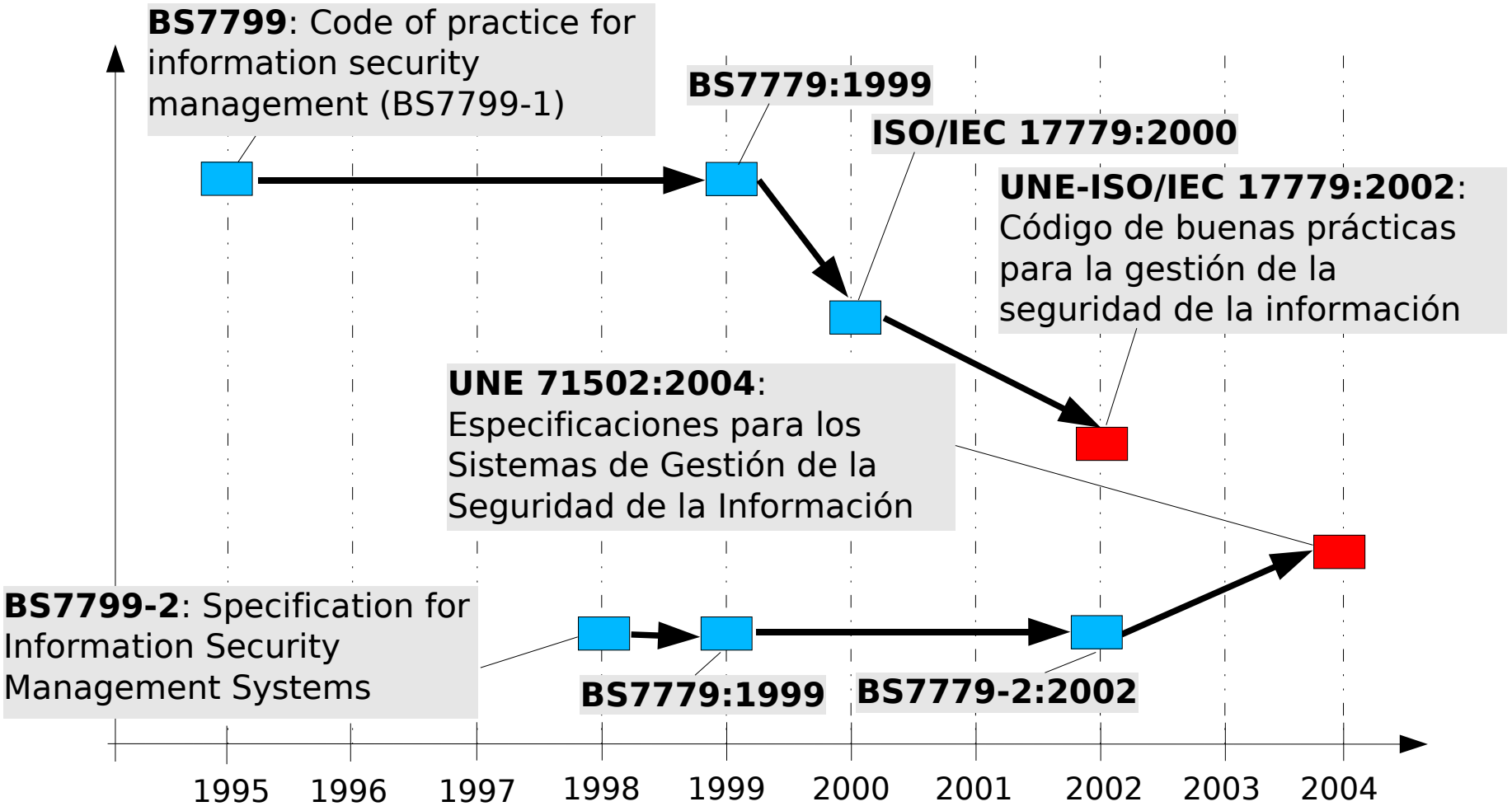
- Los **riesgos** no se eliminan: se gestionan.

- El establecimiento de un SGSI en la organización debe dar respuesta a las preguntas que nos planteábamos al principio: nos ayudará a **gestionar** nuestra seguridad.

- Podemos definir e implantar un SGSI atendiendo a múltiples criterios y estándares; dos de ellos destacan sobre los demás:
  - BS 7799-2:2002.
  - UNE 71502:2004.

- El fondo de ambas normas es muy similar: están basadas en controles y objetivos de control de ISO 17799.

SGSI: Normas *7799



SGSI: 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[1] de seguridad de la información más reconocida a nivel internacional.
- 36 objetivos de control y 127 controles.
- NO CERTIFICABLE.

1. Quizás técnica, pero no tecnológica...

- Norma que contiene las especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI):
  - Establecimiento
  - Implantación
  - Documentación
  - Evaluación
- Define la relación de procedimientos para establecer el SGSI: componente documental del sistema.
- No tiene equivalente ISO: aplicación nacional exclusivamente.
  - Norma ISO planificada para 2006 (???).
- CERTIFICABLE.

Repetimos:

La seguridad es un proceso, no un producto...

SGSI: Proceso

- El primer paso para definir un SGSI en la organización es responder a estas tres preguntas:
  - ¿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 cuestiones permitirán definir un Plan Director de Seguridad.

- Con el plan en la mano, ya podemos...
  - ...implantar.
  - ...gestionar.
  - ...medir.
    - ¿Mucho?, ¿Poco?, ¿A veces?, ¿Demasiado? ... no son términos adecuados.

- Con el SGSI implantado (total o parcialmente), podemos entrar en la fase de **auditoría** del sistema:
  - ¿Se ajusta a lo deseado?
  - ¿Ha sido implantado y se mantiene y ejecuta correctamente?
  - ¿Existen nuevos riesgos?
  - ¿Hay cambios que puedan afectar al SGSI?

- Si durante la auditoría se detectan **no conformidades** (desviaciones con respecto a la política), debemos corregirlas; si no se encuentran, debemos buscarlas.

- Comienza de nuevo el ciclo de mejora continua.

- Proceso similar a otros sistemas de gestión.

- La organización debe converger hacia un sistema de gestión único, capaz de agrupar Calidad, Medioambiente, Seguridad de la Información, etc.
  - Menores costes.
  - Ausencia de conflictos en los objetivos.
  - Simplificación del control.
  - Optimización de recursos.
  - ...

- No obstante, existen algunas diferencias críticas entre el SGSI y otros sistemas de gestión...

- Código de buenas prácticas (ISO 17799) tras la especificación del sistema de gestión.

- La seguridad de la información es un elemento que evoluciona rápidamente (especialmente, la inseguridad).
  - El control en **tiempo real** se hace imprescindible.
    - El seguimiento es importante en todo SG. En un SGSI, es **crítico**.
  - Si queremos que el SGSI prospere, se mantenga vivo en la organización y mejore con el tiempo, necesitamos **agilidad**.
    - Crítica al SG clásico: burocracia.
  - Concepto clave: **AUTOMATIZAR**.

- Una entidad independiente y competente afirma que un sistema es correcto y compromete en ello su palabra... por escrito.

- Proceso:
  - **Consultoría**. Ayuda a la organización para cumplir los requisitos especificados por la norma.
  - **Auditoría**.
    - Visita previa.
    - Auditoría inicial.
    - Plan de acciones correctoras.
    - **Certificación**.
    - Auditorías de seguimiento del sistema.

Certificación: ventajas

- Confianza, depositada en la entidad que certifica.
  - *Yo no digo que soy seguro, lo dice un tercero independiente.*

- Garantía de '*calidad de la seguridad*': mejora continua.

- Incluimos la seguridad a todos los niveles de la organización: beneficios para...
  - ... la propia organización.
  - ... los inversores.
  - ... los clientes.
  - ... los empleados.

Certificación: inconvenientes

- La certificación califica formalmente el sistema de gestión, no la seguridad técnica.
  - No es garantía de inmunidad.
- No se realizan auditorías de eficacia de los controles.
  - ¿Son adecuados? ¿Cumplen sus objetivos?
- Falta de cultura de seguridad en la organización.
  - Certificado como objetivo (“papelito”), no como reconocimiento.
- ¿Reclamo para piratas?

- Los problemas de seguridad rara vez son técnicos: suelen ser de gestión.
- Debemos **gestionar** nuestra seguridad: no es un producto, es un **proceso**.
  - *"Si alguien gusta de hablar de la Gestión de la Calidad de la Seguridad, no creo que vaya desencaminado"* (Mañas *dixit*).
- Un sistema de gestión debe contemplar la **mejora continua** del sistema: todo evoluciona, especialmente la (in)seguridad.
- La **certificación** de seguridad suele ser 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