Seguridad y Competencias Profesionales
Tema 3: Legislación y Normas en Materia de Seguridad Informática

Curso 2012–2013

Ingeniería en Informática (2° ciclo)

Departamento de Ingeniería Informática
Universidad de Cádiz

Cádiz, 15 de octubre de 2012

Índice

Introducción

- Los activos más importantes de una empresa son la información, junto a los procesos y sistemas que hacen uso de ella.
- En un ambiente competitivo de negocios, la información está amenazada por muchas fuentes. Conforme se incrementa la nueva tecnología, el número y tipo de amenazas se incrementa exponencialmente.
- Es necesario gestionar la seguridad, pero:
  - La seguridad no es un producto, es un proceso.
  - La seguridad no se compra, se gestiona.
- La forma de gestionar y parametrizar la seguridad es a través de un Sistema de Gestión de Seguridad de la Información (SGSI).

Sistema de Gestión de la Seguridad de la Información

Definición

Un SGSI (ISMS, *Information Security Management System*) es aquella parte del sistema general 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 en una organización.

Objetivos

- Gestionar los riesgos de la seguridad de la información, a fin de que consigamos la mayor fiabilidad del sistema.
- Asegurar la integridad, confidencialidad y disponibilidad de la información mediante un proceso sistemático y documentado.

Etapas de implantación de un SGSI

Etapas de desarrollo de un SGSI

1. Implantación de medidas básicas de seguridad por sentido común (copias de seguridad, etc.)
2. Adaptación a los requisitos de marco legal
3. Gestión integral de la seguridad de la información (SGSI)
4. Certificación de la gestión de seguridad: Necesidad de seguir unas normas y estándares

Elementos de un SGSI

Un SGSI está formado por los siguientes documentos:

1. Manual de seguridad: alcance, política y gestión de riesgos.
2. Procedimientos: operar y controlar eficazmente.
3. Instrucciones, listas de comprobación y formularios: cómo realizar las tareas y actividades.
4. Registros: gestión documental para evidenciar el grado de cumplimiento.

Implantación de un SGSI

Un SGSI sigue un plan de gestión de calidad PDCA.

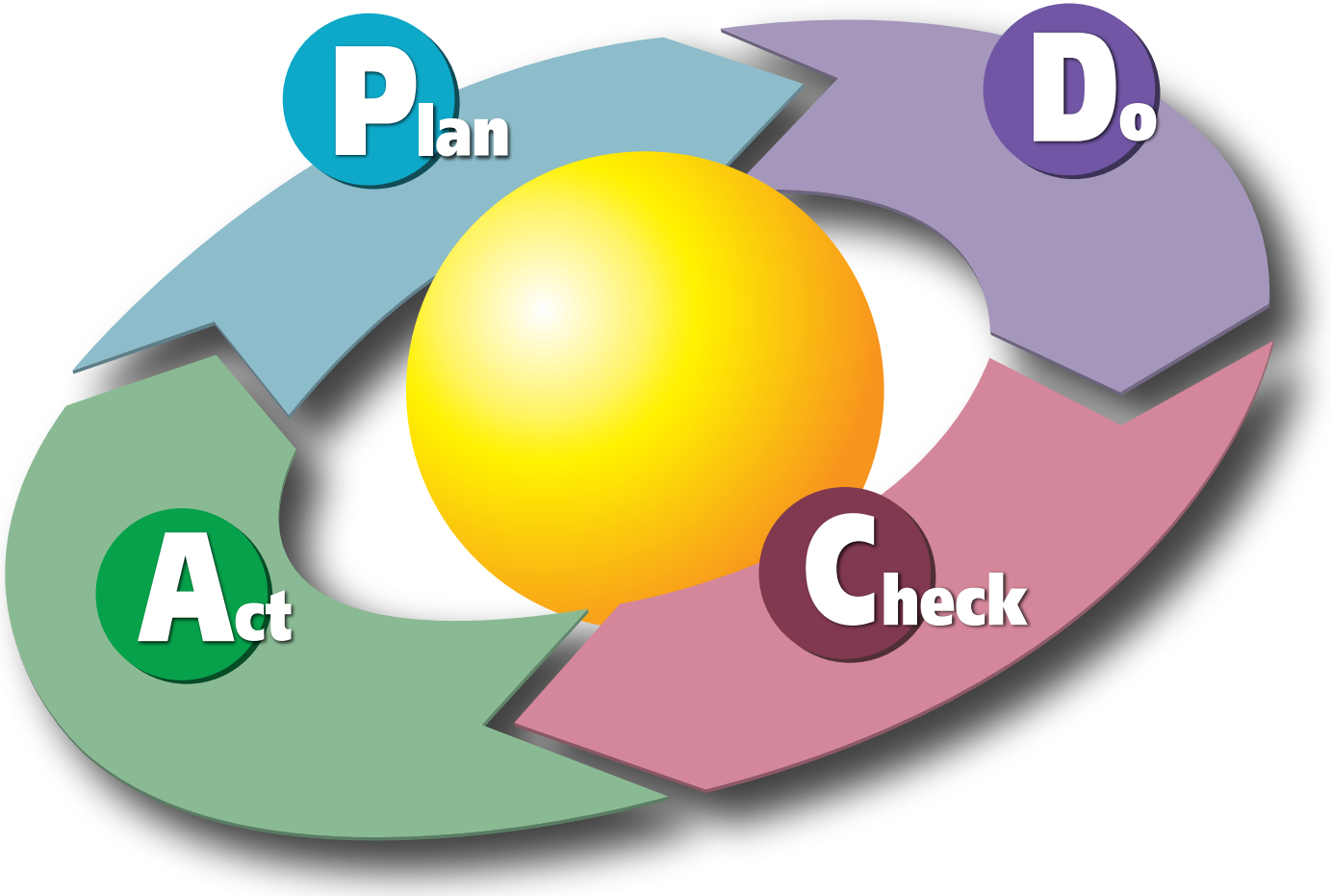


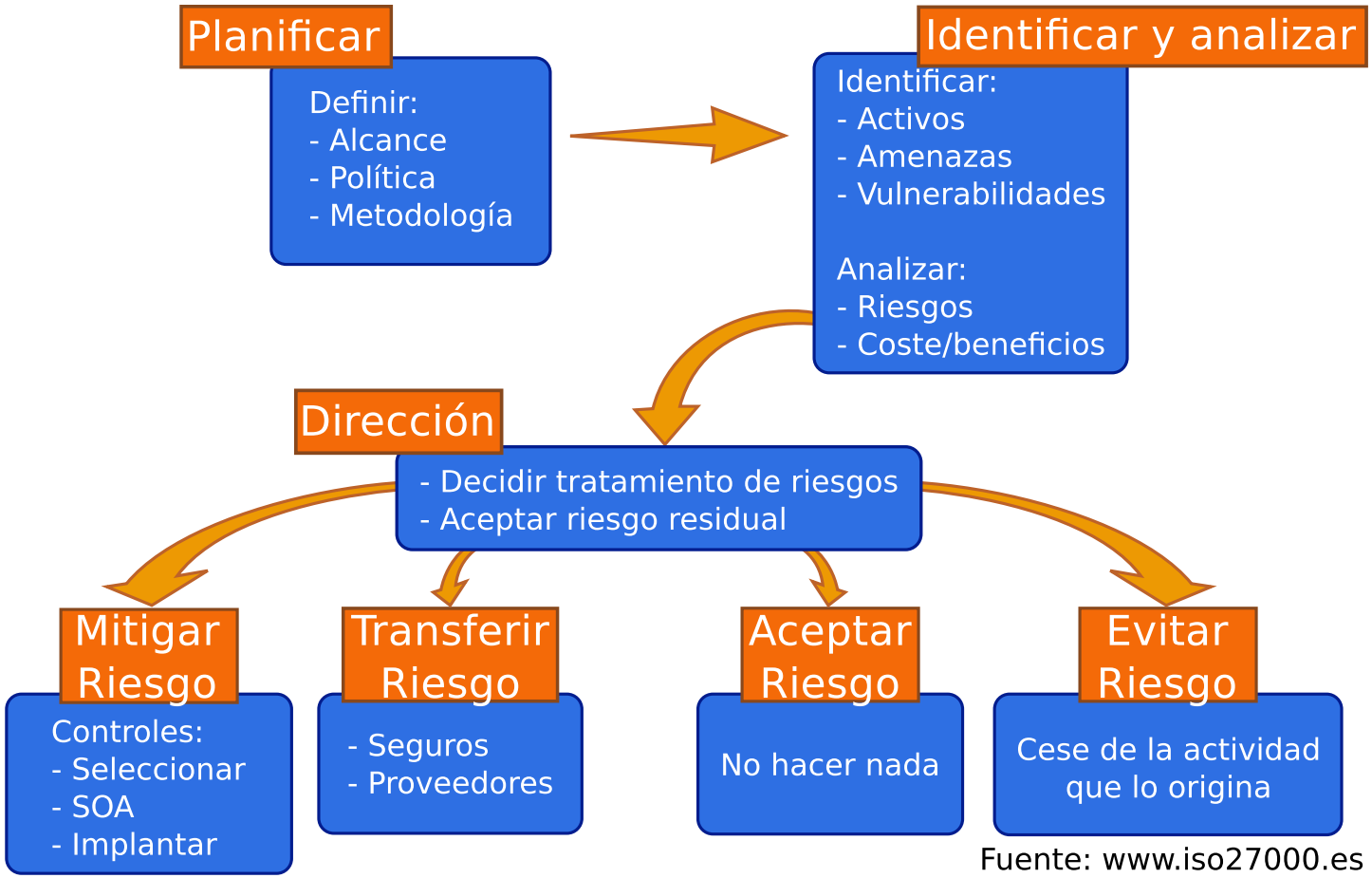
Figura de Karn G. Bulsuk (`http://blog.bulsuk.com/`)

Implantación de un SGSI (cont.)

Plan Selección y definición de medidas y procedimientos

- Definición del alcance del SGSI
- Definición de la política de seguridad: marco general, requisitos legales, etc.
- Definición de la metodología de evaluación del riesgo
- Identificación, análisis y evaluación de riesgos
- Tratamiento de riesgos
- Selección de los controles de seguridad para el tratamiento de riesgos

Implantación de un SGSI (cont.)



Fuente: www.iso27000.es

Implantación de un SGSI (cont.)

Do Implantación de medidas y procedimientos de mejora

- Implantación del plan de tratamiento de riesgos
- Implantanción de los controles de seguridad
- Definición de las métricas para controlar la efectividad de los controles
- Gestionar los recursos del SGSI
- Implantación de procedimientos y controles para detectar y responder a los incidentes de seguridad
- Programas de formación y concienciación del personal

Implantación de un SGSI (cont.)

Check Comprobación y verificación de las medidas implantadas

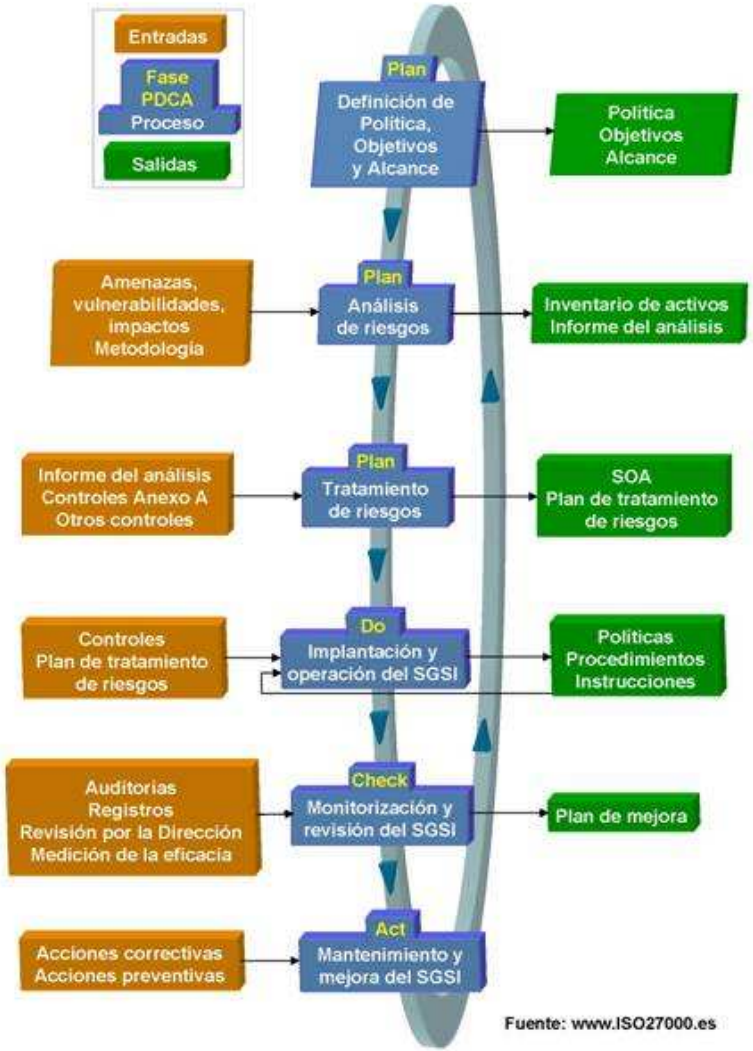
- Ejecutar procedimientos de monitorización y revisión
- Revisar la efectividad del SGSI
- Medir la efectividad de los controles de seguridad
- Revisar las evaluaciones de riesgos
- Actualizar planes y políticas de seguridad
- Registrar acciones y eventos que afecten al rendimiento y efectividad del SGSI
- Realizar auditorías internas
- Revisar el SGSI por la dirección

Implantación de un SGSI (cont.)

Act Actuación para corregir las deficiencias del sistema

- Implantar medidas identificadas
- Realizar acciones preventivas y correctivas
- Comunicar acciones y mejoras
- Asegurar que las mejoras alcanzan los objetivos

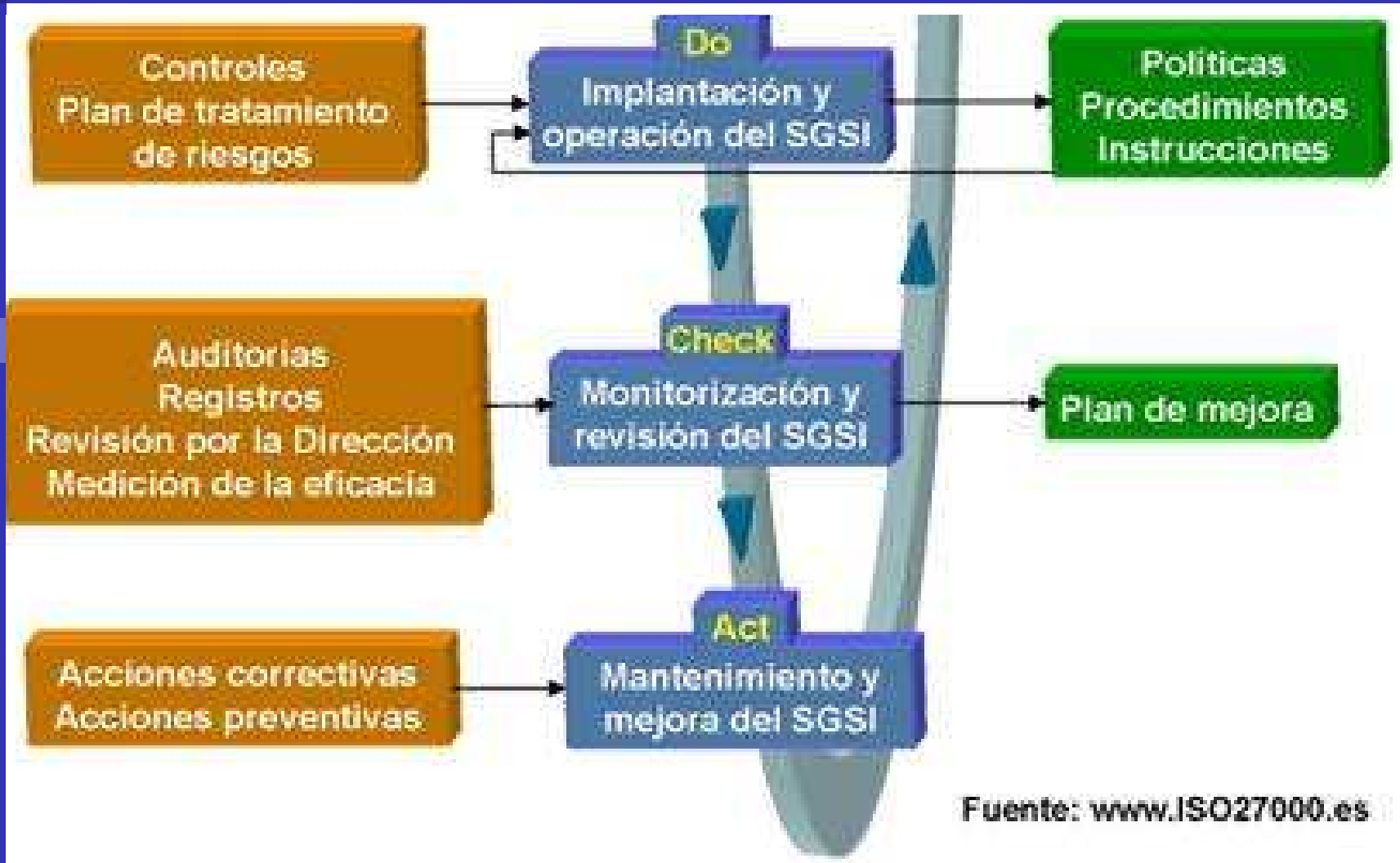
Implantación de un SGSI (cont.)



Implantación de un SGSI (cont.)

Implantación de un SGSI (cont.)

Implantación de un SGSI (cont.)



Organismos de estándares y normas

A nivel internacional

- ISO (*International Organization for Standardization*) fue creado en febrero de 1947. Consta con la representación de 153 países
- ISO e IEC (*International Electrotechnical Commission*) establecen un comité conjunto para las Tecnologías de la Información: JTC1 (*Joint Technical Committee*)
- Dentro de JTC1, el subcomité SC27 se encarga de los proyectos de seguridad, desglosándose en 5 grupos de trabajo:
  - WG1: SGSI (norma ISO 27000)
  - WG2: Mecanismos de seguridad y criptografía
  - WG3: Criterios de evaluación de la seguridad
  - WG4: Servicios y controles de seguridad
  - WG5: Tecnologías de gestión de identidad y privacidad

Organismos de estándares y normas (cont.)

A nivel nacional

- AENOR (Agencia Española de Normalización) es el subcomité espejo que coordina los trabajos de ISO en España.
- AEN/CTN 71/SC *Técnicas de Seguridad - Tecnología de la Información* es el espejo del subcomité SC27, con sus correspondientes grupos de trabajo GT1, GT2, GT3, GT4 Y GT5.

Historia de la familia ISO 27000

1995 BS 7799-1: código de buenas prácticas.

1998 BS 7799-2: especificación de SGSI.

1999 Revisión de BS 7799-1 y 7799-2.

2000 BS 7799-1 $\rightarrow$ ISO/IEC 17799:2000.

2002 Revisión de BS 7799-2.

2005 Revisión de ISO/IEC 17799:2000.

2005 BS 7799-2 $\rightarrow$ ISO/IEC 27001.

2007 ISO 17799 $\rightarrow$ ISO 27002.

Composición de la familia ISO 27000

ISO 27000 está formada por un conjunto de estándares

- ISO 27000 - ISO 27006: publicadas.
- ISO 27007 y 27008: publicadas en noviembre de 2011.
- Otras normas: ISO 27011, ISO 27013, ISO 27033, etc.

Normas ISO 27000

ISO 27000

Define el vocabulario básico.

ISO 27001

- Sustituye a la BS 7799-2.
- Es la norma principal que define los requisitos de un SGSI.
- Es la norma que permite certificar los SGSI por auditores externos.
- Contiene un anexo que resume los controles de seguridad que se pueden aplicar, que se encuentran en la norma ISO 27002.
- Traducida al español en el 2007 por AENOR, primera modificación disponible en diciembre de 2009.

La norma ISO 27000 (cont.)

ISO 27002

- Publicada el 1 de julio de 2007, traducida en diciembre de 2009 (anulando la UNE 71502 y la UNE-ISO/IEC 17799).
- Es un cambio de nomenclatura de ISO 17799:2005
- Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad.
- Define 39 objetivos de control, 133 controles, agrupados en 11 dominios.
- No es certificable.

ISO 27003

- Es una guía de implementación de un SGSI, uso del modelo PDCA y de sus requisitos.
- Está basado en el anexo B de la norma BS 7799-2.

La norma ISO 27000 (cont.)

ISO 27004

Especifica las métricas y las técnicas de medida para medir la eficacia de un SGSI y sus controles (fase "Check" del ciclo PDCA).

ISO 27005

- Guía para la gestión del riesgo de la seguridad de la información (fase "Plan" del ciclo PDCA).
- Basada en BS7799-3 (Marzo de 2006) e ISO 13335-3.

La norma ISO 27000 (cont.)

ISO 27006

Requisitos para la acreditación de entidades de auditoría y certificación de SGSI.

ISO 27007

Guía para la realización de auditorías internas y externas de SGSI y para su monitorización.

ISO 27008

Guía de mejores prácticas respecto a la auditoría de los controles específicos de seguridad (vistos en la ISO 27002).

Otras normas ISO

ISO 13335-3

- Directrices para la gestión de la seguridad.
- Técnicas de gestión de riesgos y criterios de selección de contramedidas.
- La parte 3 (evaluación de riesgos) y la parte 4 (selección de controles) han sido englobadas dentro de la norma ISO 27005.

ISO 15408

- Criterios comunes para reducir el nivel de riesgo.
- Permite seleccionar un conjunto de productos como contramedidas, certificando el nivel de aseguramiento que proporciona.

Normas españolas: UNE (AENOR)

UNE71501 IN

- Guía para la gestión de la seguridad de las tecnologías de la información.
- Está formada por tres normas:
  1. UNE71501-1 IN Parte 1: Conceptos y modelos para la seguridad TI.
  2. UNE71501-2 IN Parte 2: Gestión y planificación de la seguridad TI.
  3. UNE71501-3 IN Parte 3: Técnicas para la gestión de la seguridad TI.

Certificación del SGSI

- ISO 27001 es certificable a través de la norma ISO 27006.
- Las entidades de certificación deben estar acreditadas. En España, se realiza por la Entidad Nacional de Acreditación (ENAC).

Certificación del SGSI (cont.)