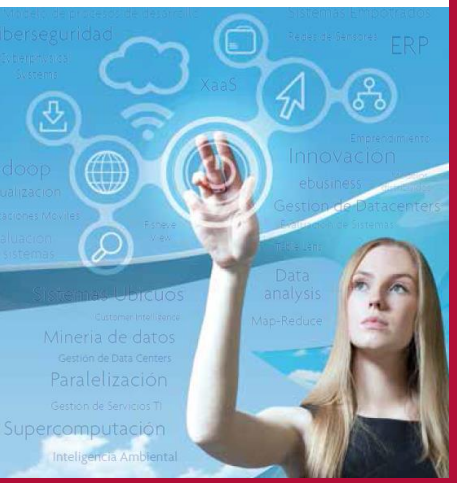
DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

Diseño de un Sistema de Gestión de Seguridad de la Información



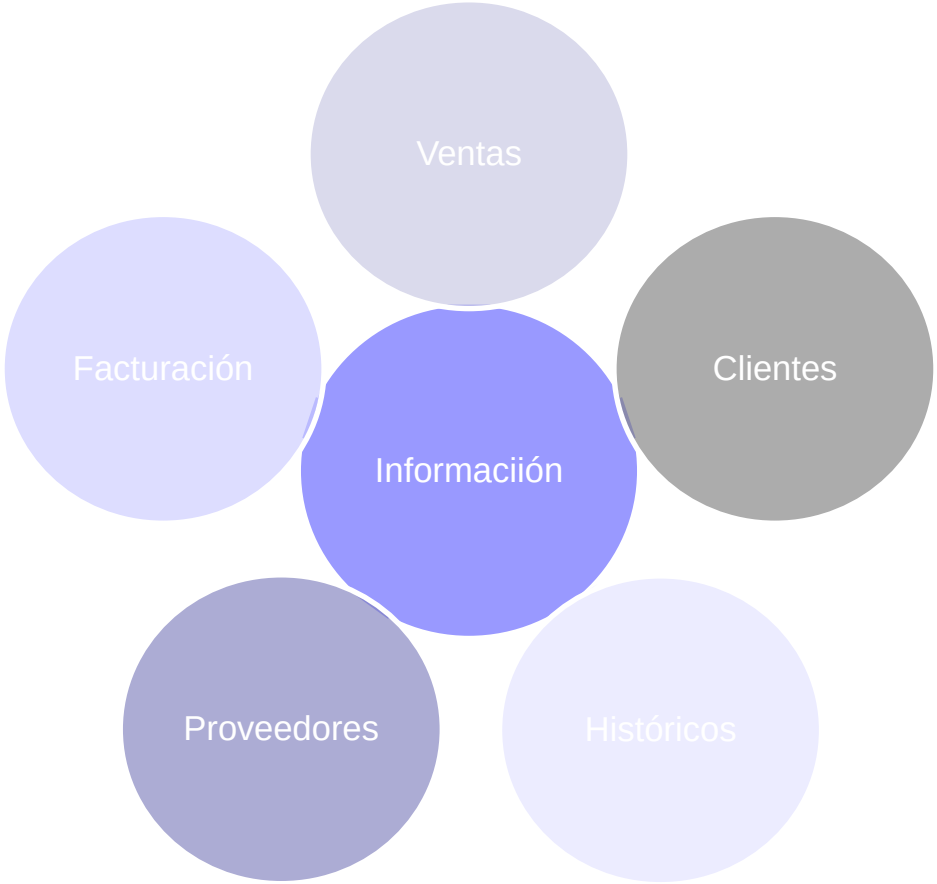
Enrique Arias
Universidad de Castilla–La Mancha

Índice

- Introducción
- Familia ISO 27000
- Introducción al SGSI
- Implantación de un SGSI

Índice

Introducción



Introducción

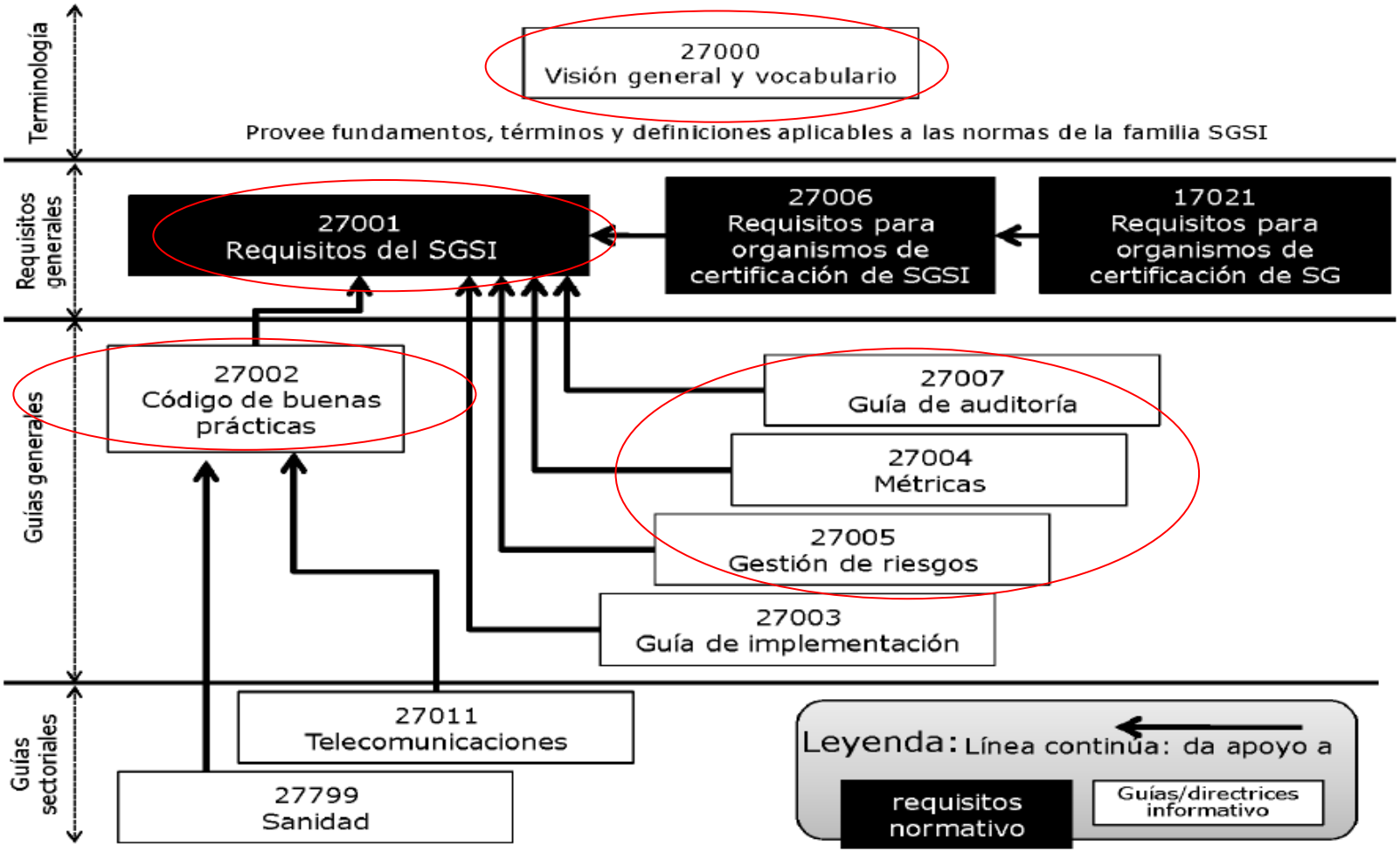
Índice

- Introducción
- Familia ISO 27000
- Introducción al SGSI
- Implantación de un SGSI

Familia 27000

- ISO/IEC 27000:2009 *Sistemas de Gestión de Seguridad de la Información. Visión de conjunto y vocabulario.*
- ISO/IEC 27001:2005 *Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.*
- ISO/IEC 27002:2005 *Código de buenas prácticas para la gestión de la seguridad de la información.*
- ISO/IEC 27003 *Guía para la implementación de los Sistemas de Gestión de Seguridad de la Información.*
- ISO/IEC 27004 *Gestión de la seguridad de la información. Métricas.*
- ISO/IEC 27005:2008 *Gestión de riesgos de seguridad de la información.*
- ISO/IEC 27006:2007 *Requisitos para entidades que auditan y certifican Sistemas de Gestión de la Seguridad de la Información (SGSI).*
- ISO/IEC 27007 *Guía para la auditoría de los Sistemas de Gestión de Seguridad de la Información (SGSI).*
- ISO/IEC 27011 *Guía para la gestión de la seguridad de la información para las organizaciones de telecomunicaciones basada en la Norma ISO/IEC 27002.*

Familia 27000



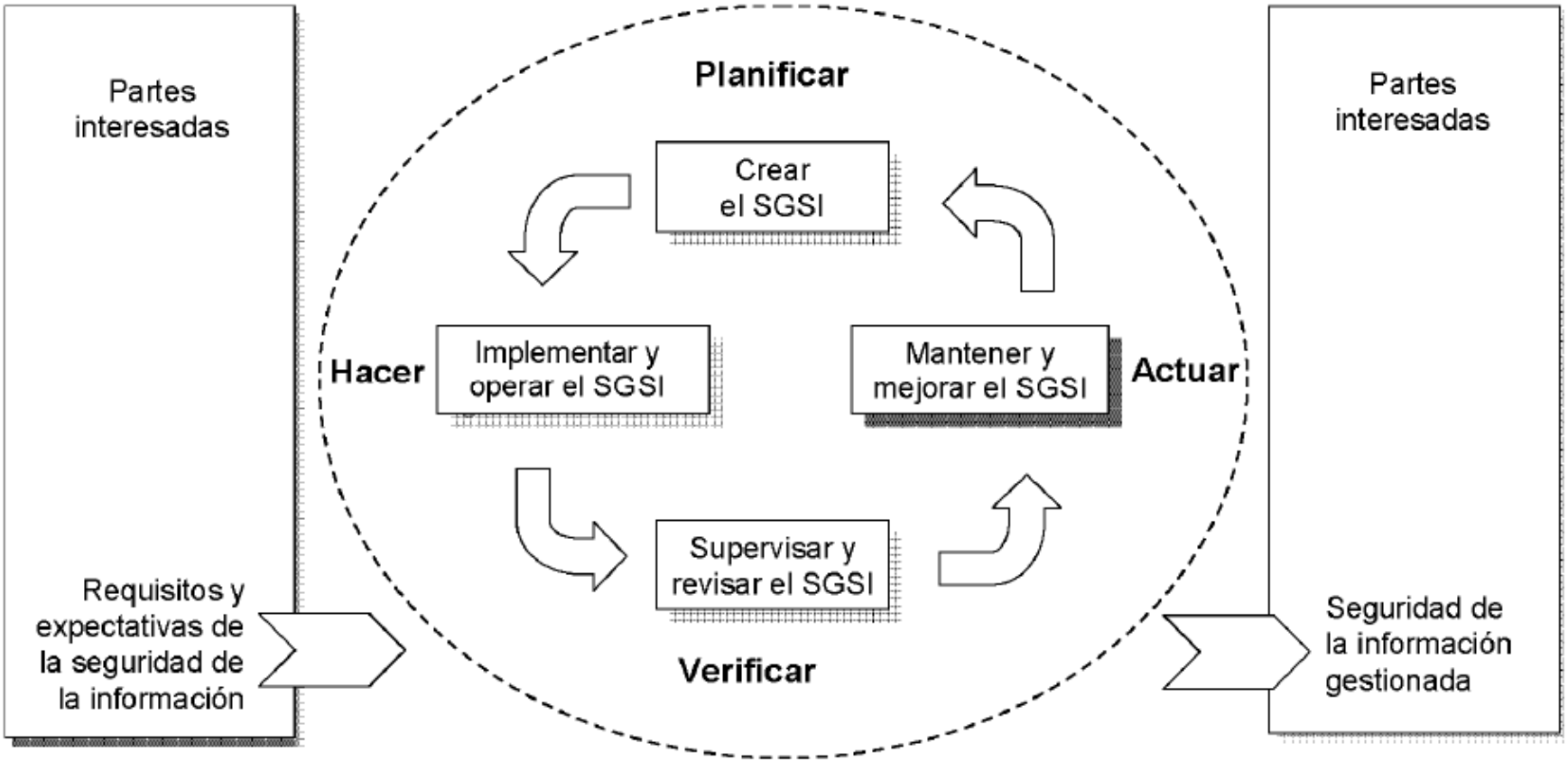
Índice

- Introducción
- Familia ISO 27000
- Introducción al SGSI
- Implantación de un SGSI

Introducción al SGSI

"SGSI proporciona un modelo para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los objetivos de negocio, basado en una apreciación del riesgo y en los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar con eficacia los riesgos" .

Introducción al SGSI



Introducción al SGSI

Planificar (creación del SGSI)	Definir la política, objetivos, procesos y procedimientos del SGSI relevantes para gestionar el riesgo y mejorar la seguridad de la información, con el fin de obtener resultados acordes con las políticas y objetivos generales de la organización.
Hacer (implementación y operación del SGSI)	Implementar y operar la política, controles, procesos y procedimientos del SGSI.
Verificar (supervisión y revisión del SGSI)	Evaluar y, en su caso, medir el rendimiento del proceso contra la política, los objetivos y la experiencia práctica del SGSI, e informar de los resultados a la Dirección para su revisión.
Actuar (mantenimiento y mejora del SGSI)	Adoptar medidas correctivas y preventivas, en función de los resultados de la auditoría interna del SGSI y de la revisión por parte de la dirección, o de otras informaciones relevantes, para lograr la mejora continua del SGSI.

Planificar: Analizar la situación de la organización, establecer los objetivos generales y las metas, y elaborar los planes para alcanzarlos.
Hacer: Hacer lo previsto.
Verificar: Medir/verificar que la medida logra cumplir los objetivos previstos.
Actuar: Aprender de los errores para mejorar las actividades para lograr mejores resultados.

Índice

- Introducción
- Familia ISO 27000
- Introducción al SGSI
- Implantación de un SGSI

Implantación de un SGSI

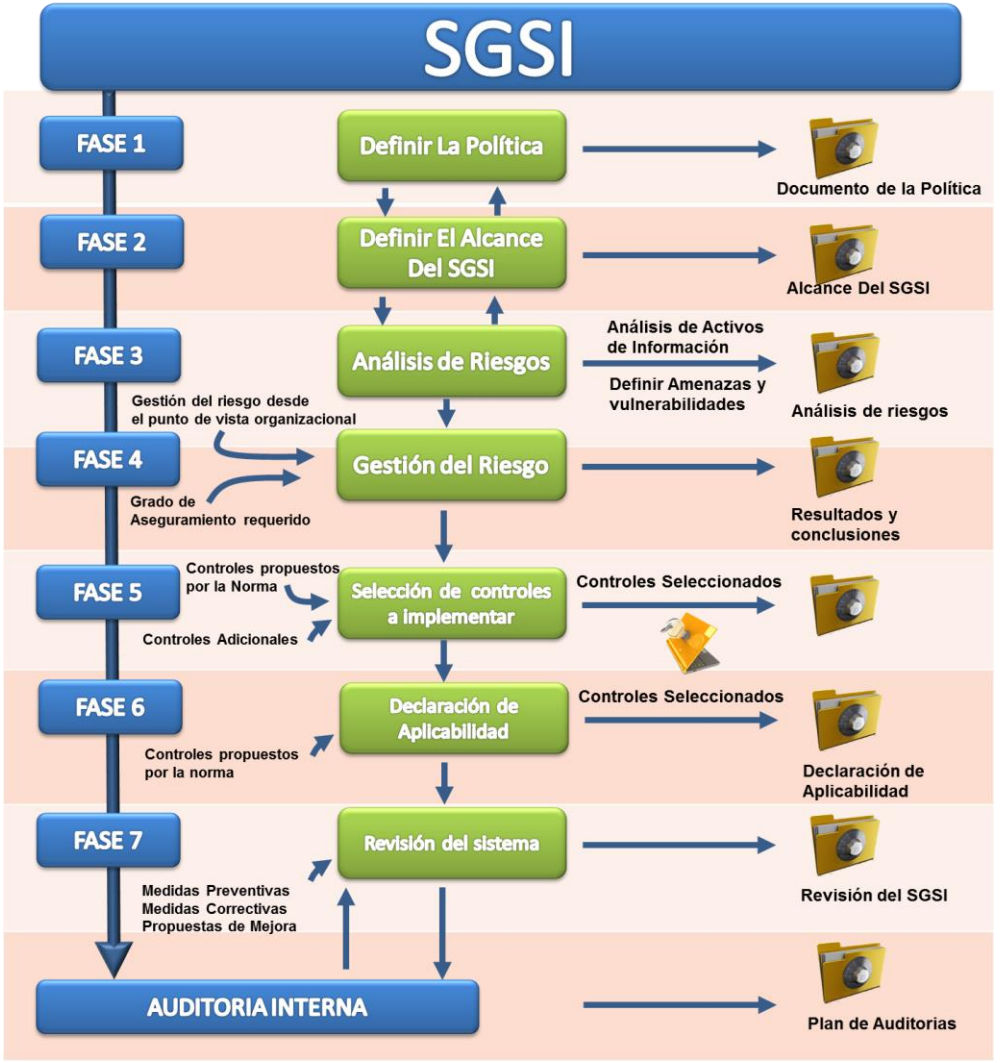
"El objetivo es diseñar o implantar un SGSI que se ajuste lo más posible a la realidad de las organizaciones, que contemple las medidas de seguridad mínimas e imprescindibles para proteger la información y cumplir la norma, pero que consuma pocos recursos e introduzca el menor número de cambios posibles"

Implantación de un SGSI
Creación y gestión

- Participación de dirección
  - Alcance
    - Sector
    - Ubicación
    - Activos
    - …
  - Políticas del SGSI
    - Regulación
    - Misión, visión y objetivos
    - KPI y KRI
    - Comunicación
  - Metodología evaluación riesgo
    - Apetito al riesgo
    - Riesgo residual
  - Designar personal responsable
  - Supervisión y revisión

Implantación de un SGSI
Creación y gestión

- Documentación básica
  - Políticas
  - Procedimientos
  - Registros

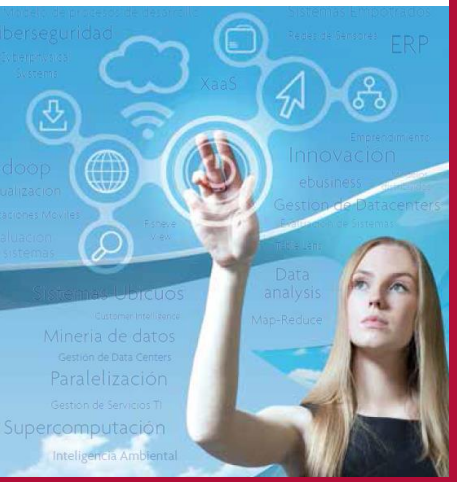


Implantación de un SGSI
Creación y gestión 17

- Documentación detallada
  - Políticas y objetivos del SGSI, estructura de la empresa, responsabilidades, etc.
  - Inventario de activos: nombre, categoría, ubicación, propietario, valor (CIA)
  - Alcance del SGSI.
  - Procedimientos y mecanismos de control (ISO 27002)
    - ¿Está implementado?
    - ¿Ayuda a reducir el riesgo?
    - ¿Coste?
    - ¿Coste mantenimiento?
    - ¿Porqué otros controles no se escogen?
  - Metodología de gestión del riesgo, p.e., MAGERIT.
  - Informe evaluación.
  - Plan de tratamiento: Objetivos de seguridad ←→Métricas
  - Registros o evidencias.

DEPARTAMENTO DE SISTEMAS INFORMÁTICOS

Diseño de un Sistema de Gestión de Seguridad de la Información



Enrique Arias
Universidad de Castilla–La Mancha