

Estándar de Seguridad de Información

ISO 27001:2005

ISO/IEC 17799:2005

Estándares de Seguridad de la Información

ISO 27001:2005

- ✓ Orientado a establecer un sistema gerencial para minimizar riesgos y proteger la información.
- ✓ Especificación para la gestión del sistema de seguridad de la información.
- ✓ Usado para la certificación.

ISO/IEC 17799:2005

- ✓ Código de práctica para la gestión de la seguridad de la información.
- ✓ Usado como documento de referencia.
- ✓ Provee un juego comprensivo de controles de seguridad.
- ✓ Basado en la mejores prácticas de seguridad de la información.

Historia

1993

1995

1998

1999

2000

2005

2007

Código de Práctica

ISO 27002

ISO 17799

BS 7799-1

Norma Británica

Código de Práctica

Par Consistente

Sistema de Gestión de SI

ISO 27001

BS 7799-2

BS 7799-2

La serie 27000

ISO 27001

Sistema de Gestión
de Seguridad de la
Información (SGSI)

ISO 27002

(ISO/IEC 17799:2005)
Código de Práctica
(Abril 2007)

ISO 27000

Fundamentos
y Vocabulario
(en desarrollo)

ISO 27003

Guía de Implementación
del SGSI
(2008)

ISO 27006

Requisitos para la acreditación
de entidades de Auditoría y
Certificación de un SGSI

ISO 27004

Métricas para determinar
la eficacia de un SGSI
(2008)

ISO 27005

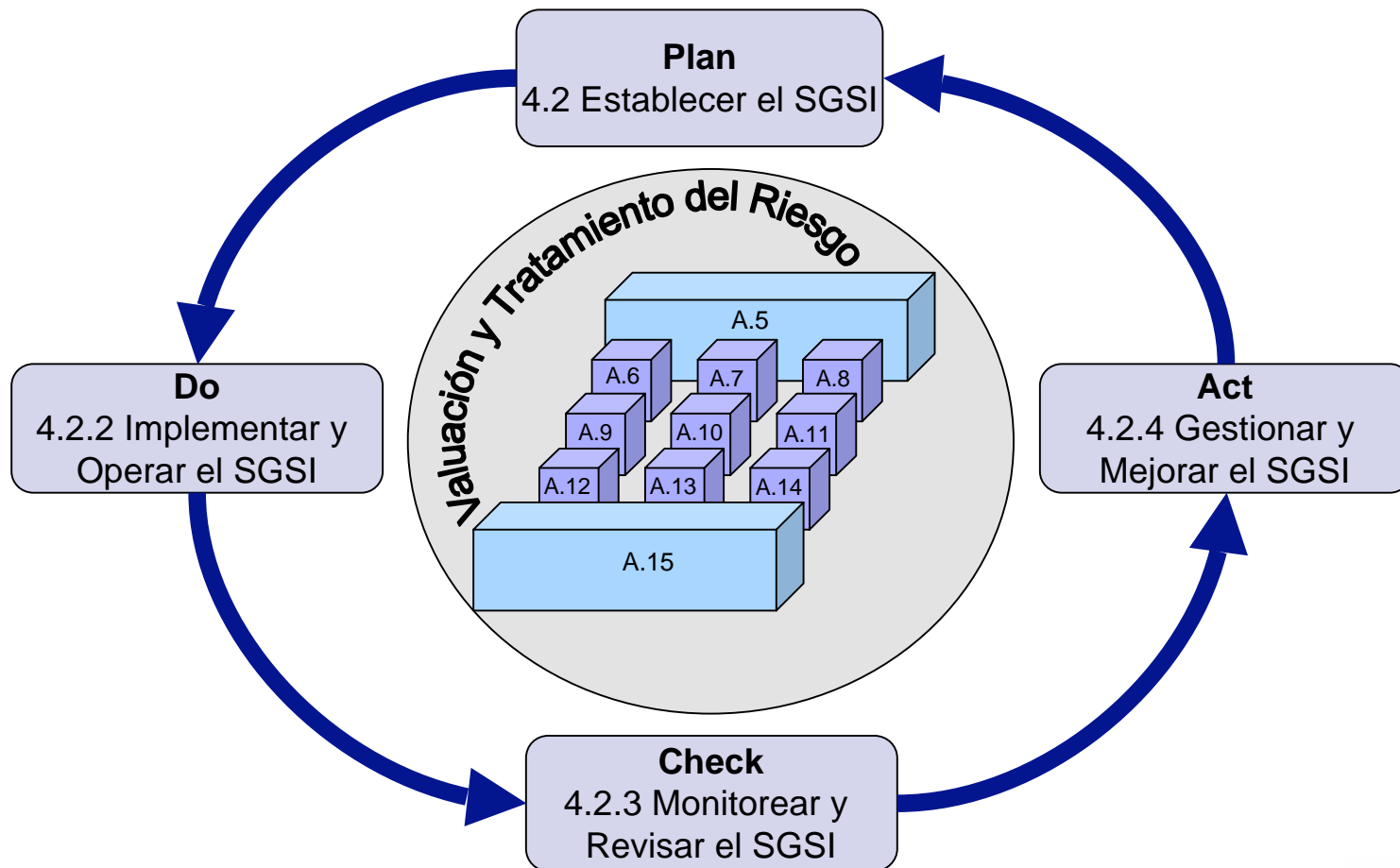
Guía para la Gestión
de Riesgo de SI
(2008)

COMPONENTES

ISO 27001:2005

ISO/IEC 17799:2005

Modelo Plan-Do-Check-Act (PDCA)



Metodología de Implementación

- ✓ Identificar necesidades.
- ✓ Inventario de activos de información.
- ✓ Evaluación del riesgo
 - ✓ Vulnerabilidades → Amenazas → Probabilidades → Impactos → Riesgos
- ✓ Selección e implementación de controles.
- ✓ Definición e implantación de métricas.
- ✓ Educación y concienciación del personal.
- ✓ Monitoreo y registro de incidencias.
- ✓ Realización de auditorías internas.
- ✓ Mejora continua del SGSI.

Componentes del Estándar ISO 27001:2005

- ✓ 0 Introducción
- ✓ 1 Campo de aplicación
- ✓ 2 Referencias normativas
- ✓ 3 Términos y definiciones
- ✓ 4 Sistema de gestión de la seguridad de la información
- ✓ 5 Responsabilidades de la Dirección
- ✓ 6 Auditorías internas del SGSI
- ✓ 7 Revisión del SGSI por la Dirección
- ✓ 8 Mejora de SGSI
- ✓ Anexo A Resumen de controles
- ✓ Anexo B Relación con los principios de la OCDE
- ✓ Anexo C Correspondencia con otras normas
- ✓ Bibliografía

Anexo de Controles

- A.5 Política de seguridad
- A.6 Organización de la seguridad de la información
- A.7 Gestión de activos
- A.8 Seguridad ligada a los recursos humanos
- A.9 Seguridad física y del entorno
- A.10 Gestión de comunicaciones y operaciones
- A.11 Control de accesos
- A.12 Adquisición, desarrollo y mantenimiento de sistemas de Información
- A.13 Gestión de incidentes de seguridad de la información
- A.14 Gestión de continuidad del negocio
- A.15 Conformidad

Beneficios

- ✓ Utilizar un modelo comprobado y repetible
- ✓ Crear resultados consistentes
- ✓ Obtención de métricas de control cuantificables y objetivas
- ✓ Claridad e institucionalidad en los procesos de seguridad de información
- ✓ Mayor comprensión de los riesgos a los que está expuesto el negocio
- ✓ Base para lanzar iniciativas de cultura de seguridad
- ✓ Poder lanzar al mercado nuevos productos con mayor confianza
- ✓ Mayor protección de la imagen institucional
- ✓ Disminuir desviaciones con relación a los requerimientos de la autoridad (mejorar cumplimiento de auditorias CNBV)
- ✓ Lanzamiento de campañas de mercadotecnia utilizando la certificación como argumento para generación de confianza