

**ISO-27001:2005**

**Giovanni Zuccardi  
Juan David Gutiérrez**

**Septiembre de 2006**

## **CONTENIDO**

Evolución del estándar  
Familia 2700x  
En que consiste 27001

## ISO-27001:2005

### Evolución del estándar

- 1995** BS 7799-1:1995 (Norma británica)
- 1999** BS 7799-2:1999 (Norma británica)
- 1999** Revisión BS 7799-1:1999
- 2000** ISO/IEC 17799:2000 (Norma internacional código de prácticas)
- 2002** Revisión BS 7799-2:2002
- 2004** UNE 71502 (Norma española) UNE ISO 27001:
- 2005** Revisión ISO/IEC 17799:2005
- 2005** Revisión BS 7799-2:2005
- 2005** ISO/IEC 27001:2005 (Norma internacional certificable)

Actualmente el **ISO-27001:2005** es el único estándar aceptado internacionalmente para la administración de la seguridad de la información y aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad. Se debe dejar claro que este es la versión actual del **ISO-17799:2002**.

La ISO 27001 le permite:

1. Diseñar una herramienta para la implementación del sistema de gestión de seguridad de la información teniendo en cuenta la política, la estructura organizativa, los procedimientos y los recursos.
2. A la dirección gestionar las políticas y los objetivos de seguridad en términos de integridad, confidencialidad y disponibilidad.
3. Determinar y analizar los riesgos, identificando amenazas, vulnerabilidades e impactos en la actividad empresarial.
4. Prevenir o reducir eficazmente el nivel de riesgo mediante la implantación de los controles adecuados, preparando la organización ante posibles emergencias, garantizando la continuidad del negocio [ICONTEC06].

### Familia 2700x

El conjunto de estándares que aportan información de la familia ISO-2700x que se puede tener en cuenta son:

- **ISO 27000** (2007) Vocabulario y Definiciones
- **ISO 27001** (2005) Estándar Certificable ya en Vigor (revised BS 7799 Part 2:2005) – Publicado el 15 de octubre del 2005
- **ISO 27002** (2007) Código de Buenas Prácticas relevo de ISO 17799 Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005
- **ISO 27003** (2008) Guía para la Implantación (bajo desarrollo)
- **ISO 27004** (2008) Métricas e Indicadores(bajo desarrollo)

- **ISO 27005** (2008) Gestión de Riesgos (BS 7799-3:2006)
- **ISO 27006** (2007) Continuidad de Negocio / Recuperación Desastres (BC/DR)

## **En que consiste**

La propuesta de esta norma, no está orientada a despliegues tecnológicos o de infraestructura, sino a aspectos netamente organizativos, es decir, la frase que podría definir su propósito es "Organizar la seguridad de la información", por ello propone toda una secuencia de acciones tendientes al "establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del **ISMS** (Information Security Management System)". El ISMS, es el punto fuerte de este estándar.

Los detalles que conforman el cuerpo de esta norma, se podrían agrupar en **tres grandes líneas**:

- **ISMS.**
- **Valoración de riesgos (Risk Assessment)**
- **Controles**

El desarrollo de estos puntos y la documentación que generan, será tratado continuación. Se tendrá en cuenta la misma enumeración y los puntos que se desarrollan en la norma

## **0. Introducción:**

### **0.1 General:**

Este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS, la adopción del ISMS debe ser una decisión estratégica de la organización, pues el mismo está influenciado por las necesidades y objetivos de la misma, los requerimientos de seguridad, los procesos, el tamaño y la estructura de la empresa, la dinámica que implica su aplicación, ocasionará en muchos casos la escalada del mismo, necesitando la misma dinámica para las soluciones.

### **0.2. Aproximación (o aprovechamiento) del modelo:**

Este estándar internacional adopta un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el ISMS en una organización. Una organización necesita identificar y administrar cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un "proceso". A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una realimentación de los mismos.

Este estándar internacional adopta también el modelo “Plan-Do-Check-Act” (PDCA), el cual es aplicado a toda la estructura de procesos de ISMS, y significa lo siguiente:

- **Plan** (Establecer el ISMS): Implica, establecer a política ISMS, sus objetivos, procesos, procedimientos relevantes para la administración de riesgos y mejoras para la seguridad de la información, entregando resultados acordes a las políticas y objetivos de toda la organización.
- **Do** (Implementar y operar el ISMS): Representa la forma en que se debe operar e implementar la política, controles, procesos y procedimientos.
- **Check** (Monitorizar y revisar el ISMS): Analizar y medir donde sea aplicable, los procesos ejecutados con relación a la política del ISMS, evaluar objetivos, experiencias e informar los resultados a la administración para su revisión.
- **Act** (Mantener y mejorar el ISMS): Realizar las acciones preventivas y correctivas, basados en las auditorías internas y revisiones del ISMS o cualquier otra información relevante para permitir la continua mejora del ISMS.

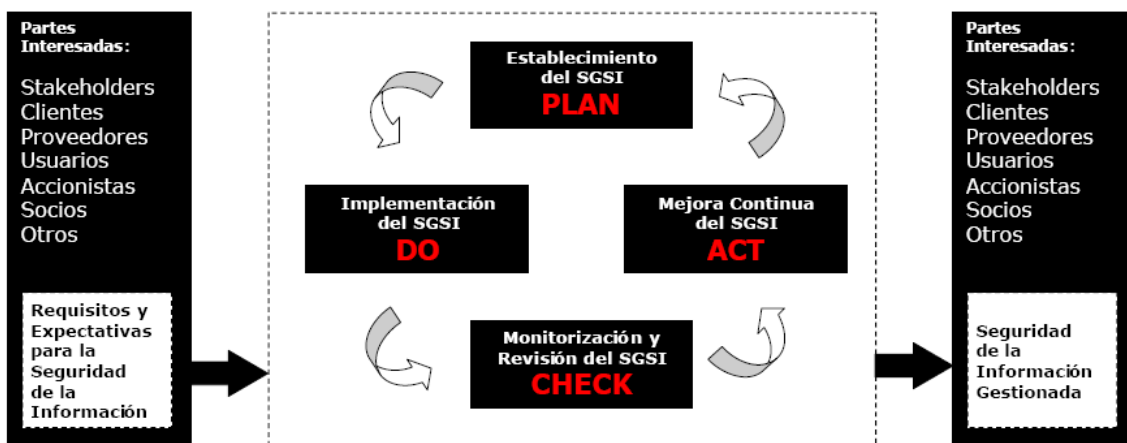
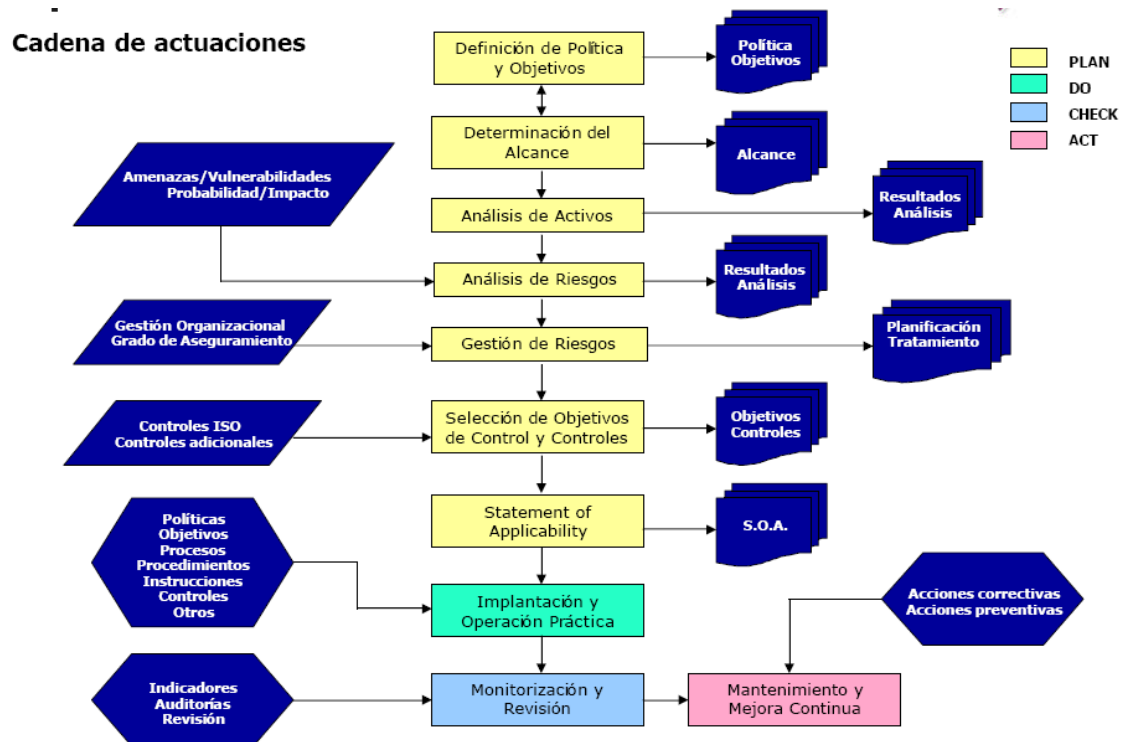


Figura 1.1: Representación del modelo “Plan-Do-Check-Act”.



**Figura 1.4:** Metodología de un SGSI según ISO 27001

## 1.2. Aplicación:

Los requerimientos de este estándar internacional, son genéricos y aplicables a la totalidad de las organizaciones. La exclusión de los requerimientos especificados en las cláusulas 4, 5, 6, 7 y 8, no son aceptables cuando una organización solicite su conformidad con esta norma.

Estas cláusulas son:

4. ISMS.
5. Responsabilidades de la Administración
6. Auditoría Interna del ISMS
7. Administración de las revisiones del ISMS
8. Mejoras del ISMS.

(Estas cláusulas realmente conforman el cuerpo principal de esta norma)

Cualquier exclusión a los controles detallados por la norma y denominados como "necesarios" para satisfacer los criterios de aceptación de riesgos, debe ser justificada y se debe poner de manifiesto, o evidenciar claramente los criterios por los cuales este riesgo es asumido y aceptado.

## 2. Normativas de referencia:

Para la aplicación de este documento, es indispensable tener en cuenta la última versión de:

“ISO/IEC 17799:2005, *Information technology — Security techniques — Code of practice for information security management*”

### **3. Términos y definiciones:**

La siguiente terminología aplica a esta norma:

3.1. Recurso (Asset): Cualquier cosa que tenga valor para la organización.

3.2. Disponibilidad (availability): Propiedad de ser accesible y usable bajo demanda por una entidad autorizada.

3.3. Confidencialidad (confidentiality): Propiedad que la información no esté disponible o pueda ser descubierta por usuarios no autorizados, entidades o procesos.

3.4. Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.

3.5. Eventos de seguridad de la información: Ocurrencia de un evento identificado sobre un sistema, servicio o red, cuyo estado indica una posible brecha en la política de seguridad de la información o fallo en el almacenamiento de la misma, también cualquier situación previa desconocida que pueda ser relevante desde el punto de vista de la seguridad.

3.6. Incidente de seguridad: uno o varios eventos de seguridad de la información, no deseados o inesperados que tienen una cierta probabilidad de comprometer las operaciones de la empresa y amenazan a la seguridad de la información.

3.7. Sistema de administración de la seguridad de la información (ISMS: Information Security Management System): Parte de los sistemas de la empresa, basado en el análisis de riesgo de negocio, cuya finalidad es establecer, implementar, operar, monitorizar, revisar, mantener y mejorar la seguridad de la información.

NOTA: el ISMS incluye las políticas, planes, actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

3.8. Integridad: Propiedad de salvaguardar la precisión y completitud de los recursos.

3.9. Riesgo residual: El riesgo remanente luego de una amenaza a la seguridad.

3.10. Aceptación de riesgo: Decisión de aceptar un riesgo.

3.11. Análisis de riesgo: Uso sistemático de la información para identificar fuentes y estimar riesgos.

3.12. Valoración de riesgo: Totalidad de los procesos de análisis y evaluación de riesgo.

3.13. Evaluación de riesgo: Proceso de comparar los riesgos estimados contra los criterios de riesgo establecidos o dados, para determinar el grado de significativo del riesgo.

3.14. Administración del riesgo: Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.

3.15. Tratamiento del riesgo: Proceso de selección e implementación de mediciones para modificar el riesgo.

3.16. Declaración de aplicabilidad: Documento que describe los objetivos del control, y los controles que son relevantes y aplicables a la organización del ISMS.

#### **4. ISMS (Information Security Managemet System).**

4.1. Requerimientos generales:

La organización, establecerá, implementará, operará, monitorizará, revisará, mantendrá y mejorará un documentado ISMS en el contexto de su propia organización para las actividades globales de su negocio y de cara a los riesgos. Para este propósito esta norma el proceso está basado en el modelo PDCA comentado en el punto 0.2.

4.3.2. Control de documentos:

Todos los documentos requeridos por el ISMS serán protegidos y controlados. Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

- Aprobar documentos y prioridades o clasificación de empleo.
- Revisiones, actualizaciones y reaprobaciones de documentos.
- Asegurar que los cambios y las revisiones de documentos sean identificados.
- Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas.
- Asegurar que los documentos permanezcan legibles y fácilmente identificables.
- Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.
- Asegurar que los documentos de origen externo sean identificados.
- Asegurar el control de la distribución de documentos.
- Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito

#### **5. Responsabilidades de administración:**

5.1. La administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del ISMS a través de:

- Establecimiento de la política del ISMS
- Asegurar el establecimiento de los objetivos y planes del ISMS.
- Establecer roles y responsabilidades para la seguridad de la información.

- Comunicar y concienciar a la organización sobre la importancia y apoyo necesario a los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una continua mejora en este aspecto.
- Proveer suficientes recursos para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el ISMS (5.2.1).
- Decidir los criterios de aceptación de riesgos y los niveles del mismo.
- Asegurar que las auditorías internas del ISMS, sean conducidas y a su vez conduzcan a la administración para la revisión del ISMS (ver 7.)

#### 5.2.2. Formación, preparación y competencia:

La organización asegurará que todo el personal a quien sean asignadas responsabilidades definidas en el ISMS sea competente y esté en capacidad de ejecutar las tareas requeridas, para ello deberá proveer las herramientas y capacitación necesaria (Documento: Planificación, guías y programas de formación y preparación).

### **6. Auditoría interna del ISMS:**

La organización realizará auditorías internas al ISMS a intervalos planeados para determinar si los controles, sus objetivos, los procesos y procedimientos continúan de conformidad a esta norma y para analizar y planificar acciones de mejora. Ninguna persona podrá auditar su propio trabajo, ni cualquier otro que guarde relación con él.

La responsabilidad y requerimientos para el planeamiento y la conducción de las actividades de auditoría, los informes resultantes y el mantenimiento de los registros será definido en un procedimiento

### **7. Administración de las revisiones del ISMS:**

Las revisiones mencionadas en el punto anterior deberán llevarse a cabo al menos una vez al año para asegurar su vigencia, adecuación y efectividad. Estas revisiones incluirán valoración de oportunidades para mejorar o cambiar el ISMS incluyendo la política de seguridad de la información y sus objetivos. Los resultados de estas revisiones, como se mencionó en el punto anterior serán claramente documentados y los mismos darán origen a esta actividad.

Esta actividad está constituida por la revisión de entradas (7.2.) y la de salidas (7.3.) y dará como resultado el documento correspondiente.

### **8. Mejoras al ISMS**

La organización deberá mejorar continuamente la eficiencia del ISMS a través del empleo de la política de seguridad de la información, sus objetivos, el resultado de las auditorías, el análisis y monitorización de eventos, las acciones preventivas y correctivas y las revisiones de administración.

## 8.2. Acciones correctivas:

La organización llevará a cabo acciones para eliminar las causas que no estén en conformidad con los requerimientos del ISMS con el objetivo de evitar la recurrencia de los mismos. Cada una de estas acciones correctivas deberá ser documentada

**El anexo A** de esta norma propone una detallada tabla de los controles, los cuales quedan agrupados y numerados de la siguiente forma:

A.5 Política de seguridad

A.6 Organización de la información de seguridad

A.7 Administración de recursos

A.8 Seguridad de los recursos humanos

A.9 Seguridad física y del entorno

A.10 Administración de las comunicaciones y operaciones

A.11 Control de accesos

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.13 Administración de los incidentes de seguridad

A.14 Administración de la continuidad de negocio

A.15 Cumplimiento (legales, de estándares, técnicas y auditorías)

**El anexo B**, que es informativo, a su vez proporciona una breve guía de los principios de OECD (guía de administración de riesgos de sistemas de información y redes - París, Julio del 2002, "www.oecd.org") y su correspondencia con el modelo PDCA.

Por último el **Anexo C**, también informativo, resume la correspondencia entre esta norma y los estándares ISO 9001:2000 y el ISO 14001:2004

## **Figuras**

**Figura 1.1:** Representación del modelo "Plan-Do-Check-Act".

**Figura 1.2:** Metodología de un SGSI según ISO 27001

## **Bibliografía**

[AnISO05] ANÁLISIS DE ISO-27001:2005, Alejandro Corletti Estrada  
Abril de 2006. Disponible en:

<http://www.mastermagazine.info/informes/9544.php>

[ICONTEC06] Instituto Colombiano de Normas Técnicas y  
Certificación Disponible en:

<http://www.icontec.org.co/MuestraContenido.asp?ChannelId=632>

[SiGeISO06] Sistema de Gestión de Seguridad de la Información  
según ISO 27001:2005. 22 de junio de 2006. José Manuel Fernández  
Domínguez Disponible en:

<http://www.nexusasesores.com/docs/ISO27001-norma-e-implantacion-SGSI.pdf>

[ISO2700106] ISO27001. Portal de ISO 27001 en español. Disponible  
en: <http://www.iso27000.es/iso27000.html>