

# ISO 27000

## Contenidos

1. Origen
2. La serie 27000
3. Contenido
4. Beneficios
5. ¿Cómo adaptarse?
6. Aspectos Clave.

La información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados -o en fase de desarrollo- por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En este apartado se resumen las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información (SGSI) basado en ISO 27001.

Acceda directamente a las secciones de su interés a través del submenú de la izquierda o descargue en .pdf el documento completo.

## 1. Origen

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

- 1979 Publicación BS 5750 - ahora ISO 9001
- 1992 Publicación BS 7750 - ahora ISO 14001
- 1996 Publicación BS 8800 - ahora OHSAS 18001

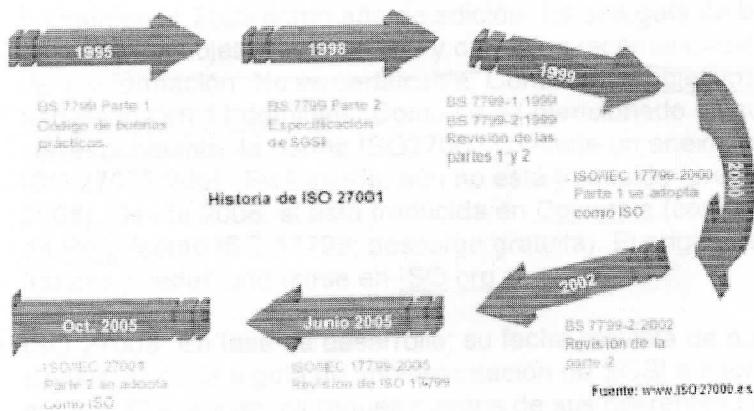
La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa -británica o no- un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.



En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

En la sección de [Artículos y Podcasts](#) encontrará un archivo gráfico y sonoro con la [historia de ISO 27001 e ISO 17799](#).

3

## 2. La serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- ISO 27000: En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tendrán un coste.
- ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en [AENOR](#).

Otros países donde también está publicada en español son, por ejemplo, Colombia, Venezuela y Argentina. El original en inglés y la traducción al francés pueden adquirirse en ISO.org.

- ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad, de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org.
- ISO 27003: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2009. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.
- ISO 27004: En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.
- ISO 27005: Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro) que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.
- ISO 27006: Publicada el 13 de Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida. El original en inglés puede adquirirse en ISO.org.

- ISO 27007: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.
- ISO 27011: En fase de desarrollo; su fecha prevista de publicación es finales de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU (Unión Internacional de Telecomunicaciones).
- ISO 27031: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
- ISO 27032: En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía relativa a la ciberseguridad.
- ISO 27033: En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y reenumeración de ISO 18028.
- ISO 27034: En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía de seguridad en aplicaciones.
- ISO 27799: Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información (palabras y números, grabaciones sonoras, dibujos, vídeos y imágenes médicas), sea cual fuere el medio utilizado para almacenar (de impresión o de escritura en papel o electrónicos de almacenamiento) y sea cual fuere el medio utilizado para transmitirlo (a mano, por fax, por redes informáticas o por correo), ya que la información siempre debe estar adecuadamente protegida. El original en inglés o francés puede adquirirse en ISO.org.

### 3. Contenido

En esta sección se hace un breve resumen del contenido de las normas ISO 27001, ISO 27002, ISO 27006 e ISO 27799. Si desea acceder a las normas completas, debe saber que éstas no son de libre difusión sino que han de ser adquiridas.

Para los originales en inglés, puede hacerlo online en la tienda virtual de la propia organización:

<http://www.iso.org/iso/en/prods-services/ISOstore/store.html>

Las normas en español pueden adquirirse en España en AENOR (vea en la sección Serie 27000 cuáles están ya traducidas):

<http://www.aenor.es/desarrollo/normalizacion/normas/buscadornormas.asp>

Las entidades de normalización responsables de la publicación y venta de normas en cada país hispanoamericano (es decir, las homólogas del AENOR español) las puede encontrar listadas en nuestra sección de Enlaces, bajo Acreditación y Normalización.

ISO 27001:2005

- Introducción: generalidades e introducción al método PDCA.
- Objeto y campo de aplicación: se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- Normas para consulta: otras normas que sirven de referencia.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- Sistema de gestión de la seguridad de la información: cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.
- Responsabilidad de la dirección: en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.
- Auditorías internas del SGSI: cómo realizar las auditorías internas de control y cumplimiento.
- Revisión del SGSI por la dirección: cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.
- Mejora del SGSI: mejora continua, acciones correctivas y acciones preventivas.

- Objetivos de control y controles: anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.
- Relación con los Principios de la OCDE: anexo informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.
- Correspondencia con otras normas: anexo informativo con una tabla de correspondencia de cláusulas con ISO 9001 e ISO 14001.
- Bibliografía: normas y publicaciones de referencia.

### ISO 27002:2005 (anterior ISO 17799:2005)

- Introducción: conceptos generales de seguridad de la información y SGSI.
- Campo de aplicación: se especifica el objetivo de la norma.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- Estructura del estándar: descripción de la estructura de la norma.
- Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- Política de seguridad: documento de política de seguridad y su gestión.
- Aspectos organizativos de la seguridad de la información: organización interna; terceros.
- Gestión de activos: responsabilidad sobre los activos; clasificación de la información.
- Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.
- Seguridad física y ambiental: áreas seguras; seguridad de los equipos.
- Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.
- Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.
- Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las

aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

- Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.
- Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.
- Bibliografía: normas y publicaciones de referencia.

Puede descargarse una lista de todos los controles que contiene esta norma aquí:  
<http://www.iso27000.es/download/ControlesISO27002-2005.pdf>

## ISO 27005:2008

Esta norma establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

8

- Preámbulo
- Introducción
- Referencias normativas
- Términos y definiciones
- Breve descripción de los términos más usados en la norma.
- Estructura del estándar
- Descripción de la estructura de la norma.
- Fundamentos del proceso de gestión de riesgos (ISRM)
- Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- Establecimiento del contexto
- Evaluación de riesgos (ISRA)
- Tratamiento de riesgos

- Aceptación del riesgo
- Comunicación del riesgo
- Monitorización y revisión del riesgo
- Anexo A: Definiendo el ámbito del proceso
- Anexo B: Valoración de activos y evaluación de impacto
- Anexo C: Ejemplos de amenazas más comunes
- Anexo D: Vulnerabilidades y métodos de evaluación
- Anexo E: Aproximación a ISRA

**ISO 27006:2007**

(Esta norma referencia directamente a muchas cláusulas de ISO 17021 -requisitos de entidades de auditoría y certificación de sistemas de gestión-, por lo que es recomendable disponer también de dicha norma, que puede adquirirse en español en [AENOR](#)).

- Preámbulo: presentación de las organizaciones ISO e IEC y sus actividades.
- Introducción: antecedentes de ISO 27006 y guía de uso para la norma.
- Campo de aplicación: a quién aplica este estándar.
- Referencias normativas: otras normas que sirven de referencia.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- Principios: principios que rigen esta norma.
- Requisitos generales: aspectos generales que deben cumplir las entidades de certificación de SGSIs.
- Requisitos estructurales: estructura organizativa que deben tener las entidades de certificación de SGSIs.
- Requisitos en cuanto a recursos: competencias requeridas para el personal de dirección, administración y auditoría de la entidad de certificación, así como para auditores externos, expertos técnicos externos y subcontratas.
- Requisitos de información: información pública, documentos de certificación, relación de clientes certificados, referencias a la certificación y marcas, confidencialidad e intercambio de información entre la entidad de certificación y sus clientes.

- Requisitos del proceso: requisitos generales del proceso de certificación, auditoría inicial y certificación, auditorías de seguimiento, recertificación, auditorías especiales, suspensión, retirada o modificación de alcance de la certificación, apelaciones, reclamaciones y registros de solicitantes y clientes.
- Requisitos del sistema de gestión de entidades de certificación: opciones, opción 1 (requisitos del sistema de gestión de acuerdo con ISO 9001) y opción 2 (requisitos del sistema de gestión general).
- Anexo A - Análisis de la complejidad de la organización de un cliente y aspectos específicos del sector: potencial de riesgo de la organización (tabla orientativa) y categorías de riesgo de la seguridad de la información específicas del sector de actividad.
- Anexo B - Áreas de ejemplo de competencia del auditor: consideraciones de competencia general y consideraciones de competencia específica (conocimiento de los controles del Anexo A de ISO 27001:2005 y conocimientos sobre SGIs).
- Anexo C - Tiempos de auditoría: introducción, procedimiento para determinar la duración de la auditoría y tabla de tiempos de auditoría (incluyendo comparativa con tiempos de auditoría de sistemas de calidad -ISO 9001- y medioambientales -ISO 14001-).
- Anexo D - Guía para la revisión de controles implantados del Anexo A de ISO 27001:2005: tabla de apoyo para el auditor sobre cómo auditar los controles, sean organizativos o técnicos.

## ISO 27799:2008

Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 (actual ISO 27002). Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma.

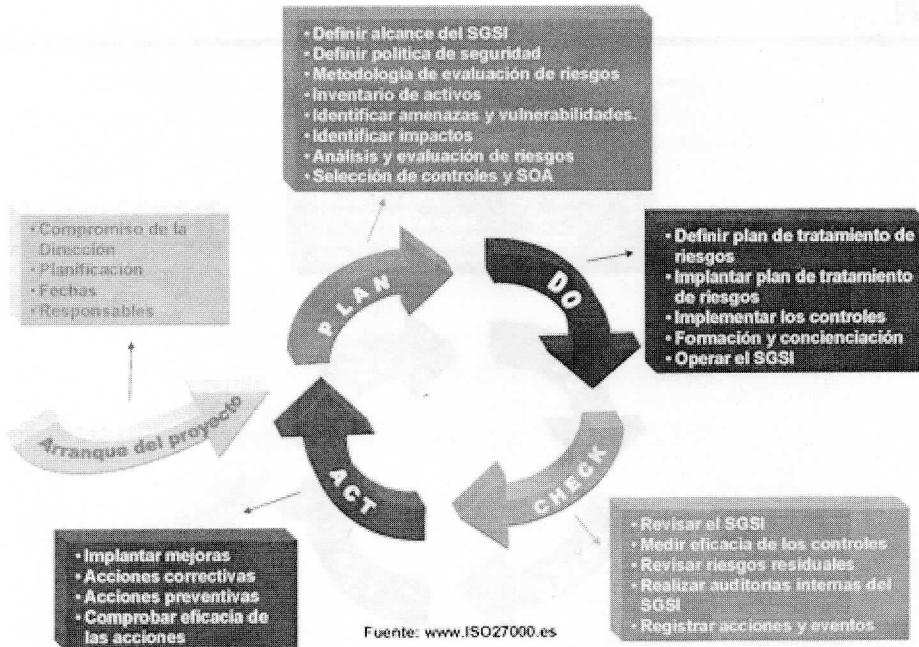
- Alcance
- Referencias (Normativas)
- Terminología
- Simbología
- Seguridad de la información sanitaria (Objetivos; Seguridad en el gobierno de la información; Infomación sanitaria a proteger; Amenazas y vulnerabilidades)
- Plan de acción práctico para implantar ISO 17799/27002 (Taxonomía; Acuerdo de la dirección; establecimiento, operación, mantenimiento y mejora de un SGSI; Planning; Doing; Checking, Auditing)

- Implicaciones sanitarias de ISO 17799/27002 (Política de seguridad de la información; Organización; gestión de activos; RRHH; Fisicos; Comunicaciones; Accesos; Adquisición; Gestión de Incidentes; Continuidad de negocio; Cumplimiento legal)
- Anexo A: Amenazas
- Anexo B: Tareas y documentación de un SGSI
- Anexo C: Beneficios potenciales y atributos de herramientas
- Anexo D: Estándares relacionados

## 4. Beneficios

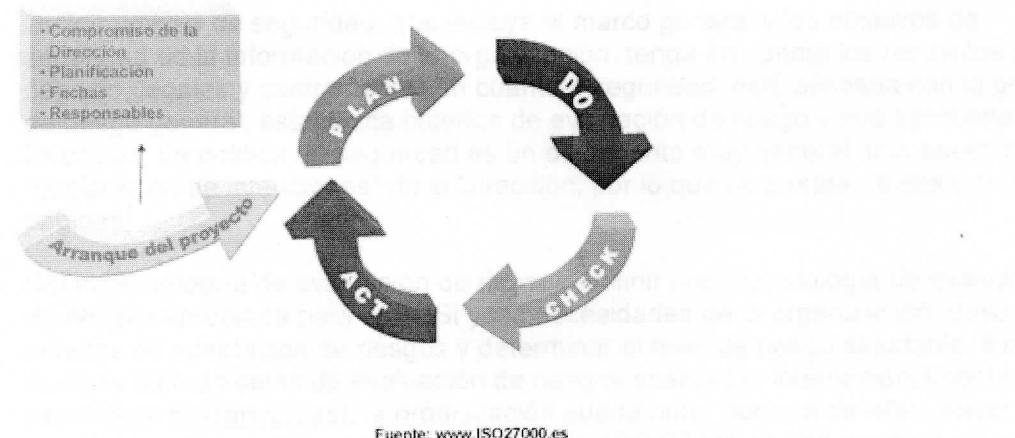
- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- Reducción del riesgo de pérdida, robo o corrupción de información.
- Los clientes tienen acceso a la información a través medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 18001).
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- Confianza y reglas claras para las personas de la organización.
- Reducción de costes y mejora de los procesos y servicio.
- Aumento de la motivación y satisfacción del personal.
- Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

## 5. ¿Cómo adaptarse?



12

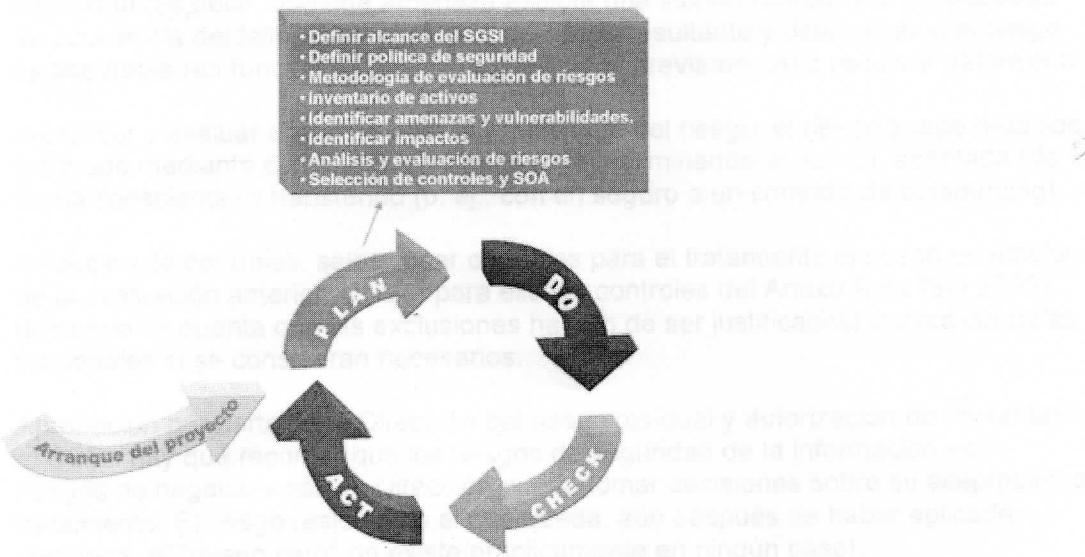
### Arranque del proyecto



- Compromiso de la Dirección: una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la organización. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.

- Planificación, fechas, responsables: como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

## Planificación



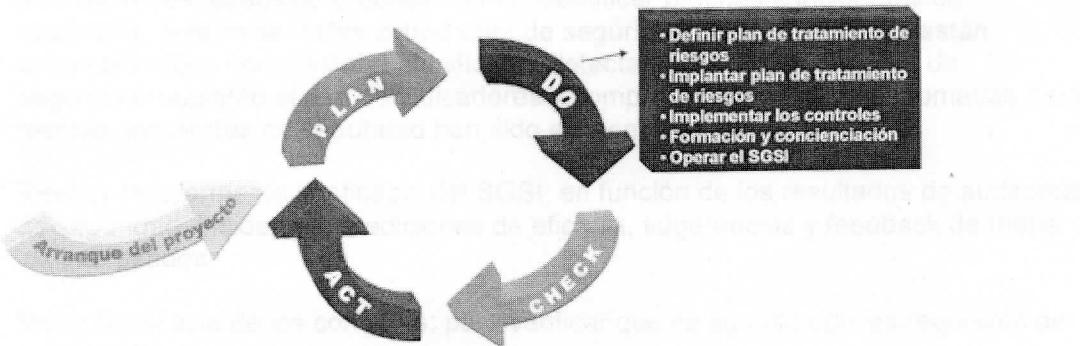
Fuente: [www.ISO27000.es](http://www.ISO27000.es)

13

- Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado).
- Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección, por lo que no pasará de dos o tres páginas.
- Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente (ver sección de Herramientas); la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla (en el futuro, ISO 27005 proporcionará ayuda en este sentido). El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.
- Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

- Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
- Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad) y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.
- Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido (mitigado mediante controles), eliminado (p. ej., eliminando el activo), aceptado (de forma consciente) o transferido (p. ej., con un seguro o un contrato de outsourcing).
- Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).
- Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

## Implementación



Fuente: [www.ISO27000.es](http://www.ISO27000.es)

- Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los que se seleccionaron en la fase anterior.
- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

## Seguimiento

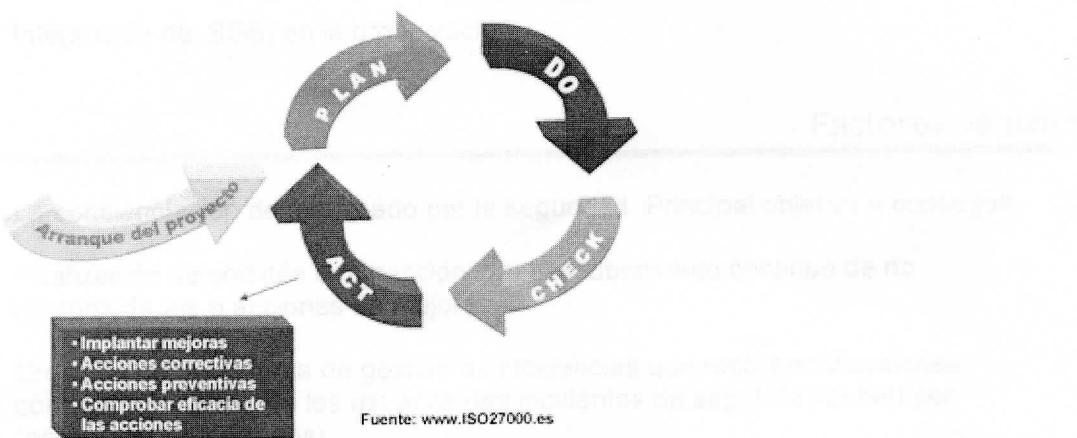


15

- Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
- Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.
- Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

- Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.
- Revisar regularmente el SGSI por parte de la Dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.
- Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

### Mejora continua



16

- Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- Acciones correctivas: para solucionar no conformidades detectadas.
- Acciones preventivas: para prevenir potenciales no conformidades.
- Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

## 6. Aspectos Clave

### Fundamentales

- Compromiso y apoyo de la Dirección de la organización.
- Definición clara de un alcance apropiado.
- Concienciación y formación del personal.
- Evaluación de riesgos exhaustiva y adecuada a la organización.
- Compromiso de mejora continua.
- Establecimiento de políticas y normas.
- Organización y comunicación.
- Integración del SGSI en la organización.

### Factores de éxito

- La concienciación del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités de dirección con descubrimiento continuo de no conformidades o acciones de mejora.
- Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.

## Riesgos

- Exceso de tiempos de implantación: con los consecuentes costes descontrolados, desmotivación, alejamiento de los objetivos iniciales, etc.
- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.
- Delegación de todas las responsabilidades en departamentos técnicos.
- No asumir que la seguridad de la información es inherente a los procesos de negocio.
- Planes de formación y concienciación inadecuados.
- Calendario de revisiones que no se puedan cumplir.
- Definición poco clara del alcance.
- Exceso de medidas técnicas en detrimento de la formación, concienciación y medidas de tipo organizativo.
- Falta de comunicación de los progresos al personal de la organización.

18

## Consejos básicos

- Mantener la sencillez y restringirse a un alcance manejable y reducido: un centro de trabajo, un proceso de negocio clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases.
- Comprender en detalle el proceso de implantación: iniciarla en base a cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación; adquirir experiencia de otras implantaciones, asistir a cursos de formación o contar con asesoramiento de consultores externos especializados.
- Gestionar el proyecto fijando los diferentes hitos con sus objetivos y resultados.
- La autoridad y compromiso decidido de la Dirección de la empresa -incluso si al inicio el alcance se restringe a un alcance reducido- evitarán un muro de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales de la norma.
- La certificación como objetivo: aunque se puede alcanzar la conformidad con la norma sin certificarse, la certificación por un tercero asegura un mejor enfoque, un objetivo más claro y tangible y, por lo tanto, mejores opciones de alcanzar el éxito.

- No reinventar la rueda: aunque el objetivo sea ISO 27001, es bueno obtener información relativa a la gestión de la seguridad de la información de otros métodos y marcos reconocidos.
- Servirse de lo ya implementado: otros estándares como ISO 9001 son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo y creando sinergias; es conveniente pedir ayuda e implicar a auditores internos y responsables de otros sistemas de gestión.
- Reservar la dedicación necesaria diaria o semanal: el personal involucrado en el proyecto debe ser capaz de trabajar con continuidad en el proyecto.
- Registrar evidencias: deben recogerse evidencias al menos tres meses antes del intento de certificación para demostrar que el SGSI funciona adecuadamente.