



## ISO/IEC 27001:2005 – Información y requisitos para la transición para auditores ISMS certificados por el IRCA

---

### Alcance:

Este documento:

1. Explica los requisitos de DPC (Desarrollo Profesional Continuo) que debe cumplir para mantener su certificación IRCA como auditor de sistemas de gestión de seguridad de la información cuando realice auditorías según la nueva norma ISO/IEC 27001:2005.
2. Resume las implicancias de la norma ISO/IEC 27001:2005 para auditores de sistemas de gestión de seguridad de la información.
3. Resume los cambios realizados en la norma ISO/IEC 27001:2005 cuando se la compara con la norma BS 7799-2:2002

### Reconocimientos:

El IRCA desea agradecer a Brian Henry, Revisor de ISMS del IRCA, quien contribuyó al desarrollo de este documento.

## 1. Transición de su certificación como auditor ISMS

---

La publicación de la norma ISO/IEC 27001:2005 constituye un hito importante en la publicación de requisitos de sistemas de gestión de seguridad de la información. Le pediremos que Ud. (como auditor ISMS certificado por el IRCA) demuestre que se ha actualizado respecto a la nueva norma y que comprende las implicancias de estos cambios en el contexto de sus actividades de auditorías de ISMS.

Las diferencias entre la nueva norma ISO/IEC 27001:2005 y la BS 7799-2:2002 no son muy importantes. La compatibilidad y consistencia entre ambas normas y una transición fácil fueron tenidas en cuenta durante el proceso de elaboración del documento. Las diferencias entre la norma ISO/IEC 27001:2005 y la BS 7799-2:2002 son esencialmente editoriales y de formato, y mucho menores a las que existieron cuando entre las versiones del 2002 y 1999 de la norma BS 7799.

Sin embargo, es vital tener en cuenta que es virtualmente imposible auditor eficazmente según la norma ISO/IEC 27001:2005 sin tener una comprensión y conocimientos acabados de la ISO/IEC 17799:2005. Esta norma proporciona lineamientos y principios generales y un código de práctica para ISMS.

La norma ISO/IEC 17799:2005 fue publicada en junio de 2005; tiene 17 conjuntos adicionales de recomendaciones y guías de las mejores prácticas, comparada con la versión previa ISO/IEC 17799:2000. Una cantidad pequeña de las recomendaciones de la norma del año 2000 fueron eliminadas o combinadas. En la nueva norma hay, en total, 134 conjuntos de recomendaciones y guías, las que corresponden a 38 objetivos de control y 134 controles especificados en su Anexo "A".

La norma ISO/IEC 17799:2005 no cambiará su número en un futuro cercano. Se está planeando asignarle el número 27002 en abril de 2007, pero el texto permanecerá sin cambios.

### Requisitos para la transición para auditores ISMS certificados por el IRCA

Todos los auditores ISMS certificados por el IRCA deberán completar **4 horas de desarrollo profesional continuo (DPC) antes** de completar auditorías según la nueva norma, aceptables para el IRCA. Esto permitirá a los auditores ISMS poder demostrar su conocimiento y comprensión de las normas ISO/IEC 27001:2005 e ISO/IEC 17799:2005 (y las normas referenciadas en éstas), y así poder desarrollar sus habilidades como auditor para estar en condiciones de auditar según los requisitos especificados en la norma ISO/IEC 27001:2005.

Las evidencias de DPC, debidamente verificadas, deberán ser enviadas al IRCA registradas en la Planilla de DPC (IRCA/173), junto a las Planillas de Auditorías (IRCA/106), demostrando las auditorías realizadas según la norma ISO/IEC 27001:2005.



## ISO/IEC 27001:2005 – Información y requisitos para la transición para auditores ISMS certificados por el IRCA

---

Las Planillas de DPC pueden ser enviadas al IRCA junto a la solicitud de cambio de grado o de renovación de la certificación.

### **Cuándo comienza el proceso?**

El IRCA aceptará solicitudes de transición con actividades de DPC y auditorías realizadas según la nueva norma a partir de Enero de 2006.

### **Qué tipo de DPC aceptará el IRCA?**

No requerimos que los auditores ISMS completen un DPC específico para la transición, y Ud. puede lograr el DPC de diversas formas, como es habitual en el enfoque del DPC que asume el IRCA:

- auto-estudio (lectura de las nuevas normas y de la documentación de soporte)
- formación o seminarios internos en su empresa
- asistencia a conferencias, seminarios o talleres pertinentes
- lectura (de esta nota u otros artículos pertinentes)
- Aprobación de un curso de auditores ISMS basado en la norma ISO/IEC 27001:2005.

El IRCA proporcionará una lista de eventos y seminarios sobre la norma ISO 27001:2005 que son aceptables como DPC; no será una lista exhaustiva y otras actividades pueden ser aceptables como DPC. Estos eventos son ofrecidos por organismos de formación aprobadas por el IRCA y por OEAs, pero no están formalmente certificados por el IRCA y, por lo tanto, no están bajo su control, aunque los aceptamos como DPC junto con otros eventos y actividades de formación. Podrá consultar una lista de estos cursos y eventos en nuestra página web, [www.irca.org](http://www.irca.org) a medida que estén disponibles. Alternativamente, el IRCA puede ser contactado en el teléfono No. + 44 (0) 0207 245 6833 para obtener información sobre este tema.

## **2. Introducción – implicancias de la norma ISO/IEC para los auditores**

---

La largamente esperada publicación de la norma ISO/IEC 27001:2005, basada en la norma BS 7799-2:2002, representa un paso muy importante hacia el reconocimiento internacional y el desarrollo de la certificación de ISMS. La nueva norma fue publicada el 15 de octubre de 2005, y en consecuencia, la norma BS 7799-2:2002 fue retirada y reemplazada por la misma.

Se espera que la publicación de la norma ISO/IEC 27001:2005 provoque una explosión en el interés de las organizaciones que están planeando implementar un ISMS para luego certificarlo según los requisitos de esta nueva norma. Se espera que esto suceda más allá del Reino Unido y Japón, países que, hasta ahora, han concentrado el interés de la certificación acreditada de ISMS.

Actualmente, hay casi 2000 organizaciones certificadas según la norma BS 7799-2:2002 en todo el mundo; los organismos de acreditación están desarrollando planes para organismos de certificación, para la transición a la nueva norma ISO/IEC 27001:2005 en un plazo definido de tiempo. Se estima que el plazo a ser concedido a los organismos de certificación para la adecuación de sus servicios a la nueva norma será el 31 de octubre de 2007.

Para las organizaciones ya certificadas, es probable que la evaluación según la nueva norma ISO/IEC 27001/2005 sea realizada en las auditorías de seguimiento regulares. Los nuevos clientes ya están siendo evaluados según la nueva norma.

Los auditores deben tener en cuenta que la publicación de la norma ISO/IEC 27001:2005 es solamente la primera de una serie de normas. Se está planificando la elaboración de otras normas en la misma serie:

ISO/IEC 27000 ISMS Principios y vocabulario



## ISO/IEC 27001:2005 – Información y requisitos para la transición para auditores ISMS certificados por el IRCA

---

ISO/IEC 27002 ISMS Técnicas de seguridad – Código de práctica (ISO/IEC 17799:2005)

ISO/IEC 27003 ISMS Directrices para la implementación

ISO/IEC 27004 ISMS Indicadores y mediciones

ISO/IEC 27005 ISMS Gestión de los riesgos

ISO/IEC 27006 ISMS Continuidad de los negocios y servicios de recuperación ante desastres

Aparentemente, los sistemas de gestión de seguridad de la información se están transformando en un tema relevante a nivel mundial en una amplio rango de organizaciones y sectores industriales y comerciales. Sin duda, los auditores ISMS se enfrentarán en un futuro cercano con nuevas oportunidades y desafíos, y, por lo tanto, deben estar adecuadamente preparados para enfrentarlos.

### **3. ISO 27001:2005 Requisitos – Resumen de los cambios más importantes**

---

A continuación se presentan los principales requisitos ordenados por cláusula de la norma, donde se han introducido cambios y las implicancias específicas para los auditores.

#### **Prefacio e Introducción**

No se introdujeron cambios significativos. La norma ISO/IEC 27001:2005 tiene todavía la amplia introducción de la BS 7799-2:2002. Se mantiene la referencia al enfoque por procesos, pero con mayor grado de elaboración.

Conserva la importante advertencia sobre la alineación con las normas ISO 9001:2000 e ISO 14001:2004, y que esta norma ha sido diseñada para permitir a cualquier organización alinear o integrar su ISMS con otros sistemas de gestión.

#### **Alcance – Cláusula 1**

Se aclara que esta norma es aplicable a todas las organizaciones. Asimismo, en la sub-cláusula "Aplicación" hace referencia a los requisitos de las cláusulas 4 a 8 que no pueden ser excluidos cuando se desee alegar conformidad con esta norma.

#### **Referencias normativas – Cláusula 2**

Se deja claro que la norma ISO/IEC 27001:2005, para su aplicación, está directamente relacionada con la ISO/IEC 17799:2005.

#### **Términos y definiciones – Cláusula 3**

Se agregaron algunas definiciones y otras fueron modificadas o reemplazadas para alinearse con otras normas, tales como ISO/IEC 13335-1:2004 e ISO/IEC TR 18044:2004. Asimismo, se aclararon o modificaron algunas definiciones para evitar interpretaciones incorrectas.

#### **Requisitos generales – Cláusula 4.1**

Se clarificó el requisito, incluyendo las actividades de operación, monitoreo y revisión del ISMS documentado.

#### **Estableciendo y monitoreando el ISMS – cláusula 4.2**

##### **4.2.1 Establecer el ISMS**

- a) Definir el alcance – este requisito ha sido modificado para asegurar que en el "alcance" se definan también los límites del ISMS. La necesidad de establecer los límites del ISMS estuvo siempre implícita, pero ahora está claramente expresado y debe incluir la justificación de cualquier exclusión.

- b) Definir la política de ISMS – muy pocos cambios editoriales en el texto – ahora está más claro que debe estar “alineada con el contexto de la gestión estratégica de riesgos de la organización”.

Hay una nueva “NOTA” que indica que la política de ISMS es un subconjunto de la Política de Seguridad de la Información.

- c) Definir el enfoque de evaluación de riesgos de la organización – se ha modificado el texto para presentar un listado de ítemes. Un texto agregado deja claro que la evaluación de riesgos seleccionada debe producir resultados comparables y reproducibles.

Hay una nueva “NOTA” que hace referencia a los ejemplos de metodologías de evaluación de riesgos incluidos en el documento ISO/IEC TR 13335-3

- d) Identificación de riesgos – el texto no ha sido modificado, pero se agregó una nota al pie clarificando el término “dueño de activos”.

- e) Analizar y evaluar riesgos – antes era “evaluar los riesgos” – cambios editoriales menores, con términos tales como “daños a los negocios” que fue reemplazado por “impactos en los negocios de la organización”.

- g) Seleccionar objetivos de control – el texto se ha ampliado para clarificar que la selección e implementación de objetivos de control y de controles se realiza para poder cumplir con los requisitos identificados durante los procesos de evaluación y tratamiento de riesgos. Una oración adicional requiere tener en cuenta los criterios para aceptar riesgos, así como los requisitos legales, regulatorios y contractuales.

Se han ampliado los requisitos para la selección de objetivos de control y de los controles; asimismo, se revisó la “NOTA” que explica el contenido y propósito del Anexo A.

- h & i) Obtener la aprobación y autorización de la alta dirección para implementar y operar el ISMS – el texto actual se reestructuró.

- j) Preparar una Declaración de Aplicabilidad – el texto actual fue ampliado y reformateado en una lista de ítemes para clarificar que la Declaración de Aplicabilidad debe incluir los objetivos de control y los controles existentes.

Se agregó una NOTA nueva, para puntualizar que la Declaración de Aplicabilidad provee un resumen de las decisiones relacionadas con el tratamiento de riesgos y con la justificación de exclusiones, lo que constituye una verificación cruzada de que no se omitieron controles en forma inadvertida

#### ***4.2.2 Implementar y operar el ISMS***

- a) Formular un plan de tratamiento de riesgos – se agregó “recursos” al listado de acciones pertinentes de la dirección.

- d) Definir cómo medir – éste es un agregado a los requisitos de implementar y operar el ISMS. Ahora se requiere definir cómo medir la eficacia de los controles o de grupos de controles y también cómo estas mediciones serán usadas para evaluar el control de la eficacia para producir resultados comparables y reproducibles. Asimismo, se agregó una “NOTA” que clarifica que la medición de la eficacia de los controles permite determinar cuán bien los controles logran los objetivos de control planificados.

- f) Gestionar las operaciones – se clarifica qué operaciones deben ser gestionadas
- g) Gestionar recursos – se clarifica qué recursos deben ser gestionados

#### **4.2.3 Seguimiento (monitoreo) y revisión del ISMS**

- a) Ejecutar procedimientos de seguimiento/monitoreo – Requiere que su aplicación sea extendida de solamente seguimiento/ monitoreo a la revisión de los procedimientos. En la sub-cláusula a)2, la palabra "failed" ha sido reemplazada por "attempted" de tal manera de asegurar que todos las violaciones e incidentes de seguridad sean incluidos.

Se agregó la cláusula a)4 para incluir la detección de eventos de seguridad y, por lo tanto, prevenir incidentes de seguridad haciendo uso de indicadores. La sub-cláusula 5 se ha modificado para asegurar que se determine si las acciones tomadas para resolver una violación de la seguridad ha sido eficaz.

- b) Realizar revisiones regulares – este requisito ha sido modificado para incluir los resultados de las mediciones de eficacia en esta revisiones regulares. También, la "política de seguridad" previa se transformó en "política de ISMS", ya que esto impacta en la revisión del ISMS.
- c) Medición de la eficacia de los controles – éste es un agregado al requisito existente de monitorear y revisar el ISMS. Ahora se necesita medir la eficacia de los controles para verificar si los requisitos de seguridad han sido cumplidos.
- d) Revisar las evaluaciones de riesgo – se modificó el texto para incluir que la revisión de la evaluación de riesgos se realice a intervalos planificados. Se agrega la sub-cláusula d)5 para incluir en la revisión la eficacia de los controles implementados. En la sub-cláusula d)6 se agregaron las palabras "obligaciones contractuales modificadas".
- e) Conducir auditorías de ISMS internas – no se ha modificado el texto, pero se hace referencia al texto modificado de la Sección 6. Se agregó una "NOTA" que explica qué son las auditorías internas y quién las conduce.
- f) Realizar revisiones por la dirección – se eliminó la referencia a una frecuencia mínima de una vez al año.
- g) Actualizar los planes de seguridad – constituye un requisito nuevo.

#### **4.2.4 Mantener y mejorar el ISMS**

- c) Comunicar las acciones y mejoras – se ha modificado el texto para no solo incluir la comunicación de resultados pero también para asegurar que hay un nivel de detalle apropiado a las circunstancias y, si es pertinente, un acuerdo de cómo proceder.

### **Requisitos sobre la documentación - cláusula 4.3**

#### **4.3.1 General**

Nuevos párrafos introductorios explican en forma detallada qué se espera de este requisito; por ejemplo, la conservación de registros de las decisiones de la dirección de la organización, la trazabilidad de las acciones a las decisiones y política de la dirección, la reproducibilidad de los resultados conservados en registros. Asimismo, deja claro la importancia de poder demostrar la relación de los controles seleccionados con los resultados de la evaluación y tratamiento de riesgos, y subsecuentemente, con la política y objetivos de ISMS.

**ISO/IEC 27001:2005 – Información y requisitos para la transición para auditores ISMS  
certificados por el IRCA**

---

- a) Declaraciones documentadas – modificada para requerir “política y objetivos de ISMS” en lugar de “política de seguridad y objetivos de control”.
- b) El alcance del ISMS – se elimina la referencia a “procedimientos y controles en apoyo al ISMS”.
- c) Se incorpora la referencia a “procedimientos y controles en soporte al ISMS”.
- d) Descripción de la metodología de evaluación de riesgos – aclara la necesidad de que la documentación del ISMS incluya una descripción de la metodología de evaluación de riesgos.
- g) Procedimientos documentados – se amplió el texto para tener en cuenta la necesidad de describir cómo medir la eficacia de los controles.

**4.3.2 Control de documentos**

- d) Asegurar que las versiones pertinentes – se cambió de “versiones más recientes de los documentos pertinentes” a “versiones pertinentes de los documentos aplicables”.
- f) Asegurar que los documentos están disponibles – se agrega una aclaración para asegurar que los documentos están disponibles para las personas que los necesitan, y que son transferidos, almacenados y finalmente dispuestos de acuerdo con los procedimientos aplicables, según sea su clasificación.

**4.3.3 Control de registros**

En el primer párrafo, la segunda oración fue modificada a: “Deberán ser protegidos y controlados”. La tercera oración fue ampliada para cubrir también “requisitos regulatorios y obligaciones contractuales”. La quinta oración también fue ampliada para requerir que los controles estén “documentados e implementados”. La última oración de este requisito en la norma BS 7799-2:2002 fue eliminada.

En el segundo párrafo, la palabra “significativo” fue agregada en referencia a “incidentes de seguridad”.

Se proporcionan ejemplos de registros.

**Responsabilidad de la Dirección – Cláusula 5**

**5.1 Compromiso de la dirección**

- a) Establecer un ISMS – la expresión “política de seguridad de la información” fue reemplazado por “política de ISMS” como el foco principal del ISMS en este párrafo.
- b) Asegurar que el ISMS – la expresión “objetivos de seguridad de la información” fue reemplazado por “objetivos de ISMS” como el principal foco del ISMS en este párrafo.
- e) Proveer recursos suficientes – la descripción de las actividades del ISMS se alinearon con la definición de ISMS.
- f) Decidiendo los criterios – Este requisito se ha ampliado para cubrir al decisión sobre “criterios para aceptar riesgos y para la aceptabilidad de los niveles de riesgos”.
- g) Asegurando que las auditorías internas – Constituye una aclaración y agregado al compromiso de la dirección de asegurar que se lleven a cabo auditorías internas al ISMS. Incluye una referencia a la nueva cláusula 6.

## 5.2 Gestión de los recursos

### 5.2.1 Provisión de recursos

- a) Establecer, implementar, operar – ampliado para cubrir todo el rango de actividades relacionadas con el ISMS.

### 5.2.2 Formación, toma de conciencia y competencia

- b) Proveer formación – se ha modificado el texto para tener en cuenta la posibilidad de otras acciones (por ejemplo: emplear personal); este cambio se introdujo para alinear el requisito con la norma ISO 9001:2000.
- c) Evaluar la eficacia – este requisito se ha reducido a “evaluar la eficacia de las acciones tomadas”.

## Auditorías internas al ISMS – Cláusula 6

Se transformó la sub-cláusula 6.4 en la norma BS 7799-2:2002 en una cláusula principal en la norma ISO/IEC 27001:2005, permaneciendo el texto sin modificaciones excepto las siguientes:

Cuarto párrafo – en la segunda oración, la expresión “actividades de mejora” se ha reemplazado por “actividades de seguimiento”.

Se agregó una NOTA nueva para hacer referencia a la norma ISO 19011:2002 Directrices para las auditorías de los sistemas de gestión de la calidad y/o del medioambiente.

## Revisión del ISMS por la dirección – Cláusula 7

Se ha modificado la numeración de la cláusula para tener en cuenta la inserción de la nueva cláusula 6.

- 7.1 General – cambio en la numeración – Primer párrafo – en la primera oración “al menos una vez al año” se ha agregado luego de “intervalos” (proveniente de la cláusula 4.2.3 de la norma BS 7799-2:2002).

También se modificó el texto “política de seguridad y objetivos de seguridad”; fue reemplazado por “política de seguridad de la información y objetivos de seguridad de la información” con el fin de clarificar qué se debe incluir en la revisión.

- 7.2 Datos de entradas para la revisión – cambio de numeración – la oración fue simplificada a “Los datos de entrada para la revisión por la dirección deben incluir”

- 7.3 Datos de salida de la revisión – cambio en la numeración

- b) Actualización de los riesgos – clarificación y ampliación del texto para requerir la actualización de la evaluación de los riesgos y del plan de tratamiento de riesgos.
- c) Modificaciones de los procedimientos – se amplió el texto para incluir a “las modificaciones de procedimientos y controles”
- c) 5 obligaciones contractuales - clarificación
- c) 6 niveles de riesgos – se amplió el texto para incluir “niveles de riesgos y/o criterios de aceptación de riesgos”.
- e) Mejoras – clarificación del texto

## Mejora del ISMS – Cláusula 8

Se ajustó la numeración de la cláusula debido a la introducción de la nueva cláusula 6.

### 8.1 Mejora continua

Primer párrafo – lse agregó a palabra “información” en referencia a “objetivos de seguridad”.

### 8.2 Acción correctiva

Se ajustó la numeración de la cláusula – el texto relacionado con “asociado con la implementación y operación del ISMS” fue reemplazado por “con los requisitos del ISMS”

- a) identificación de no conformidades – se simplificó el texto.

### 8.3 Acción preventiva

Primer párrafo – se ajustó la numeración – se modificó el texto – “prevenir no conformidades futuras” fue reemplazado por “con los requisitos de ISMS”

- b) evaluación de la necesidad – texto nuevo

Segundo párrafo – se introdujo un párrafo nuevo usando la última viñeta de la lista anterior requiriendo que la organización identifique los riesgos modificados y que la organización identifique requisitos de acciones preventivas focalizándose en cambios significativos en los riesgos.

## ANEXO A

Ha sido actualizado – los controles y los objetivos de control se corresponden con las directrices de la norma ISO/IEC 17799: 2005

## ANEXO B

El texto del Anexo B de la norma BS7799-2: 2002 no ha sido incluido, ya que se prevé su uso en del desarrollo de la norma ISO/IEC 27003 ISMS “Directrices para la implementación”. La tabla anterior B.1 constituye el Anexo B en la norma ISO/IEC 27001:2005.

## ANEXO C

Ha sido actualizado para tener en cuenta la re-estructuración y la alineación con la norma ISO 9001:2000 y, por supuesto, la re-estructuración de la norma ISO 14001:2004

## ANEXO D

Este anexo fue eliminado.

## BIBLIOGRAFÍA

Ha sido actualizada para reflejar la publicación de las nuevas normas y publicaciones.

Si tiene alguna duda, contáctenos en [registration@irca.org](mailto:registration@irca.org).

Para obtener más información sobre la certificación IRCA de auditores ISMS, visite nuestra página web [www.irca.org](http://www.irca.org).

Suscríbese a nuestra publicación gratuita, *IRCA INforma*, por email a [registration@irca.org](mailto:registration@irca.org) o a [www.irca.org](http://www.irca.org).

Fin del documento