ANÁLISIS DE ISO-27001:2005

Por: Alejandro Corletti Estrada
Mail: acorletti@hotmail.com

Madrid, abril de 2006.

PRÓLOGO

Este texto, trata de presentar un análisis de la situación actual que presenta ISO/IEC para cualquier empresa que desee planificar e implementar una política de seguridad orientada a una futura certificación dentro de este estándar.

Se debe dejar claro que el tema de certificación en aspectos de seguridad, tal vez aún no ha sido considerado con la seriedad que merece en el ámbito empresarial, pero no cabe duda que lo será en el muy corto plazo. Justamente, la sensación que deja el análisis de esta norma, es que se está gestando con toda rigurosidad este hecho, y que como cualquier otra certificación ISO, este estándar internacional ha sido desarrollado (por primera vez con relación a la seguridad, a juicio de este autor) con toda la fuerza y detalle que hacía falta para empezar a presionar al ámbito empresarial sobre su aplicación. Es decir, **se puede prever, que la certificación ISO-27001, será casi una obligación de cualquier empresa que desee competir en el mercado en el corto plazo**, lo cual es lógico, pues si se desea interrelacionar sistemas de clientes, control de stock, facturación, pedidos, productos, etc. entre diferentes organizaciones, se deben exigir mutuamente niveles concretos y adecuados de seguridad informática, sino se abren brechas de seguridad entre sí.....este estándar apunta a poder exigir dichos niveles; y ya no puede caber duda que las empresas, para competir con sus productos (sean de la índole que fueren) en este mercado cibernético actual, tienen cada vez más necesidad de interrelacionar sus infraestructuras de información.....**ISO-27001 en este sentido es una muy buena y sólida opción.**

DESARROLLO

I. ORIGEN Y POSICIONAMIENTO DEL ESTÁNDAR:

ISO (Organización Internacional de Estándares) e **IEC** (Comisión Internacional de Electrotécnia) conforman un especializado sistema especializado para los estándares mundiales. Organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de Normas Internacionales a

través de comités técnicos establecidos por la organización respectiva para tratar con los campos particulares de actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo. Otras organizaciones internacionales, gubernamentales y no gubernamentales, en relación con ISO e IEC, también forman parte del trabajo.

En el campo de tecnología de información, ISO e IEC han establecido unir un comité técnico, ISO/IEC **JTC 1** (Join Technical Committee Nº1). Los borradores de estas Normas Internacionales adoptadas por la unión de este comité técnico son enviados a los organismos de las diferentes naciones para su votación. La publicación, ya como una Norma Internacional, requiere la aprobación de por lo menos el 75% de los organismos nacionales que emiten su voto.

El Estándar Internacional **ISO/IEC 17799** fue preparado inicialmente por el Instituto de Normas Británico (como **BS 7799**) y fue adoptado, bajo la supervisión del grupo de trabajo "Tecnologías de la Información", del Comité Técnico de esta unión entre ISO/IEC JTC 1, en paralelo con su aprobación por los organismos nacionales de ISO e IEC.

El estándar ISO/IEC 27001 es el nuevo estándar oficial, su título completo en realidad es: **BS 7799-2:2005 (ISO/IEC 27001:2005)**. También fue preparado por este JTC 1 y en el subcomité **SC 27**, IT "Security Techniques". La versión que se considerará en este texto es la primera edición, de fecha 15 de octubre de 2005, si bien en febrero de 2006 acaba de salir la versión cuatro del mismo.

1870 organizaciones en 57 países han reconocido la importancia y los beneficios de esta nueva norma. A fines de marzo de 2006, son seis las empresas españolas que poseen esta certificación declarada.

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

- **ISO/IEC 27000** Fundamentals and vocabulary
- **ISO/IEC 27001 ISMS** - Requirements (revised BS 7799 Part 2:2005) – Publicado el 15 de octubre del 2005
- **ISO/IEC 27002** Code of practice for information security management - Actualmente ISO/IEC 17799:2005, publicado el 15 de junio del 2005
- **ISO/IEC 27003 ISMS** implementation guidance (bajo desarrollo)
- **ISO/IEC 27004** Information security management measurement (bajo desarrollo)
- **ISO/IEC 27005** Information security risk management (basado e incorporado a ISO/IEC 13335 MICTS Part 2) (bajo desarrollo)

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

A los efectos de la certificación, la **transición** entre ambas normas queda propuesta (o establecida) por el **TPS-55** de **UKAS** (United Kingdom Acreditation Service): *"Transition Statement Regarding Arrangements for the Implementation of ISO 27001:2005"*. Establece que las empresas (en realidad los auditores, lo cual afecta directamente a las empresas) durante los primeros seis meses (desde que se firmó el acuerdo "MoU: Memorandum of Understanding" entre UKAS y el Departamento de Comercio e Industria de Reino Unido), pueden elegir acerca de qué estándar aplicar, a partir del 23 de julio del

2006, la única certificación que se deberá aplicar será la ISO/IEC 27001:2005. Ante cualquier no conformidad con la aplicación de la misma motivada claramente por su transición, se establece un plazo de un año para solucionarla, es decir, hasta el 23 de julio de 2007.

II. PRESENTACION DE ESTE TEXTO

El presente documento es un muy breve resumen de los aspectos más importantes a tener en cuenta para la aplicación del Estándar Internacional **ISO-27001:2005**. Se debe dejar claro que este es la versión actual del **ISO-17799:2002**, y dentro del primero se detallan claramente todos los aspectos de compatibilidad entre ellos. El verdadero enfoque que se debe encarar para tratar de alcanzar la compatibilidad con este estándar es aplicar la Norma ISO-27001 con todo detalle y a través del seguimiento de todos los aspectos que propone, se estará cumplimentando también con la anterior (lo cual no elude el hecho que se deba conocer también esta predecesora).

III. CONSIDERACIONES CLAVE DEL ESTANDAR

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, implemanetación, operación, monitorización, revisión, mantenimiento y mejora del **ISMS** (Information Security Management System)" (como podrán apreciar que se recalcará repetidas veces a lo largo del mismo). 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 riegos (Risk Assesment)**
- **Controles**

El desarrollo de estos puntos y la documentación que generan, es lo que se tratará en este texto.

IV. BREVE RESUMEN DEL ESTANDAR

Se presentan a continuación las líneas que se consideran de especial interés para la aplicación de esta norma.

Los párrafos siguientes son una breve descripción de los puntos que se considerarán en este texto para poder llegar finalmente y avalando la importancia de la documentación que es necesaria preparar y mantener.

Se consideró importante el mantener la misma puntuación que emplea el Estándar Internacional, para que, si fuera necesario, se pueda acceder directamente al mismo, para ampliar cualquier aspecto, por lo tanto, la numeración que sigue a continuación, no respeta la de este texto, pero sí la de 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.

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 riegos, debe ser justificado y se debe poner de manifiesto, o evidenciar claramente los criterios por los cuales este riesgo es asumido y aceptado. En cualquier caso en el que un control sea excluido, la conformidad con este estándar internacional, no será aceptable, a menos que dicha exclusión no afecte a la capacidad y/o responsabilidad de proveer seguridad a los requerimientos de información que se hayan determinado a través de la evaluación de riesgos, y sea a su vez aplicable a las regulaciones y legislación vigente.

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 riego: 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.

ACLARACIÓN AJENA A LA NORMA: En definitiva la “Evaluación del riesgo”, es el resultado final de esta actividad, pero no debe ser pensada únicamente con relación a “Análisis y Valoración”, sino también a los criterios de riesgo que la organización haya definido a lo largo de toda su política empresarial.

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.

NOTA: el término "**control**" en esta norma es empleado como sinónimo de "Medida o medición".

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.

NOTA: Estos controles están basados en los resultados y conclusiones de la valoración y los procesos de tratamiento de riesgo, los requerimientos y regulaciones legales, las obligaciones contractuales y los requerimientos de negocio para la seguridad de la información que defina la organización.

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 (Ver: Procedimiento de Revisión del ISMS - Periódicas y aperiódicas

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 (Ver: Documento de administración de las revisiones del ISMS).

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 (Ver: Documento de acciones correctivas)

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

V. DOCUMENTACIÓN A CONSIDERAR:

A continuación se presenta un listado de los documentos que se deben considerar como mínimo y sobre los cuales el estándar hacer referencia. Dentro de cada uno de ellos, se especifica brevemente algunas consideraciones y los puntos desde donde son referenciados en la norma.

Estos documentos son:

- Declaración de Aplicabilidad (3.16)
- Documento ISMS (4.1.)

Debe incluir:

- Ámbito y límites del ISMS en términos de características del negocio, la organización, ubicaciones, recursos y tecnologías empleadas y también detalles y justificaciones para cualquier exclusión fuera del mismo, como se especifica en 1.2.

- Definición de la política de este ISMS, en los mismos términos anteriores y teniendo en cuenta:

  ➔ Establecimiento del marco y objetivos de la dirección y principales líneas de acción en temas de seguridad de la información.
  ➔ Considerar requerimientos legales y de empresa y también obligaciones contractuales en aspectos relacionados a la seguridad.
  ➔ Establecer la alineación con el contexto de la estrategia de administración de riesgo de la empresa dentro del cual se establecerá y mantendrá el ISMS.
  ➔ Establecer los criterios contra los cuales se evaluarán loa riesgos y han sido evaluados por la dirección.
  NOTA: Para los criterios de este estándar internacional, la política del ISMS puede ser considerada como una parte del documento de "Política de seguridad" general de la empresa.

- Definición de la Valoración de riesgo de la organización:
  ➔ Identificar la metodología de valoración de riesgo, la información de seguridad identificada de la empresa y los requerimientos y regulaciones legales.
  ➔ Desarrollar un criterio para la aceptación de riesgo y los diferentes niveles de aceptación del mismo.

- Descripción de la metodología que se aplica para la valoración de riesgos

- Identificación de riesgos

  ➔ Identificar los recursos que se encuentran dentro del ámbito del ISMS y los propietarios de los mismos.
  ➔ Identificar las amenazas hacia los mismos.
  ➔ Identificar las vulnerabilidades que pueden ser explotados por esas amenazas.
  ➔ Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad, pueden ocasionar sobre esos recursos.

- Análisis y evaluación de riesgos:

  ➔ Valorar el impacto de negocio hacia la organización que puede resultar desde cualquier fallo de seguridad, teniendo en cuenta la pérdida de confidencialidad, integridad y/o disponibilidad de los recursos.

➔ Probabilidad real de la ocurrencia de fallos de seguridad a la luz de las amenazas, vulnerabilidades e impacto asociado a esos recursos y los controles actualmente implementados.
➔ Estimación del nivel de riesgo.
➔ Determinación si un riesgo es aceptable o requiere el uso de algún tipo de tratamiento de los criterios de riesgo establecidos.

- Identificación y evaluación de las opciones de tratamiento de riesgo.
  Las posibles acciones incluyen:
  ➔ Aplicación de los controles apropiados.
  ➔ Conocimiento y objetividad para la aceptación de riesgos, proveyendo una clara satisfacción de ellos con la política y criterios de aceptación.
  ➔ Evitar riesgos y transferencia de los riesgos asociados a otras partes, por ejemplo, proveedores, socios, etc.

- Selección de controles objetivos para el tratamiento del riesgo.
  Estos controles serán seleccionados e implementados de acuerdo a los requerimientos identificados por la valoración del riesgo y los procesos de tratamiento del riesgo.
  El anexo A de esta norma proporciona una buena base de referencia, no siendo exhaustivos, por lo tanto se pueden seleccionar más aún.

- Obtención de aprobación de la dirección para los riesgos residuales propuestos.

- Obtener autorización de la dirección para implementar y operar el ISMS.

- Preparar una declaración de aplicación, la cual debería incluir:
  ➔ Los objetivos de control, los controles seleccionados y las razones para su selección.
  ➔ Los controles actualmente implementados y la exclusión y justificación de los que figuran en el Anexo A

- Planificación, guías y programas de formación y preparación (5.2.2)

- Documento de administración de las revisiones del ISMS (7.)
  Deberá incluir:
  ➔ Resultados de la revisión.
  ➔ Realimentación hacia las partes interesadas.
  ➔ Técnicas, productos o procedimientos que pueden ser empleados en la organización para mejorar su eficiencia.
  ➔ Estado de acciones preventivas y correctivas.
  ➔ Vulnerabilidades o amenazas que no se adecuan a la valoración de riesgo previa.
  ➔ Resultado de la eficiencia en las mediciones (o controles).
  ➔ Acciones seguidas desde la última revisión.
  ➔ Cualquier cambio que pudiera afectar al ISMS y las recomendaciones de mejora.
  ➔ Actualización de la valoración de riesgos y plan de tratamiento de riesgo.
  ➔ Modificación de procedimientos y/o controles que afecten a la seguridad de la información.
  ➔ Necesidad de recursos.
  ➔ Mejoras en cuanto a la efectividad con que están siendo medidos los controles.

- Documento de acciones correctivas (8.)
  Deberá incluir:
  - ➔ Identificación de no conformidades.
  - ➔ Determinación de las causas de las mismas.
  - ➔ Evaluación de necesidades para acciones que aseguren la no recurrencia de las mismas.
  - ➔ Determinación e implementación de las acciones correctivas necesarias.
  - ➔ Registro de resultados y acciones llevadas a cabo.
  - ➔ Revisión de la actividad correctiva llevada a cabo.

- Procedimientos de:
  - Control de documentos (Ver los detalles del mismo en el punto 4.3.2 de este documento).

  - De registro: Debería existir un procedimiento general, y dentro del mismo, algunos específicos como son:
    - ➔ De actividad (reportes, autorizaciones de acceso, auditorías, cambios, permisos temporales, bajas, etc.) (4.3.3.)
    - ➔ de mejoras y decisiones que afectan al ISMS

  - Respuesta a incidentes de seguridad.

  - Detección de eventos de seguridad.

  - Recolección y centralización de eventos de seguridad.

  - Revisión del ISMS (Periódica y aperiódica)(punto 6.).

  - Revisión y medición de la efectividad de los controles.

Todos estos documentos y registros pueden realizarse en cualquier formato, tipo o medio.

Como se mencionó en esta norma se especifican (en el Anexo A), una serie de controles (o mediciones) a considerar y documentar, que se pueden considerar uno de los aspectos fundamentales del ISMS (junto con la Valoración de riesgo). Cada uno de ellos se encuentra en estrecha relación a todo lo que especifica la norma ISO/IEC 17799:2005 en los puntos 5 al 15, y tal vez estos sean el máximo detalle de afinidad entre ambos estándares. Se reitera una vez más que la evaluación de cada uno de ellos debe quedar claramente establecida en los documentos que se presentaron en este texto, y muy especialmente la de los controles que se consideren excluidos de la documentación.

Alejandro Corletti Estrada, Madrid, abril de 2006.