ITAudit
Vol. 9, Febrero 10, 2006

Estrategias clave para la implantación de ISO 27001

La implantación de ISO 27001 puede convertirse en una ardua tarea. Definir el ámbito de la implantación, así como el tiempo y esfuerzos requeridos, puede ayudar a las organizaciones a diseñar un proceso TI de conformidad más efectivo.

POR KK MOOKHEY, CHIEF TECHNOLOGY OFFICER
NETWORK INTELLIGENCE INDIA PVT. LTD.

KHUSHBU JITHRA, INFORMATION DEVELOPER
NETWORK INTELLIGENCE INDIA PVT. LTD.

En 1995, el *British Standard Institute* (BSI) publicó el estándar *British Standard (BS) 7799*, conjunto de las mejores prácticas ampliamente difundido y que ayuda a las organizaciones a implantar de forma efectiva un Sistema de Gestión para la Seguridad de la Información (SGSI, en inglés ISMS o *Information Security Management Systems*), así como a establecer controles de seguridad para áreas de negocio específicas.

En Octubre de 2005, el estándar fue adoptado por el *International Organization for Standardization* (ISO). Como resultado, la implantación de BS 7799 – ahora ISO 27001:2005 – ha alcanzado un mayor grado de atención por las compañías europeas y por aquellas que desarrollan sus actividades en ésta región.

En función del tamaño de la organización, la naturaleza de sus actividades y la madurez de sus procesos, la implantación de ISO 27001 puede implicar una inversión considerable de recursos que requiere del compromiso de la alta gerencia.

Adicionalmente, y debido al énfasis de la norma en la seguridad de los datos, muchos auditores internos perciben el estándar únicamente dentro del dominio de la tecnología y recomiendan, con frecuencia, a los departamentos de TI cumplir con los requisitos del estándar desconociendo la cantidad de tiempo y recursos que se requieren para lograr la conformidad. Con objeto de garantizar la aceptación de la gerencia y el éxito, es vital realizar unos análisis iniciales y una planificación.

Dado que los auditores internos están en la mejor posición para aportar valor a los procesos TI de la organización, pueden ayudar a los departamentos de TI a preparar los pilares de una estrategia eficiente y efectiva de implantación de ISO 27001 durante la fase de planificación inicial. Esto ayudará a las compañías a garantizar que sus procesos TI estén mejor alineados con los requisitos del estándar y asegurar la conformidad a largo plazo.

RECOMENDACIONES PARA LA CONFORMIDAD EFICAZ EN ISO 27001

Implantar ISO 27001 puede llevar tiempo y consumir recursos no previstos, especialmente si las compañías no disponen de un plan de implantación al inicio del proceso de conformidad. Con objeto de intensificar los esfuerzos en la conformidad, los auditores internos pueden ayudar a las compañías a identificar sus objetivos principales de negocio y el ámbito para la implantación.

Los auditores deberían trabajar con los departamentos TI para definir los niveles de madurez de conformidad actuales y analizar el retorno de inversión (ROI) del proceso de conformidad. Estos pasos pueden ser realizados por un equipo formado por miembros de la plantilla o por consultores externos con experiencia previa en la implantación del estándar.

Los consultores externos deberían trabajar en colaboración con un equipo interno, que esté formado por representantes de las principales unidades de negocio de la compañía. A continuación se describe cada recomendación.

Identificación de los objetivos de negocio
Los planes para la adopción de ISO 27001 deben ser respaldados por un análisis específico de negocio que comprende la enumeración de los objetivos principales de negocio y la garantía de lograr el consenso entre los participantes más relevantes de la compañía. Los objetivos de negocio pueden derivarse de la misión de la compañía, el plan estratégico y objetivos TI actuales, y pueden incluir:

- La garantía de la gestión eficaz del riesgo, que identifique los activos de información y efectúe evaluaciones precisas del riesgo.
- La preservación de las ventajas competitivas de la compañía, si la industria en su conjunto hace uso de información sensible para los negocios.
- La preservación de la reputación y buen nombre de la organización entre los líderes de la industria.
- El aporte de confianza que se proporciona a clientes y socios, concerniente al compromiso de la organización para la protección de los datos.
- El aumento de ingresos de la compañía, beneficio y ahorro en las áreas donde los controles de protección resulten efectivos.

El estándar también enfatiza la conformidad con las obligaciones contractuales, lo cual podría considerarse otro objetivo de negocio clave. Por ejemplo, para una división de banca electrónica *on-line*, la implantación del estándar proporcionaría a clientes y socios un elevado grado de confianza sobre la gestión adecuada de los riesgos derivados del uso de los sistemas de información.

Selección del ámbito de implantación apropiado

Identificar el ámbito de implantación puede ahorrar miles de euros y tiempo. A menudo, la organización no necesita acometer la implantación del estándar en toda la compañía.

El ámbito de conformidad puede restringirse a una división específica, unidad de negocio, tipo de servicio o localización física. Además, una vez se logra con éxito la conformidad para un restringido (aunque relevante) ámbito, puede ser ampliado a otras divisiones o localidades.

La elección del ámbito apropiado es uno de los factores más importantes a lo largo del proceso de conformidad, porque afecta a la viabilidad y costes de implantación del estándar y al retorno efectivo de la inversión realizada por la organización.

ISO 27001, ámbito de implantación

ISO 27001 afirma que todo ámbito de implantación debe comprender un todo o una parte de una organización. Las compañías, sin embargo, no son requeridas para determinar un ámbito de implantación particular.

Acorde con la sección del estándar "B.2.3: Scope of the ISMS", solo los procesos, unidades de negocio y vendedores externos o subcontratas que están en el ámbito de implantación del SGSI deben ser especificados para lograr la certificación.

El estándar también precisa de un listado de las compañías excluidas del ámbito y las razones de su exclusión.

Por consiguiente, es importante la elección de un ámbito que ayude a conseguir los objetivos de negocio identificados. Para ello, la organización deberá evaluar las distintas opciones de ámbitos posibles y clasificarlas en relación a lo bien que se adaptan a cada objetivo.

Las organizaciones también podrían firmar memorandos de acuerdo (*Memorandums Of Understanding*) o acuerdos de nivel de servicio (*Service Level Agreements*) con vendedores y socios comerciales con objeto de implantar un tipo de conformidad indirecta con el estándar. Por ejemplo, una compañía de ropa de confección podría tener un contrato con un proveedor de software para el mantenimiento y actualización de las aplicaciones. Por tanto, la compañía no sería responsable de la conformidad con el estándar del ciclo de vida del desarrollo de la aplicación, siempre y cuando tenga un MOU o SLA firmado con el proveedor de software.

Finalmente, el nivel de operaciones global de la organización es un parámetro esencial para determinar la conformidad en el nivel de complejidad del proceso. Para conocer el nivel correspondiente, las organizaciones necesitan considerar su número de empleados, procesos de negocio, localizaciones de trabajo y productos o servicios ofrecidos.

Determinar los niveles de madures en ISO 27001
Cuando se evalúa el nivel de madurez de conformidad de la organización, los auditores deberían determinar si el equipo de implantación es capaz o no de contestar a las siguientes cuestiones:

- **¿Existe un documento que especifique el ámbito de conformidad?**
  Conforme a ISO 27001, se requiere un documento que especifique el ámbito cuando se planifica la implantación del estándar. El documento debe enumerar todos los procesos de negocio, instalaciones y medios técnicos dispuestos por la organización, en relación a los tipos de información considerados en el SGSI. En el proceso de identificación del ámbito de conformidad, las compañías deben definir claramente las dependencias y conexiones que existan entre la organización y las entidades externas.
- **¿Están los procesos de negocio y flujos de información claramente definidos y documentados?**
  Responder a esta pregunta ayuda a determinar los activos de información contenidos en el ámbito de conformidad y su importancia, además de ayudar en el diseño de un conjunto de controles adecuado para proteger la información cuando es almacenada, procesada y transmitida entre distintos departamentos y unidades de negocio.
- **¿Existe un inventario de activos de información? ¿Está actualizado?**
  Todos los activos que puedan repercutir en la seguridad de la organización deberían estar incluidos en un inventario de activos de información. Los activos de información habitualmente incluyen *software*, *hardware*, documentos, informes, bases de datos, aplicaciones y sus propietarios. Debe mantenerse un inventario estructurado que incluya activos particulares o grupos de activos disponibles en la compañía, su ubicación, uso y propietario. El inventario debe ser actualizado regularmente para garantizar que se utiliza información precisa durante el proceso de certificación de conformidad.
- **¿Como se clasifican los activos de información?**
  Los activos de información deben ser clasificados en función de su importancia desde el punto de vista de la organización y nivel de impacto, y si su confidencialidad, disponibilidad e integridad pudieran estar comprometidas.
- **¿Existe una política de alto nivel de seguridad en activo?**
  Para implantar un estándar para la seguridad de la información es indispensable disponer de una política de seguridad precisa. La política debe transmitir claramente el compromiso de la dirección en relación a la protección de la información y establecer el marco general de seguridad para el negocio y su orientación. Debería también identificar todos los riesgos de seguridad, como serán gestionados y el criterio requerido para la evaluación de riesgos.

- **¿Dispone la organización de un proceso de evaluación de riesgos?**
  Debe realizarse una evaluación de riesgos exhaustiva y que tenga en consideración el valor y vulnerabilidades de los activos TI corporativos, los procesos internos y amenazas externas que pudieran explotar estas vulnerabilidades, así como la probabilidad de cada amenaza. Si existe una metodología de evaluación de riesgos ya implantada, el estándar recomienda que las organizaciones continúen con su uso.

- **¿Existe una lista de controles?**
  Los controles prioritarios deberían ser identificados en base a la información de la evaluación del riesgo y la estrategia general de la organización para mitigar el riesgo global. Los controles seleccionados deberían entonces ser confrontados con el Anexo A del estándar – el cual identifica 133 controles divididos en 11 dominios – para completar el documento de declaración de aplicabilidad, conocido como SOA (*Statement Of Applicability*). Una revisión completa del Anexo A sirve como mecanismo de supervisión para descubrir la posible falta alguna de las áreas de control en la planificación de la conformidad.

Puntos importantes de las declaraciones de aplicabilidad (SOAs)

- Al completar las SOAs, las organizaciones deberían ser capaces de identificar todos los objetivos de control y los controles actuales seleccionados para la implantación.
- Las SOAs no necesitan incluir activos confidenciales ni información de los procesos.
- Los controles adicionales a los ya establecidos en el estándar pueden estar adicionalmente declarados como parte de las SOAs.
- Cualquier control de ISO 27001 que no haya sido seleccionado para la conformidad debe ser justificado.

- **¿Están implantados y documentados los procesos de seguridad?**
  Se deben tomar medidas para mantener el conjunto estructurado de documentos que detalla todos los procedimientos TI de seguridad, los cuales deben estar documentados y monitorizados para garantizar que se implantan acorde a las políticas de seguridad establecidas.
- **¿Está establecido un proceso de gestión para la continuidad de negocio?**
  Debe estar establecido un proceso de gestión que defina el marco general para la continuidad de negocio de la compañía . Debería redactarse un detallado análisis de impacto en base al plan de continuidad de negocio y someterse a prueba y actualización periódicamente.

- **¿Tiene implantada la compañía un programa de concienciación en seguridad?**
  Los esfuerzos realizados en la planificación y documentación deberían ir acompañados de un programa adecuado de concienciación en seguridad TI para que todos los empleados reciban formación concerniente a las necesidades de la seguridad de la información.
- **¿Se realizó alguna auditoria interna?**
  Debe realizarse una auditoria interna para garantizar la conformidad con el estándar y la fidelidad a las políticas de seguridad de la organización y procedimientos.
- **¿Se realizó algún análisis de diferencias?**
  Otro importante parámetro que debe ser determinado es el nivel de conformidad de la organización con respecto a los 133 controles del estándar. Un análisis de disparidades ayuda a las organizaciones a relacionar los controles apropiados con la unidad de negocio pertinente y puede llevarse a cabo durante cualquier momento del proceso de conformidad. Muchas organizaciones realizan el análisis de diferencias al inicio del proceso de conformidad con el objeto de determinar el nivel de madurez de la compañía.
- **¿Fueron identificadas e implantadas las acciones correctivas y preventivas?**
  El estándar está asociado al ciclo Plan-Do-Check-Act" (PDCA) (PDF, 62KB) para ayudar a la organización a conocer lo lejos que ha llegado y lo bien que lo ha hecho en cada ciclo. Esto influye directamente en las estimaciones de tiempo y costes para lograr la conformidad. Para completar el ciclo PDCA, las diferencias identificadas en la auditoría interna deben ser reconducidas mediante la identificación de los controles correctivos y preventivos que sean necesarios y la conformidad de la compañía basada en el análisis de diferencias.
- **¿Están establecidos los mecanismos para medir la efectividad de los controles?**
  Medir la efectividad de los controles es una de las últimas modificaciones introducidas en el estándar. Acorde a ISO 27001, las organizaciones deben integrar métricas que permitan la medición de la efectividad de los controles y que generen resultados que puedan ser comparados y reproducibles.
- **¿Existe una supervisión de la evaluación del riesgo y de los planes para el tratamiento del riesgo?**
  Las evaluaciones del riesgo y de los planes para el tratamiento del riesgo deben revisarse a intervalos regulares establecidos al menos anualmente como parte de la supervisión del SGSI de la organización.

Análisis del retorno de inversión
En base a las labores realizadas hasta este punto, las compañías deberían ser capaces de aproximarse a los tiempos y costes estimados para la implantación del estándar y para cada una de las opciones de ámbito. Las organizaciones necesitan tener presente que cuanto más tiempo se espere para obtener la certificación, mayores son los costes en consultoría o el esfuerzo del personal interno. Por ejemplo, los costes de implantación llegan a ser incluso más críticos cuando la implantación está conducida por las necesidades de mercado o de los clientes. Por lo tanto, cuanto más tiempo se espere para estar en conformidad, más tiempo tarda la organización en llegar al mercado con una certificación adecuada.

AVANZANDO

Implantar ISO 27001 requiere una cuidadosa reflexión, planificación y coordinación que asegure una adaptación cómoda. La decisión acerca de cuando y como implantar el estándar puede verse influida por un número de factores que incluyen los distintos objetivos de negocio, los niveles actuales de madurez TI y esfuerzos para la conformidad, aceptación y concienciación de los usuarios, necesidades de los clientes u obligaciones contractuales y la capacidad de la organización de adaptación al cambio y adopción de los procesos internos.

Para conocer más sobre los estándar, BSI ha preparado una guía disponible en su Web, http://asia.bsi-global.com/InformationSecurity/ISO27001+Guidance/download.xalter. Además, el Web site, www.standardsdirect.org/iso27001.htm, pone a disposición la última versión del estándar.

K. K. Mookhey es fundador y principal consultor de Network Intelligence India (NII) Pvt. Ltd., firma de consultoría en seguridad TI situada en Mumbai, India, que ofrece servicios de hacking ético, auditorías de seguridad, BS 7799 y de gestión de continuidad de negocio. Mookhey ha trabajado en proyectos de investigación para ISACA y ha publicado varios artículos y recomendaciones. También ha liderado equipos en numerosas auditorías de seguridad y labores de implantación y ha formado a personal de firmas financieras del Big Four y compañías del *Fortune* 500 en asuntos relacionados con la seguridad TI.

Khushbu Jithra ha participado en proyectos de documentación para la seguridad de la información para NII y ayuda en la dirección de investigaciones en seguridad para la organización. Además, ella diseña y revisa las propuestas comerciales e informes de consultoría en seguridad, especialmente, aquellas relacionadas con pruebas de penetración, evaluación de vulnerabilidades, ISO 27001 y auditorías de seguridad.

Originally published in *ITAudi*t, Vol. 9, February10, 2006, published by The Institute of Internal Auditors Inc., www.theiia.org/itaudit.

Translation to Spanish made by www.iso27000.es with express authorization of authors K. K. Mookhey y Khushbu Jithra and *ITAudi*t.

Any comment about contents or further distribution, please get contact with *ITAudi*t, www.theiia.org/itaudit.

Any comment about Spanish translation, please get contact with www.iso27000.es.

Originalmente publicado en *ITAudi*t, Vol. 9, February 10, 2006, publicado por The Institute of Internal Auditors Inc., www.theiia.org/itaudit.

Traducción al español realizada por www.iso27000.es con autorización expresa de los autores K. K. Mookhey y Khushbu Jithra y de la publicación *ITAudi*t.

Cualquier comentario sobre el contenido o su distribución, contacten por favor con *ITAudi*t, www.theiia.org/itaudit

Cualquier comentario sobre la traducción, contacten por favor con www.iso27000.es