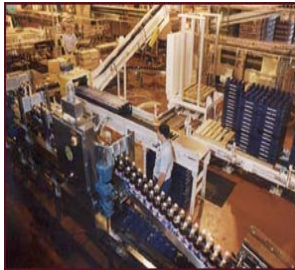




Instituto Nacional de Sistemas Industriales



Boletín Informativo

ISO/IEC 17799:2005 e ISO/IEC 27001:2005 Sistemas de Administración de la Seguridad de la Información



ISO/IEC 17799:2005 – ISO/IEC 27001:2005

Sistemas de Administración de la Seguridad de la Información

La información es el alma de las organizaciones y puede existir en muchas formas. Puede ser impresa o escrita en papel, almacenada electrónicamente, transmitida por correo electrónico o por medios electrónicos, mostrar en videos o hablada en conversaciones. En el actual ambiente competitivo, esta información está constantemente bajo amenaza de varias fuentes. Puede ser interna, externa, accidentalmente o maliciosamente. Con el uso incrementado de nuevas tecnologías para almacenar, transmitir y recuperar información, nos hemos expuesto a un mayor número y tipo de amenazas.

Existe la necesidad de establecer una Política de Seguridad de la Información integral dentro de todas las organizaciones. Se necesita asegurar la confidencialidad, integridad y disponibilidad de la información corporativa más importante y la información de los clientes. La norma para los Sistemas de Administración de la Seguridad de la Información BS 7799-2 (predecesora de ISO / IEC 27001:2005) se ha convertido en uno de los más implantados.

¿Qué es un Sistema de Administración de la Seguridad de la Información?

El Sistema de Administración de Seguridad de la Información es un enfoque sistemático para administrar la información de la organización para que permanezca segura. Incluye personas, procesos y sistemas de tecnología de la información. *British Standard Institute (BSI)* ha creado un código de prácticas para estos sistemas, que ahora han sido internacionalmente adoptados como ISO/IEC 27001:2005.



¿Qué es ISO/IEC 17799:2005?

ISO/IEC 17799, Código de prácticas para Administración de la Seguridad de la Información, establece guías y principios generales para las organizaciones para poder iniciar, implementar, mantener y mejorar la administración de la seguridad de la información. Los objetivos mencionados ofrecen una guía general para las metas más comunes en cuestión de administración de la seguridad de la información. Contiene las mejores prácticas para los objetivos de control y controles en las siguientes áreas de la administración de la seguridad de la información:

- Política de seguridad.
- Organización de la seguridad de la información.
- Administración de activos.
- Seguridad de los recursos humanos.
- Seguridad física y del ambiente.
- Comunicación y administración de operaciones.
- Control de accesos.
- Adquisición de sistemas de información, desarrollo y mantenimiento.
- Administración de los incidentes relacionados con la seguridad de la información.
- Administración de la continuidad de negocios.
- Cumplimiento.

¿Qué es ISO/IEC 27001:2005?

ISO/IEC 27001:2005 (anteriormente BS 7799-2:2002) es una norma que establece los requisitos para un Sistema de Administración de la Seguridad de la Información. Ayuda a identificar, administrar y minimizar el rango de amenazas a las cuales la información está expuesta. La norma está diseñada para asegurar la selección de controles de seguridad adecuados para proteger los activos de la información y brindar confianza a las partes interesadas incluyendo a los clientes de la organización.

Es adecuado para diferentes tipos de usos organizacionales, incluyendo los siguientes:

- Formulación de requerimientos de seguridad y objetivos.
- Asegurar que los riesgos de seguridad son administrados eficientemente en cuanto a costos.
- Asegurar el cumplimiento de leyes.
- Como un marco para la implementación y administración de controles para asegurar que los objetivos específicos de seguridad de una organización son cumplidos.
- Identificación y aclaración de procesos de administración de la seguridad de la información existentes.

- Determinar el estado de las actividades de administración de la seguridad de la información.
- Ser utilizadas por auditores internos o externos para determinar el grado de cumplimiento de las políticas, directrices y normas implantadas por una organización.
- Proporcionar información relevante acerca de políticas de seguridad de la información, directrices, normas y procesos para socios del mercado.
- Proporcionar información relevante a los clientes acerca de la seguridad de la información.



Transición de BS 7799-2:2002 a ISO/IEC 27001:2005

BS 7799 parte 2 ha sido sustituida y publicada por ISO (*International Organization for Standardization*) como ISO/IEC 27001:2005 el 15 de octubre de 2005.

La nueva versión internacional de la norma aclara y fortalece los requisitos de la norma original e incluye cambios en las siguientes áreas:

- Evaluación de riesgos.
- Obligaciones contractuales.
- Alcance.
- Decisiones de administración.
- Medición de la efectividad de controles seleccionados.

El periodo de transición será en un total de 18 meses desde la fecha de emisión del Memorando de Entendimiento (MoU) entre el *UK Department of Trade and Industry (DTI)* y *UKAS* que fue firmado el 23 de enero de 2006. Esto significa que hasta el 23 de julio de 2006 (seis meses) las organizaciones que estén considerando certificarse en BS 7799:2002 parte 2 o están obligadas a una visita de evaluación, pueden escoger ser evaluados según la norma BS 7799:2002 parte 2 o ISO/IEC 27001:2005.

Desde el 23 de julio de 2006 las organizaciones serán evaluadas contra la nueva norma internacional ISO/IEC 27001:2005.

Todos los certificados deben ser transferidos a ISO/IEC 27001:2005 para finales del mes 18 del periodo de transición y cualquier no conformidad debe ser aclarada antes del 27 de julio de 2007. Después de esta fecha los certificados emitidos por BSI en BS7799:2002 parte 2 no serán válidos.

Publicación de ISO/IEC 17799:2005

La versión revisada de ISO/IEC 17799:2005 fue publicada el 10 de junio de 2005. La versión ISO/IEC 17799:2000 ha sido retirada.

Esta nueva versión contiene 17 nuevos controles y algunos controles de la versión anterior han sido eliminados o combinados con otros. En total, ahora existen 134 controles.

La versión 2005 habla de aspectos como:

- Seguridad de servicios de entrega externos y la provisión de servicios de outsourcing.
- Localización de las vulnerabilidades actuales, tales como administración de ajustes o parches.
- Seguridad antes, durante y al finalizar el empleo.
- Mayor enfoque en el manejo de riesgos e incidentes
- Comunicación móvil, remota y distribuida así como el tratamiento de la información.



Relación entre ISO/IEC 17799:2005 e ISO/IEC 27001:2005

ISO/IEC 17799:2005 sigue siendo un código de prácticas la cual define las mejores prácticas para controles. Sigue utilizando el término “debería” en todos los controles dejando la selección de todos los controles y su implementación a decisión de la organización. Por el contrario, la norma ISO/IEC 27001:2005 es una especificación de requisitos y usa el término “debe de” en todos los controles permitiendo a las organizaciones utilizarla para propósitos de certificación.

La relación entre ISO/IEC 17799:2005 e ISO/IEC 27001:2005 sigue existiendo ya que esta última incluye el Anexo A que contiene los controles de ISO/IEC 17799:2005.

Para información adicional sobre cómo adquirir servicios de asesoría, consultoría o los documentos mencionados en este boletín informativo (ISO/IEC 27001:2005, ISO/IEC 17799:2005, etc), así como sobre nuestros cursos de capacitación sobre estas normas, favor de comunicarse con la Lic. Matilde Mota a los teléfonos (55) 3330-2720 ó 3330-2721 de 9:00 a 18:00 horas de lunes a viernes, o envíe un mensaje de correo electrónico a la dirección info@insi.org
