Guía de Transición

Pasando de ISO/IEC 27001:2005 a ISO/IEC 27001:2013

El nuevo estándar internacional para los sistemas de gestión de seguridad de la información

bsi.

...making excellence a habit.™

Los negocios exitosos entienden el valor de la información oportuna y precisa, de las buenas comunicaciones y de la discreción. La seguridad de la información se trata tanto de explotar las oportunidades de nuestro mundo interconectado así como de la gestión de riesgos.

Es por ello que las organizaciones necesitan una gestión robusta de seguridad de la información.

Esta guía ha sido diseñada para ayudarle a conocer los requerimientos del nuevo estándar internacional para la gestión de la seguridad de la información ISO/IEC 27001:2013, el cual es la primera revisión de ISO/IEC 27001:2005.

ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI) para cualquier organización sin importar su tipo o tamaño. BSI recomienda que cada organización tenga un sistema implementado para mantener la confidencialidad, integridad y disponibilidad de la información. Esto deberá incluir su propia información así como la información de sus clientes y de otras partes interesadas. En un mundo cada vez más interconectado no debe sobre estimarse hacerlo.

Conocer los requerimientos del nuevo estándar internacional nunca fue más fácil. Esta guía está basada en el nuevo libro de David Brewer 'An introduction to ISO/IEC 27001:2013', que comparte una guía práctica sobre cómo lograr los requerimientos de ISO/IEC 27001:2013 y en 'Understanding the new ISO management system requirements', que hace la revisión de un sistema de gestión en general y cómo hacer la transición de este a nuevos estándares. Estos libros se encuentran disponibles en BSI Shop.

Esta guía de transición le ayudará a comprender la relación entre ISO/IEC 27001:2013 y su predecesora ISO/IEC 27001:2005, así como el impacto que el nuevo estándar tendrá en su SGSI existente.

Nota. *Esta guía de transición está diseñada para leerse en conjunto con BS ISO/IEC 27001:2013 – Information Technology – Security techniques – Information Security management systems – Requirements. No contiene el contenido completo del estándar y no debe utilizarse como fuente principal de referencia en lugar del estándar.*

¿Por qué adoptar un estándar de seguridad de la información?

Existen varias razones por las que las organizaciones eligen tener un sistema de gestión de seguridad de la información (SGSI). Estas generalidades se ajustan a dos categorías: garantía del mercado y gobernabilidad. La garantía del mercado se refiere a la habilidad de un SGSI para proveer confianza dentro del mercado, en la capacidad de una organización para cuidar de la información de forma segura. En particular, inspirar la confianza de que la organización mantendrá la confidencialidad, integridad y disponibilidad de la información del cliente. La gobernabilidad se refiere a como son gestionadas las organizaciones. En este caso, un SGSI es reconocido por ser una forma proactiva de gestionar la seguridad de la información.

Un escenario típico en el caso de la garantía del mercado es cuando una compañía demanda varias garantías de sus proveedores para mantenerlos como proveedores para esa compañía. Lo común solía ser que esas compañías requirieran a sus proveedores cumplir con ISO 9001, pero ahora las empresas también están buscando garantías de sus proveedores con respecto a ISO/IEC 27001. En este caso, la compañía tendrá el deber de preservar la seguridad de la información bajo su custodia. Si tal información es compartida con un proveedor, entonces la compañía fallará en este deber si el manejo de la información por parte del proveedor fuera inseguro. No importa si la empresa opta por hacer esto por razones de gobierno corporativo o garantía del mercado, solo importa lo que haga.

Como ambas categorías están cercanamente relacionadas, una organización puede elegir inicialmente tener un SGSI para inspirar confianza dentro del mercado. Una vez que tenga un SGSI, y a medida que madure, el personal de la organización a menudo experimentará los beneficios de ser capaz de mejorar la gestión de la seguridad de la información. Por lo tanto las razones de la organización para tener un SGSI pueden expandirse para cubrir tanto la garantía del mercado como el gobierno corporativo. Igualmente, otra organización puede iniciar teniendo un SGSI para una mejor gestión. Sin embargo, a medida que su SGSI madure, debe comunicar las experiencias y noticias sobre las auditorías exitosas de certificación al mercado y conocer el poder de la garantía del mercado para atraer nuevos clientes.

Implementando ISO/IEC 27001

ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un SGSI. Estos requerimientos describen el comportamiento previsto de un SGSI una vez que es completamente operacional. El estándar no es una guía paso a paso sobre cómo construir o crear un SGSI.

Sin embargo existe una serie de libros y otros estándares en la serie ISO/IEC 27000 que le pueden asistir. Hay tres estándares principales:

1. ISO/IEC 27003: Tecnología de Información – Técnicas de seguridad – Guía de implementación del sistema de gestión de seguridad de la información;
2. ISO/IEC 27004, Tecnología de Información – Técnicas de seguridad – Gestión de seguridad de la información – Medidas; y
3. ISO/IEC 27005, Tecnología de Información – Técnicas de seguridad – Gestión de riesgos de seguridad de la información.

Los tres estándares guía se encuentran en revisión y en la actualidad sólo se refieren a los requerimientos de ISO/IEC 27001:2005

Comparando ISO/IEC 27001:2013 con ISO/IEC 27001:2005

ISO/IEC 27001:2013 es la primera revisión de ISO/IEC 27001. En primer lugar y ante todo la revisión ha tomado en cuenta la experiencia práctica del uso del estándar: actualmente hay 17,000 certificados en el mundo. Sin embargo, ha habido otras dos influencias mayores en la revisión. La primera es un requerimiento de ISO que todo estándar nuevo o revisado debe ajustarse a la estructura de alto nivel y debe tener el texto central idéntico definido en el Anexo SL de la Parte 1 de las Directrices de ISO/IEC. Conforme a estos requerimientos se tendrá una tendencia para hacer que todos los estándares de sistemas de gestión luzcan igual, con la intención de que los requerimientos del sistema de gestión que no son una disciplina específica sean redactados de la misma manera en todos los estándares de sistemas de gestión. Estas son buenas noticias para todas las organizaciones que operan sistemas de gestión integrados, por ejemplo los sistemas de gestión que conforman varios estándares, como ISO 9001 (calidad), ISO 22301 (continuidad del negocio) así como ISO/IEC 27001. La segunda influencia fue una decisión para alinear ISO/IEC 27001 con los principios y guías dados por ISO 31000 (gestión de riesgos). De nuevo, estas son buenas noticias para los sistemas de gestión integrados pues ahora una organización puede aplicar la misma metodología de riesgos a través de varias disciplinas.

El resultado es que estructuralmente ISO/IEC 27001:2013 luce muy diferente a ISO/IEC 27001:2005. Además, no hay requerimientos duplicados y están expresados de una manera que permite mayor libertad de elección sobre como implementarlos. Un buen ejemplo de esto es que la identificación de activos, amenazas y vulnerabilidades no es más larga que un pre requisito para la identificación de riesgos para la seguridad de la información. El estándar ahora es más claro en cuanto a que los controles no deben de ser seleccionados del Anexo A, pero son determinados a través del proceso de tratamiento de riesgos. Sin embargo, el Anexo A continúa sirviendo como una verificación para asegurar que no existen controles necesarios que se hayan pasado por alto.

Se han introducido nuevos conceptos (ó actualizado) como los siguientes:

Concepto nuevo/actualizado	Explicación
Contexto de la organización	El ambiente en el que la organización opera
Problemas, riesgos y oportunidades	Reemplaza acciones preventivas
Partes interesadas	Reemplaza accionistas (stakeholders)
Liderazgo	Requerimientos específicos para la alta dirección
Comunicación	Hay requerimientos específicos tanto para comunicaciones internas como externas
Objetivos de seguridad de la información	Los objetivos de seguridad de la información ahora se establecen como funciones relevantes y niveles
Evaluación de riesgos	La identificación de activos, amenazas y vulnerabilidades ya no es un pre requisito para la identificación de riesgos de seguridad de la información
Propietario de riesgo	Reemplaza propietario de los activos
Plan de tratamiento de riesgos	La efectividad del plan de tratamiento de riesgos es ahora considerado como más importante que la efectividad de los controles
Controles	Los controles ahora son determinados durante el proceso de tratamiento de riesgos, en lugar de ser seleccionados del Anexo A
Información documentada	Reemplaza documentos y registros
Evaluación del desempeño	Cubre las mediciones del SGSI y de la efectividad del plan de tratamiento de riesgos
Mejora continua	Se pueden utilizar metodologías distintas a Planear-Hacer-Verificar-Actuar (PDCA por sus siglas en inglés)

Cláusula 0: Introducción
Esta cláusula es mucho más corta que su predecesora. En particular la sección sobre el modelo PDCA ha sido eliminada. La razón para esto es que el requerimiento es para la mejora continúa (ver Cláusula 10) y el PDCA es solo una propuesta para cumplir con este requerimiento. Hay otras propuestas y las organizaciones son ahora libres de utilizarlas si así lo desean.

La introducción también hace énfasis en el orden en el cual serán presentados los requerimientos, estableciendo que el orden no refleja la importancia o implica el orden en el cual serán implementados.

Cláusula 1: Alcance
Esta también es una cláusula mucho más corta. En particular no hay referencia a la exclusión de controles en el Anexo A.

Cláusula 2: Referencias normativas
La única referencia normativa es ISO/IEC 27000, Tecnología de información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Resumen y vocabulario.

Cláusula 3: Términos y definiciones
No hay ningún término o definición en ISO/IEC 27001:2013. En su lugar, los lectores son referidos a ISO/IEC 27000. Sin embargo, por favor asegúrese de que está utilizando una versión de ISO/IEC 27000 que haya sido publicada posterior a ISO/IEC 27001:2013, de otra manera esta no contendrá los términos y condiciones correctos. Este es un documento importante para leer. Muchas definiciones, por ejemplo 'sistema de gestión' y 'control' han sido cambiados y ahora conforman las definiciones dadas en las nuevas directrices de ISO e ISO 31000. Si un término no está definido en ISO/IEC 27000, por favor utilice la definición dada en el Diccionario Inglés Oxford. Esto es importante, de otra manera puede resultar en confusión y malos entendidos.

Cláusula 4: Contexto de la organización
Esta es una nueva cláusula que en parte direcciona el concepto depreciado de acciones preventivas y en parte establece el contexto para el SGSI. Cumple con estos objetivos al reunir asuntos relevantes internos y externos (por ejemplo, aquellos que afectan la habilidad de la organización para lograr los resultados esperados del SGSI) con los requisitos de las partes interesada para determinar el alcance del SGSI.

Deberá notar que el término 'asunto' cubre no solo problemas, que pueden haber sido el tema de una acción preventiva en el estándar previo, sino también temas importantes para direccionar el SGSI, como cualquier garantía del mercado y las metas del gobierno corporativo que la organización establezca para su SGSI. Mayor orientación se da en la Cláusula 5.3 de ISO 31000:2009.

Note que el término 'requerimiento' es una 'necesidad o expectativa establecida, generalmente implícita u obligatoria'. Combinada con la Cláusula 4.2, esto en si mismo puede ser pensado como un requisito del gobierno, en sentido estricto como un SGSI que no se ajusta a las expectativas públicas generalmente aceptadas y que ahora podría ser gobernado no conforme al estándar.

El requerimiento final (Cláusula 4.4) es establecer, implementar, mantener y mejorar continuamente el SGSI de acuerdo con los requerimientos del estándar.

Cláusula 5: Liderazgo
Esta cláusula pone los requerimientos a la 'alta dirección' que es la persona o grupo de personas que dirigen y controlan la organización al más alto nivel. Tenga en cuenta que si la organización que es tema del SGSI es parte de un corporativo, entonces el término 'alta dirección' se refiere a la organización pequeña. El propósito de este requerimiento es demostrar el liderazgo y compromiso liderando desde la dirección.

Una responsabilidad particular de la alta dirección es establecer la política de seguridad de la información, y el estándar define las características y propiedades que la política debe incluir.

Finalmente, la cláusula establece requerimientos en la alta dirección para asignar responsabilidades y autoridades relevantes a la seguridad de la información, destacando dos roles en particular concernientes a la conformidad del SGSI con ISO/IEC 27001 y reportando el desempeño del SGSI.

Cláusula 6: Planeación
Cláusula 6.1.1, General: Esta cláusula trabaja con las Cláusulas 4.1 y 4.2 para completar la nueva forma de trabajar con las acciones preventivas. La primera parte de la cláusula (por ejemplo hasta e incluyendo 6.1.1 c)) concierne a evaluación de riesgos, mientras que la cláusula 6.1.1. d) concierne a tratamiento de riesgos.

Cláusula 6.1.2, Evaluación de riesgos de la seguridad de información: Esta cláusula específicamente concierne a la evaluación de riesgos de la seguridad de información. En alineación con los principios y guías dadas en ISO 31000, esta cláusula quita la identificación de activos, amenazas y vulnerabilidades como pre requisito de identificación de riesgos. Esto amplía la elección de métodos de evaluación de riesgos que una organización puede usar y que aún conforman el estándar. La cláusula también ser refiere a los 'criterios de aceptación de la evaluación de riesgos', que permite otros criterios además de un solo nivel de riesgos. Los criterios de aceptación de riesgos pueden ser expresados ahora en términos de otros niveles, por ejemplo, los tipos de control utilizados para el tratamiento de riesgos.

La cláusula se refiere a los 'propietarios del riesgo' más que a los 'propietarios de los activos' y posteriormente (en la Cláusula 6.1.3 f)) requiere la aprobación del plan de tratamiento de riesgos y riesgos residuales.

En otros aspectos la cláusula se parece mucho a su contraparte en ISO/IEC 27001:2005 al requerir a las organizaciones evaluar las consecuencias, probabilidades y niveles de riesgo.

Cláusula 6.1.3, Tratamiento de riesgos de seguridad de la información: Esta cláusula concierne al tratamiento del riesgo de la seguridad de la información. Es similar a su contraparte en ISO/IEC 27001:2005, sin embargo, se refiere a la 'determinación' de controles necesarios más que a la selección de controles del Anexo A. Sin embargo, el estándar mantiene el uso del Anexo A como una verificación para asegurar que un control necesario no se ha pasado por alto y las organizaciones son todavía requeridas para producir un Enunciado de Aplicabilidad (SOA por sus siglas en inglés). La formulación y aprobación del plan de tratamiento de riesgos es ahora parte de esta cláusula.

Cláusula 6.2, Objetivos de la seguridad de la información y planeación para lograrlos: Esta cláusula concierne a los objetivos de seguridad de la información. Se utiliza la frase 'funciones y niveles relevantes', aquí el término 'función' se refiere a las funciones de la organización y el término 'nivel', a sus niveles de gestión, en el que 'alta dirección' es el mayor. La cláusula define las propiedades que los objetivos de seguridad de la información de la organización deben poseer.

Cláusula 7: Soporte

Esta cláusula inicia con un requerimiento que las organizaciones deben determinar y proveer los recursos necesarios para establecer, implementar, mantener y mejorar continuamente el SGSI. Expresado de forma simple, este es un requerimiento muy poderoso que cubre todas las necesidades de recursos de un SGSI.

La cláusula continua con los requerimientos para competencia, conocimiento y comunicación, que son similares a sus contrapartes en ISO/IEC 27001:2005.

Finalmente, existen requerimientos para 'información documentada'. La 'información documentada' es un término nuevo que reemplaza las referencias en el estándar 2005 de 'documentos' y 'registros'. Estos requerimientos están relacionados con la creación y actualización de información documentada y su control. Los requerimientos son similares a sus contrapartes en ISO/IEC 27001:2005 para el control de documentos y para el control de registros.

Tenga en cuenta que los requerimientos para la información documentada están presentes en la cláusula a la que se refieren. No se encuentran resumidos en una cláusula para ellos mismos, como lo estaban en ISO/IEC 27001:2005.

Cláusula 8: Operación

Esta cláusula trata sobre la ejecución de los planes y procesos que son tema en las cláusulas anteriores.

1. **Cláusula 8.1** trata sobre la ejecución de acciones determinadas en la Cláusula 6.1, el logro de los objetivos de seguridad de la información y los procesos sub contratados;

2. **Cláusula 8.2** trata sobre el desempeño de las evaluaciones de riesgo de la seguridad de la información en intervalos planeados, o cuando los cambios significativos son propuestos u ocurren; y

3. **Cláusula 8.3** trata sobre la implementación del plan de tratamiento de riesgos.

Cláusula 9: Evaluación del desempeño

Cláusula 9.1, Monitoreo, medición, análisis y evaluación: El primer párrafo de la Cláusula 9.1 establece los objetivos generales de la cláusula. Como recomendación general, determine qué información necesita para evaluar el desempeño de la seguridad de información y la efectividad de su SGSI. Trabajar hacia atrás desde esta 'necesidad de información' para determinar qué medir y controlar, cuándo, a quién y cómo. No tiene mucho sentido el monitorear y hacer mediciones sólo porque su organización tiene la capacidad de hacerlas. El seguimiento y la medición por si apoyan el requisito de evaluar el desempeño de seguridad de la información ya la eficacia del SGSI.

Tenga en cuenta que una organización puede tener muchas necesidades de información, y estas necesidades pueden cambiar con el tiempo. Por ejemplo, cuando un SGSI es relativamente nuevo, puede ser importante solo el monitoreo para supervisar la asistencia a, por así decir, los eventos de concientización de seguridad de la información. Una vez que la tasa prevista se logra, la organización debe ver más hacia la calidad de un evento de conocimiento. Se debe hacer esto estableciendo objetivos de conocimiento específicos y determinando el grado en que los asistentes han entendido lo aprendido. Más tarde, la información necesita extenderse para determinar que impacto tiene este nivel de conocimiento en la seguridad de la información de la organización.

Cláusula 9.2, Auditoría interna: Esta cláusula es similar a su contraparte en ISO/IEC 27001:2005. Sin embargo, el requerimiento tiene gestión responsable para asegurar que las acciones de auditoría que se tomen sin demora indebida se han eliminado, ya que están efectivamente cubiertas por los requerimientos de la Cláusula 10.1 (en particular 10.1 a),c) y d)). El requerimiento que los auditores no deben auditar su propio trabajo ha sido también eliminado, ya que está cubierto por el requerimiento de asegurar la objetividad e imparcialidad (Cláusula 9.2 e)).

Cláusula 9.3, Revisión de la gestión: Más que especificar entradas y salidas específicas, esta cláusula ahora ubica los requerimientos sobre los temas para consideración durante la revisión. El requerimiento para revisiones que tendrán lugar a intervalos determinados permanece pero el requerimiento para mantener las revisiones por lo menos una vez al año ha sido eliminado.

Cláusula 10: Mejora

Debido a la nueva forma de manejar las acciones preventivas, no hay requerimientos para las acciones preventivas en esta cláusula. Sin embargo, hay algunos requerimientos para las nuevas acciones correctivas. La primera es reaccionar ante las no conformidades y tomar acción, como aplica, para controlar y corregir las no conformidades y trabajar con las consecuencias. La segunda es determinar donde existen no conformidades similares, o donde pueden ocurrir potencialmente. Aunque el concepto de acciones preventivas ha evolucionado aún hay una necesidad de considerar las no conformidades potenciales, aunque como una consecuencia de una no conformidad actual. También existe un nuevo requerimiento para asegurar que las acciones correctivas son apropiadas a los efectos de las no conformidades encontradas.

El requerimiento para la mejora continua se ha extendido para cubrir la idoneidad y suficiencia de un SGSI así como su efectividad, pero ya no especifica cómo una organización puede lograr esto.

Anexo A

El título del Anexo A es ahora "objetivos de control de referencia y controles" y la introducción es simplificada. Establece que los objetivos de control y los controles derivan directamente de ISO/IEC 27002:2013 y que el Anexo es utilizado en el contexto de la Cláusula 6.1.3.

Durante la revisión de ISO/IEC 27002 el número de controles ha sido reducido de 133 controles a 114 controles, y el número de cláusulas mayores ha sido expandido de 11 a 14. Algunos controles son idénticos o muy similares; algunos se han fusionado; algunos han sido eliminados y otros son nuevos. Por ejemplo:

1. A.5.1.1, las políticas para la seguridad de la información son muy similares a las originales A.5.1.1, Documento de Políticas de Seguridad de la información.
2. El anterior A.10.10.1, Registro de Auditoría, A.10.10.2, Monitoreo del uso del sistema, y A.10.10.5, Registro de fallas, han sido fusionados para formar el nuevo A.12.4.1, Registro de eventos.
3. El anterior A.11.6.2, Aislamiento del sistema sensible, ha sido eliminado debido a que en un mundo interconectado, este control interfiere con el objetivo de ser interconectado.
4. A.17.2.1, Disponibilidad de instalaciones de procesamiento de información, es un nuevo control.

Es importante apreciar que la utilidad de un control para una organización no debe cambiar por haber sido este eliminado del Anexo A. De acuerdo con la Cláusula 6.1.3, los controles ahora son determinados con las bases del tratamiento de riesgos. Si una organización desea tratar riesgos particulares deliberadamente sin conectar una computadora a Internet u otras redes, entonces tendrá que utilizar un control como el anterior A.11.6.2 independientemente de si se encuentra en el Anexo A o no.

El Anexo A permanece como un 'anexo normativo'. Esto no es porque el Anexo A contenga requerimientos normativos, sino porque, por las normas ISO, se hace referencia a un requisito normativo, por ejemplo en este caso, las Cláusulas 6.1.3 c) y d).

Otros anexos

El Anexo original B, los principios OECD y este estándar internacional, han sido eliminados ya que ahora son una referencia antigua, que refiere al PDCA.

El antiguo Anexo C, Correspondencia entre ISO 9001:2000, ISO 14001:2004 y este estándar internacional, también han sido eliminados porque ambos estándares han sido revisados y utilizarán la misma estructura de alto nivel e idéntico texto principal al de ISO/IEC 27001:2013.

El Anexo B, Bibliografía, de ISO/IEC 27001:2013 es una versión actualizada de su contraparte, el Anexo D en ISO/IEC 27001:2005.

Información documentada

Los requerimientos para la información documentada están distribuidos en el estándar. Sin embargo, en resumen son:

1.3	Alcance del SGSI
5.2	Política de seguridad de la información
6.1.2	Proceso de evaluación de riesgos de seguridad de la información
6.1.3	Proceso de tratamiento de riesgos de seguridad de la información
6.1.3 d)	Enunciado de aplicabilidad
6.2	Objetivos de seguridad de la información
7.2 d)	Evidencia de competencia
7.5.1 b)	La información documentada determinada por la organización como siendo necesaria para la efectividad del SGSI
8.1	Control y planeación operacional
8.2	Resultados de la evaluación de riesgos de seguridad de la información
8.3	Resultados del tratamiento de riesgos de seguridad de la información
9.1	Evidencia de los resultados del monitoreo y mediciones
9.2 g)	Evidencia de los programas y resultados de auditoría
9.3	Evidencia de los resultados de las revisiones de gestión
10.1 f)	Evidencia de la naturaleza de las no conformidades y cualquier acción tomada subsecuentemente
10.1 g)	Evidencia de los resultados de cualquier acción correctiva

Tablas de mapeo

Las siguientes dos tablas ilustran la relación entre ISO/IEC 27001:2013 e ISO/IEC 27001:2005. La Tabla A trabaja con el cuerpo principal del estándar y la Tabla B con el Anexo A. Estas tablas están simplificadas para motivos ilustrativos solamente. Un mapeo de datos más detallado está disponible como PDF descargable (en idioma inglés) en el sitio web de BSI **www.bsigroup.com/27kmapping**

La Tabla A enlista en la columna de la izquierda los títulos de las cláusulas menores en ISO/IEC 27001:2013. Para cada una, la entrada en la columna derecha muestra los títulos de la cláusula en ISO/IEC 27001:2005 que de alguna manera corresponden. Para ver exactamente cuál es nuevo y cuál ha sido eliminado, por favor consulte el mapeo de datos detallado.

Tabla A: Mapeo de las cláusulas de ISO/IEC 27001:2013 a ISO/IEC 27001:2005

0	Introducción	**0**	Introducción
1	Alcance	**1**	Alcance
2	Referencias normativas	**2**	Referencias normativas
3	Términos o definiciones	**3**	Términos o definiciones
4.1	Comprender la organización y su contexto	**8.3**	Acciones preventivas
4.2	Comprender las necesidades y expectativas de las partes interesadas	**5.2.1 (c)**	Identificar y conducir los requerimientos legales y regulatorios y las obligaciones contractuales de seguridad
4.3	Determinar el alcance del sistema de gestión de seguridad de la información	**4.2.1 a)** **4.2.3 f)**	Defina el alcance y los límites Asegure que el alcance sea adecuado
4.4	Sistema de gestión de seguridad de la información	**4.1**	Requerimientos generales
5.1	Liderazgo y compromiso	**5.1**	Compromiso de la dirección
5.2	Políticas	**4.2.1 b)**	Definir una política de SGSI
5.3	Roles organizacionales, responsabilidades y autoridades	**5.1 c)**	Establecer roles y responsabilidades para la seguridad de la información
6.1.1	Acciones para hacer frente a riesgos y oportunidades – general	**8.3**	Acciones preventivas
6.1.2	Evaluación de riesgos de seguridad de la información	**4.2.1 c)** **4.2.1 d)** **4.2.1 e)**	Defina el enfoque de la evaluación de riesgos Identificar los riesgos Analizar y evaluar los riesgos

Continua

Tablas de mapeo - continuación

6.1.3	Tratamiento de riesgos de seguridad de la información	**4.2.1 f)** **4.2.1 g)** **4.2.1 h)** **4.2.1 i)** **4.2.1 j)** **4.2.2 a)**	Identifique y evalúe opciones para el tratamiento de riesgos Seleccionar objetivos de control y controles para el tratamiento de riesgos Obtener aprobación de la dirección sobre los riesgos residuales propuestos Preparar un enunciado de aplicabilidad Preparar un enunciado de aplicabilidad Formular un plan de tratamiento de riesgos
6.2	Objetivos de seguridad de la información y planeación de los mismos	**5.1 b)**	Asegurar los objetivos del SGSI y establecer los planes
7.1	Recursos	**4.2.2 g)** **5.2.1**	Gestión de recursos para el SGSI Provisión de recursos
7.2	Competencia	**5.2.2**	Capacitación, conocimiento y competencia
7.3	Conocimiento	**4.2.2 e)** **5.2.2**	Implementar capacitación y programas de conocimiento Capacitación, conocimiento y competencia
7.4	Comunicación	**4.2.4** **5.1 d)**	Comunicar las acciones y mejoras Comunicar a la organización
7.5	Información documentada	**4.3**	Requerimientos de documentación
8.1	Planeación operacional y control	**4.2.2 f)**	Gestionar operaciones del SGSI
8.2	Evaluación de riesgos de seguridad de la información	**4.2.3 d)**	Revisar evaluaciones de riesgos en intervalos planeados
8.3	Tratamiento de riesgos de seguridad de la información	**4.2.2 b)** **4.2.2 c)**	Implementar el plan de tratamiento de riesgos Implementar controles
9.1	Monitoreo, medición, análisis y evaluación	**4.2.2 d)** **4.2.3 b)** **4.2.3 c)**	Definir como medir la efectividad Tomar revisiones regulares de la efectividad del SGSI Medir la efectividad de los controles
9.2	Auditoría interna	**4.2.3 e)** **6**	Conducir auditorías internas al SGSI Auditorías internas del SGSI
9.3	Revisión de la gestión	**4.2.3 f)** **7**	Tomar una revisión de la gestión del SGSI Revisión de la gestión del SGSI
10.1	No conformidades y acciones correctivas	**4.2.4** **8.2**	Mantener y mejorar el SGSI Acciones correctivas
10.2	Mejora continua de la información	**4.2.4** **8.1**	Mantener y mejorar el SGSI Mejora continua

La Tabla B enlista los grupos de control en el Anexo A para ISO/IEC 27001:2013 en la columna del lado izquierdo. Cada uno de ellos tiene un objetivo de control común. El número en la parrilla se refiere al número de controles en cada ese grupo en particular. Del lado derecho hay once columnas que corresponden a los controles en cada uno de los títulos de las once cláusulas mayores en el Anexo A de ISO/IEC 27001:2005. Una X significa que hay una correspondencia entre los controles del 2013 y del 2005. Para poder ver esas relaciones exactas, por favor consulte el mapeo de datos detallado.

Tabla B: Mapeo de controles del Anexo A

ISO/IEC 27001: 2013 (Número de controles)	ISO/IEC 27001:2005										
	Política de seguridad	Organización	Gestión de activos	Recursos Humanos	Físicos	Comunicaciones	Control de acceso	Adquisiciones	Incidentes	Continuidad del negocio	Cumplimiento
	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15
A.5.1 Dirección de la gestión de la seguridad de información (2)	X										
A.6.1 Organización interna (5)		X		X		X					
A.6.2 Dispositivos móviles y tele trabajo (2)							X				
A.7.1 Antes de emplear (2)				X							
A.7.2 Durante el empleo (3)				X							
A.7.3 Despido y cambio del empleado (1)				X							
A.8.1 Responsabilidad para los activos (4)			X	X							
A.8.2 Información clasificada (3)			X			X					
A.8.3 Manejo de medios (3)						X					
A.9.1 Requerimientos del negocio de control de acceso (2)							X				
A.9.2 Gestión de acceso de usuario (6)				X			X				
A.9.3 Responsabilidades de los usuarios (1)							X				
A.9.4 Sistema y aplicación de acceso de control (5)							X	X			
A.10.1 Controles criptográficos (2)								X			
A.11.1 Áreas de seguridad (6)					X						
A.11.2 Equipo (9)					X		X				
A.12.1 Procedimientos operacionales y responsabilidades (4)						X					
A.12.2 Protección contra el mal uso						X					
A.12.3 Copia de seguridad (1)						X					
A.12.4 Acceso y monitoreo (4)						X					
A.12.5 Control de software operacional (1)								X			
A.12.6 Gestión de la vulnerabilidad técnica (2)								X			
A.12.7 Consideraciones de auditoría del sistema de información (1)											X
A.13.1 Gestión de seguridad de la red (3)						X	X				
A.13.2 Transferencia de información (4)		X				X					
A.14.1 Requerimientos de seguridad de los sistemas de información (3)						X		X			
A.14.2 Seguridad en el desarrollo y procesos de soporte (9)						X		X			
A.14.3 Datos de prueba (1)								X			
A.15.1 Seguridad de información en relaciones con proveedores (3)		X									
A.15.2 Gestión de prestación de servicios del proveedor (2)						X					
A.16.1 Gestión de los incidentes y mejoras de la seguridad de información (7)									X		
A.17.1 Continuidad de la seguridad de información (3)										X	
A.17.2 Redundancias (1)											
A.18.1 Cumplimiento con requerimientos legales y contractuales (5)											X
A.18.2 Revisiones de seguridad de la información (3)		X								X	

Guía de Transición

Estrategias

La estrategia de transición puede ser una de las siguientes:

1 *Un sencillo "cambio de imagen", tomando los cambios mínimos necesarios para los procesos existentes del SGSI y la documentación existente, o*

2 *Tomando una imagen completamente fresca de su SGSI, utilizando el estándar revisado para hacer mejoras, que pueden ser significativas para algunas organizaciones.*

La transición utilizando la estrategia minimalista podría llevarse a cabo con mucha rapidez. Dadas las mejoras de ISO/IEC 27001:2013 sobre su predecesora, las organizaciones están motivadas para hacer la transición tan pronto como puedan. Sin embargo, una vez que la planeación detallada de la transición se pone en marcha, las organizaciones pueden desear hacer mejoras. Si bien esto motiva, las organizaciones deben decidir si:

1 *Destacarlo como oportunidades para mejorar con la intención de hacer cambios en un tiempo apropiado en el futuro; o*

2 *Hacer los cambios inmediatamente.*

El primer curso de acción es más típico para una organización que ha adoptado una estrategia de transición minimalista, mientras que el segundo es mejor si la organización está usando la transición como una razón para hacer otros cambios.

Dónde comenzar

En ambos casos, un lugar sensible para comenzar es el análisis Gap entre el SGSI existente y la nueva versión del estándar. Esto formará las bases para las tareas requeridas del 'proyecto' de transición. Conociendo cómo el SGSI existente se ajusta al estándar anterior también puede ayudar, ya que identifica las áreas existentes con información documentada que requerirán cambiar.

Cambios en el SGSI

Recuerde que los cambios que usted haga a la información documentada existente deberán ser guardados para cumplir con la Cláusula 7.5

Áreas donde el cambio será mínimo

Información documentada
La 'información documentada' es un nuevo término que aplica a lo que la versión 2005 del estándar se refiere como 'documentos' y 'registros'. En la transición a ISO/IEC 27001:2013, simplemente reemplaza los términos 'documentos' y 'registros' con el término 'información documentada'. Si necesita hacer una distinción, reconozca que los documentos son intenciones declaradas, mientras que los registros son evidencias de resultados anteriores.

Políticas
Existe un requerimiento en ISO/IEC 27001:2005 para producir una política SGSI, la cual contiene la política de seguridad de la información y el criterio de riesgos.

El requerimiento de política en ISO/IEC 27001:2013 (Cláusula 5.2) solo se refiere a la política de seguridad de la información, pero hay un requerimiento (Cláusula 6.1.2) para establecer y mantener los criterios de riesgos, y posteriormente en esta cláusula un requerimiento para retener información documentada sobre el proceso de evaluación de riesgos. Como una organización tendrá ya documentada su política de seguridad de la información y el criterio de riesgos en su política de SGSI, y dado que ISO/IEC 27001:2013 no otorga nombres a los documentos, una organización debe decidir mantener su política de SGSI igual. No hay necesidad de cambiar el nombre. Toda la organización necesita es saber cuál de los requerimientos de información documentada de ISO/IEC 27001:2013 cumple.

Sin embargo, hay otros requerimientos de seguridad de la información en ISO/IEC 27001:2013 que una organización debe considerar para las cuestiones de política y que por lo tanto deben ser incluidas en la política del 'SGSI'. Estas son:

1 *El criterio para llevar a cabo evaluaciones de riesgos de seguridad de la información (ver Cláusula 6.1.2 a)2));*

2 *La política organizacional hacia la liberación de su política de seguridad de la información a las partes interesadas (ver Cláusula 5.2 g)); y*

3 *La política organizacional con respecto a las comunicaciones externas (ver Cláusula 7.4).*

Existen también dos requerimientos que conciernen al 'compromiso', ver las Cláusulas 5.2 c) y d). Mientras que las políticas pueden ser escritas para demostrar compromiso, las organizaciones pueden desear incluir dos declaraciones de intenciones, una para cada uno de estos requerimientos.

Evaluación de riesgos
En contraste con ISO/IEC 27001:2005, ISO/IEC 27001:2013 no requiere explícitamente la identificación de activos, amenazas y vulnerabilidades como prerrequisitos para la identificación de riesgos. También utiliza el vocabulario de ISO 31000 (Gestión de riesgos – principios y guías) y por lo tanto ISO/IEC 27001:2013 se refiere a las consecuencias más que a los impactos. Sin embargo, la estructura general del requerimiento (identificar riesgos, evaluar las consecuencias y probabilidades) es la misma que en ISO/IEC 27001:2005 y por lo tanto un método que se ajusta a los requerimientos de ISO/IEC 27001:2005 debe también conformar los requerimientos de ISO/IEC 27001:2013. Esto significa que si no hay cambios o los cambios mínimos deben de requerirse para la información documentada existente relacionada con la evaluación de riesgos/metodología de tratamiento de riesgos o su implementación.

Control documental
No se requerirán cambios a los procedimientos documentados existentes en materia de control de documentación.

Términos de referencia para la alta dirección
Será necesario un cambio para acomodar las responsabilidades específicas dadas en la Cláusula 5.1 a) al h).

Responsabilidades
Será necesario un cambio para acomodar las responsabilidades específicas dadas en la Cláusula 5.3 a) y b).

Conciencia
Será necesario un cambio para acomodar los requerimientos de la Cláusula 7.4 como el proceso de creación de conciencia que puede ser considerado como una forma de comunicación.

Auditoría interna
No serán necesarios cambios a los procedimientos de documentación existente relacionados con auditoría interna.

Revisión de la gestión
No serán necesarios cambios a los procedimientos documentados existentes de revisión de la gestión, además de asegurar que los temas enlistados en las Cláusulas 9.3 a)-f) son considerados.

Acciones correctivas
Los procedimientos existentes pueden necesitar ser reforzados para asegurarse de que reaccione ante las no conformidades y tome acción, como aplica, controlarlos y corregirlos y trabajar con las consecuencias. Usted también puede requerir determinar si existen no conformidades similares, o que puedan potencialmente ocurrir, y asegurar que las acciones correctivas apropiadas son implementadas para trabajar con los efectos.

Mejora
Asegura que existen procedimientos para la mejora continua que se extienden para cubrir la idoneidad y adecuación de un SGSI así como su efectividad.

Áreas que potencialmente requieren un replanteamiento

Alcance del sistema de gestión
La redacción de la Cláusula 4.3 (y en particular 4.3 c)) pretende aclarar que el alcance del SGSI (como distinto del alcance de la certificación) incluye todo lo que es de interés del SGSI. Por lo tanto el alcance incluirá fuentes de riesgos externos, tales como hackers y desastres naturales, así como cualquier función que esté sub contratada.

Si, después de un análisis, una organización considera que hay entidades que deben de ser incluidas en el alcance de su SGIS que previamente fueron excluidas, la transición a ISO/IEC 27001:2013 provee una oportunidad para redefinir el alcance del SGSI, así como de demostrar conformidad con la Cláusula 4.3

Objetivos de seguridad de la información
Si una organización considera sus objetivos de seguridad de la información como objetivos de políticas atemporales, el requerimiento de la Cláusula 6.2, que se refiere a 'funciones y niveles relevantes', puede ser un shock. Sin embargo, solo puede requerir un cambio a la forma en que la conformidad se describe. Es probable que una organización establezca objetivos en todos los niveles y funciones pertinentes, y es sólo cuestión de reconocer que lo hace y describir cómo lo hace.

Por ejemplo, es una buena práctica cuando se plantean acciones para definir objetivos, asignar responsabilidades y establecer fechas límite para completarlas. Si una organización ya hace esto, entonces está ya cumpliendo con la cláusula.

Áreas que necesitan actualización

El enunciado de aplicabilidad
El Anexo A ha sido actualizado para reflejar los controles que ahora están descritos en ISO/IEC 27002:2013. Mientras las organizaciones no necesitan ya seleccionar controles del Anexo A, este aún se utiliza para determinar si cualquier control necesario ha sido omitido (ver Cláusula 6.1.3c)) y las organizaciones están obligadas a producir un SOA. El formato de un ISO/IEC 27002:2013 conforme a SOA no necesita ser diferente del estándar anterior. Sin embargo, el establecimiento de controles es diferente, y por lo tanto las organizaciones requerirán actualizar sus SOAs. Cuando haga esto, tenga cuidado de asegurar que el control de la implementación se ajuste estrictamente a la redacción dada en el Anexo A.

Nuevos requerimientos que deben de cumplirse ya

Partes interesadas y sus requerimientos
La Cláusula 4.2 requiere que la organización determine las partes interesadas que son relevantes para el SGSI y sus requerimientos. Es probable que una organización ya conozca esta información. Por ejemplo, las partes interesadas pueden incluir clientes y proveedores y sus requerimientos estarán documentados en contratos, órdenes de compra, especificaciones, etc. Por lo tanto todo lo que hay que hacer es identificar donde se documenta esta información y hacer referencia a ella. Es probable que la organización que ya hace uso de esta información, provea conformidad con otras cláusulas tales como 6.1

Integración
La Cláusula 5.1 b) requiere que la alta dirección asegure la integración de los requerimientos del SGSI en los procesos de negocio de la organización. Si las funciones de negocio de una organización debían ser representadas por uno o varios diagramas de flujo de trabajo y por lo tanto las actividades que corresponden a los requerimientos del SGSI se extienden a lo largo de los flujos de trabajo, entonces el requerimiento de integración probablemente se está cumpliendo. Sin embargo si los requerimientos del SGSI están contenidos un solo flujo de trabajo que no contiene nada más, entonces el requerimiento de integración probablemente no se esté cumpliendo.

En el primer caso, se trata de la mejor manera de demostrar la conformidad. Si los diagramas de flujo de trabajo existen, o pueden visualizarse, por ejemplo: a través de una interface de software, entonces será una forma fácil de demostrar la conformidad. Si el requerimiento de integración no se cumple, entonces el concepto de flujo de trabajo puede proveer una ruta para lograr la conformidad.

Comunicación
Los requerimientos de la Cláusula 7.4 (comunicaciones) son más específicos que los requerimientos equivalentes en la versión anterior del estándar. Sin embargo, los nuevos requerimientos siguen prácticas comunes y por lo tanto los requerimientos de comunicación pueden estar ya satisfechos.

Los nuevos requerimientos que pueden presentar un cambio

Problemas
Es probable que los problemas mencionados en la Cláusula 4.1 sean bien conocidos por una organización, pero no necesariamente por escrito y desde luego no de una forma que demuestre la conformidad.

Un problema importante para la mayoría de las organizaciones podría ser su motivación para tener un SGSI. Una organización podría saber lo que era y habría sido un factor importante sobre como el SGSI original había sido diseñado. Tenga en cuenta que esta motivación puede cambiar con el tiempo: la motivación original puede ser sustituida por otras como los beneficios de tener un sistema de gestión SGSI.

Otro problema importante podría ser aquellos concernientes a la seguridad de la información. Si estos son desconocidos o la organización tiene incertidumbre sobre ellos, puede ser posible aplicar la ingeniería inversa a ellos a partir de una consideración de la política de seguridad de la información, de los objetivos y de la evaluación de riesgos de seguridad de la información y el tratamiento de riesgos.

Otros problemas, que probablemente ya han sido abordados por la organización podrían relacionarse con la operación del SGSI, como el compromiso de la dirección y la motivación del personal. Finalmente, las organizaciones deben considerar buscar a través de las actas de las reuniones de dirección y sus registros de acciones preventivas para otros problemas. Después de todo, las Cláusulas 4.1 y 6.1.1 son la nueva forma de trabajar con las acciones preventivas.

Acciones para abordar riesgos y oportunidades – general
Los procedimientos existentes de acciones preventivas necesitan ser revisados o reemplazados para asegurar la conformidad con las Cláusulas 4.1, 4.2 y 6.1.1. Las organizaciones son dirigidas hacia la información dada anteriormente en este folleto.

Monitoreo, medición, análisis y evaluación
Los requerimientos de la Cláusula 9.1 son más detallados y exactos que los requerimientos para el SGSI y el control de efectividad en ISO/IEC 27001:2005. Desde la perspectiva de la transición puede ser mejor comenzar con una hoja en blanco. Las organizaciones son dirigidas hacia la información dada anteriormente en este folleto.

Observaciones finales

Todas las organizaciones son diferentes y esta guía necesita ser interpretada en el contexto de las necesidades individuales de cada organización. Lo que puede llegar a ser fácil para algunos puede ser un reto para otros y viceversa. Se espera que esta guía sea un punto de partida útil para la mayoría de las organizaciones.

ISO/IEC 27001
cursos de capacitación

Desarrolle su conocimiento de ISO/IEC 27001:2013 con los cursos de capacitación de BSI.

Nuestros instructores expertos pueden ayudarle a obtener habilidades adicionales para realizar la transición. O si usted se encuentra iniciando con un nuevo sistema de gestión de seguridad de la información podemos enseñarle todo lo que necesita saber acerca del estándar, cómo implementarlo y auditarlo en conformidad al mismo dentro de su negocio.

Para conocer más visite:
bsigroup.com.mx/iso27001

Nuevos libros sobre Seguridad de la Información están disponibles

¿Necesita información adicional para ayudarle a realizar la transición?
Ya sea usted nuevo con el estándar, esté iniciando con el proceso de certificación, o se encuentre ya en el camino, nuestros libros le darán una comprensión detallada de los nuevos estándares, guías de implementación y detalles de certificación y auditorías – todos escritos por líderes especialistas en seguridad de la información, incluyendo a David Brewer, Bridget Kenyon, Edward Humphreys y Robert Christian.
Capítulos de ejemplo están disponibles

Encuentre más información en www.bsigroup.com/27books

Biografía de David Brewer

David Brewer, PhD, FBCS, es reconocido mundialmente por las contribuciones que ha hecho a la gestión de seguridad de la información. Él fue uno de los primeros consultores en asesorar al Gobierno Británico en materia de seguridad de la información a principios de 1980 y fue uno de los desarrolladores del estándar original de SGSI, BS 7799-2:2002. Ha impartido capacitación sobre SGSI y consultoría en Europa, Estados Unidos, África Oriental, Oriente Medio y el lejano Oriente y administra un sistema de gestión integrado conforme a ISO 9001, ISO/IEC 27001 e ISO 22301. Es miembro del comité ISO responsable de la serie de estándares ISO/IEC 27001, jugando un rol significativo en el desarrollo de ISO/IEC 27001:2013 y es co-editor de la revisión de ISO/IEC 27004.

BSI/MX/77/SC/1013/es

Conocemos ISO/IEC 27001;

BSI dio forma al estándar original.

BSI...

- Dio forma al estándar original ISO/IEC 27001
- Cuenta con los instructores más altamente capacitados y especializados
- Ofrece la más amplia gama de soluciones de soporte en el mercado
- Es el organismo de certificación número uno en el Reino Unido, Estados Unidos y Corea
- Cuenta con más de 70,000 clientes alrededor del mundo
- Tiene una reputación internacional incomparable por su excelencia

BSI Group México S de RL de CV

Oficinas Ciudad de México
Torre Mayor, Paseo de la Reforma No. 505
Piso 50, Suite A
Col. Cuauhtémoc, C.P. 06500,
México, D.F.
Tel: +52 (55) 5241 1370
Lada sin costo 01 800 044 0274