Extraído de GESTION Edición Octubre 2012

NUEVO ESTÁNDAR INTERNACIONAL EN CONTINUIDAD DEL NEGOCIO ISO 22301:2012

El pasado 15 de mayo, el comité técnico 223 de la Organización Internacional para la Normalización (ISO, por sus siglas en inglés), publicó la versión final ISO 22301:2012 "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos". Esta norma reemplazará al estándar BS 25999-2:2007 "Gestión de la Continuidad del Negocio: Especificaciones". El nuevo modelo es certificable y auditable. El estándar trae nuevos términos y novedades en la documentación requerida. Seguidamente, se presentará su naturaleza, la documentación exigida y el proceso de transición del BS 25999-2:2007 al nuevo estándar.

Por Alberto G. Alexander, Ph.D., AMBCI

INTRODUCCIÓN

El Sistema de Gestión de la Continuidad del Negocio (SGCN) se ha convertido en una exigencia para las empresas que compiten el día de hoy en los mercados globalizados. La tendencia mundial es que ya las empresas no compitan entre sí: la competencia es entre cadenas de suministros. Una cadena de suministros, para mantenerse operando, no puede tener ningún eslabón débil; ninguno de sus componentes puede dejar de operar ya que si un elemento del todo dejara de funcionar se paraliza toda la serie, generando el caos. Cada miembro del sistema tiene que demostrar que es un proveedor confiable. Esto se logra teniendo en cada empresa un SGCN que proteja a los procesos esenciales que permiten originar los productos o servicios que desea el cliente.

¿Qué es un SGCN? Es parte del sistema de gestión gerencial que establece, implementa, opera, evalúa, mantiene y mejora la continuidad del negocio. "Un SGCN da confianza a terceros ya que ha identificado los procesos esenciales que soportan a los productos o servicios que se desean proteger de escenarios de amenazas producto del análisis del riesgo" (Alexander, 2007). Cada escenario de amenazas tiene una estrategia de continuidad que se materializa a través de planes de reanudación de operaciones que son ensayados regularmente. Una empresa con un SGCN ensayado periódicamente es muy difícil que deje de operar y no pueda suministrar sus productos o servicios.

NATURALEZA DEL ISO 22301:2012

El nuevo estándar ISO 22301:2012 tiene por nombre "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio". Este modelo aparece como producto de una evolución de lineamientos, buenas prácticas y estándares en continuidad del negocio. En la Figura Nº 1, se presenta un bosquejo de la evolución.

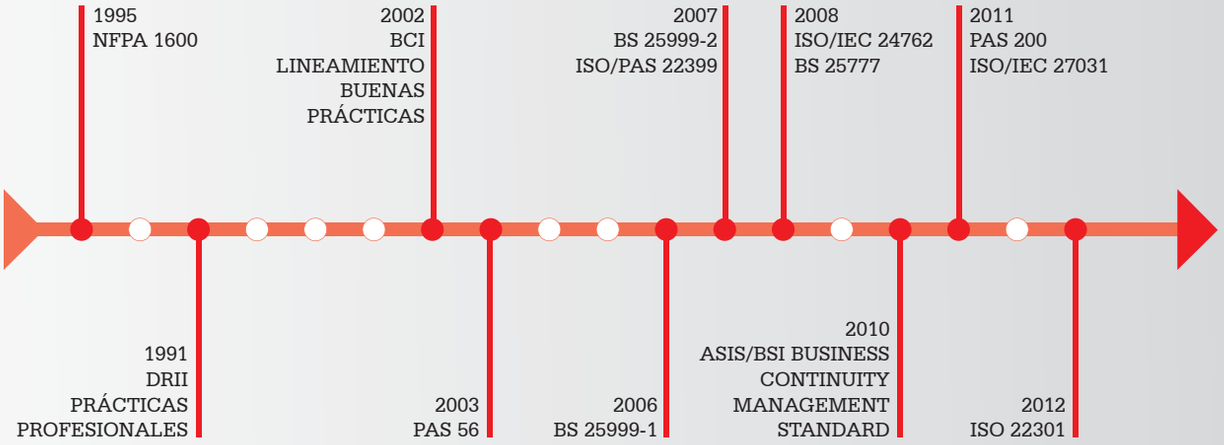
El lineamiento más antiguo es el NFPA 1600, publicado en 1995, el cual estableció una serie de conjuntos de criterios para la gestión de desastres, emergencias y programas de continuidad para las organizaciones. En 1997 el Disaster Recovery Institute International (DRII), publicó las "Prácticas Profesionales para la Gestión del Negocio".

En el año 2002, el Business Continuity Institute publicó los lineamientos de "Buenas Prácticas para la Continuidad del Negocio". En 2003, se publica el lineamiento PAS 56. Esta guía estableció el proceso, principios y terminología de un sistema de gestión de continuidad del negocio. Describió las actividades y resultados involucrados en el establecimiento de un proceso de gestión de continuidad del negocio. Desarrolló una serie de recomendaciones para las buenas prácticas para la anticipación a incidentes, y respuesta y técnicas para la evaluación.

En 2006, se publicó el lineamiento BS 25999-1, el cual describió de manera concreta el ciclo de vida de la continuidad del negocio. Su enfoque representó las opciones continuas del programa de continuidad del negocio en la organización.

FIGURA Nº 1

EVOLUCIÓN DE LOS ESTÁNDARES EN CONTINUIDAD DEL NEGOCIO



En el año 2007, se publicó el estándar BS 25999-2:2007, el primer estándar internacional certificable y auditable. Fue elaborado con el objetivo de definir los requisitos para un enfoque de sistemas de gestión para la gestión de la continuidad del negocio basado en buenas prácticas, para su uso por organizaciones grandes, medianas y pequeñas que operan en los sectores industrial, comercial, público y de beneficencia.

En el mismo año se publicó el ISO/PAS 22399, el cual generó los lineamientos genéricos para una organización interesada en desarrollar un sistema de gestión con criterios para el desempeño de preparación ante incidentes y continuidad operacional.

En el año 2008, se publicó el lineamiento ISO/IEC 24762 que desarrolló guías para la provisión de información y comunicación frente a la recuperación de desastres. Ese mismo año, se publicó el BS 25777, un código de buenas prácticas sobre gestión de la continuidad. Una norma que, emparentada con la BS 25999 sobre continuidad de negocio, definió un código de buenas prácticas sobre continuidad centrado en las infraestructuras TIC de las organizaciones.

En el año 2010, se publicó el "ASIS/BSI Business Continuity Management Standard." Este lineamiento, basado en el BS 25999 (parte 1 y 2), especifica los requerimientos para un sistema de gestión de continuidad del negocio, para permitir a las organizaciones identificar, desarrollar e implementar políticas, objetivos, capacidades, procesos y programas para poder atender eventos alteradores que pudieran paralizar a la organización.

En 2011, se publicó el PAS 200, "Gestión de Crisis - Lineamiento y Buena Práctica". Es un lineamiento diseñado para ayudar a las empresas a tomar pasos prácticos para mejorar su habilidad de manejar crisis. También en el año 2011, se publicó el lineamiento ISO/IEC 27031, el cual describe los conceptos y principios de tecnología de información y comunicación (ICT) para preparar a una organización para la continuidad del negocio. Es aplicable a todo tipo de empresa.

Finalmente, en el año 2012, la Organización Internacional para la Normalización (ISO) publicó el estándar "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos". Este estándar certificable y auditable capta los principales conceptos de los demás lineamientos publicados desde 1995.

El estándar ISO 22301:2012 "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos" aplica el ciclo **Plan-Do-Check-Act** (PDCA por sus siglas en inglés) para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y la mejora continua de su efectividad. El modelo ha sido creado con consistencia con otros estándares de gestión, tales como: ISO 9001:2008, ISO 27001:2005, ISO 20000-1:2011, ISO 14001:2004 y con el ISO 28000:2007.

FIGURA Nº 2

CICLO PDCA APLICADO AL PROCESO DE CONTINUIDAD DEL NEGOCIO

En la figura Nº 2, se puede apreciar como el "SGCN toma insumos de las partes interesadas, requerimientos para la gestión de la continuidad, y a través de las necesarias acciones y procesos produce resultados de continuidad para cumplir con los requerimientos". (ISO 22301:2012)

En esta misma figura, se observa cada componente del modelo. El "establecimiento" es el ***Plan***. Allí se aprecian los principales requerimientos. Las secciones 4, 5, 6 y 7 de la norma corresponden al establecimiento. Seguidamente se tiene la "implementación y operación", el cual es el ***Do***; esta etapa del proceso está compuesta por los requerimientos de la sección 8. Contemplamos en la figura Nº 2 sus principales requerimientos. Luego se tiene la fase "monitoreo y revisión", la cual representa al ***Check***. Allí se pueden apreciar los principales requerimientos de esta sección. Esta fase comprende los requerimientos de la sección 9 de la norma. Finalmente, se tiene la fase de "mantenimiento y mejora", representando a la fase ***Act***, la cual engloba todos los requerimientos de la cláusula 10 de la norma.

DOCUMENTACIÓN REQUERIDA POR EL ISO 22301:2012

El nuevo modelo exige cierta documentación obligatoria. La documentación obligatoria que una empresa de acuerdo a su alcance debe desarrollar es la siguiente:

1	Lista de requisitos legales, normativos y de otra índole.
2	Alcance del SGCN.
3	Política de la continuidad del negocio.
4	Objetivos de la continuidad del negocio.
5	Evidencia de competencias del personal.
6	Registros de comunicación con las partes interesadas.
7	Análisis del impacto en el negocio.
8	Evaluación de riesgos, incluido un perfil del riesgo.
9	Estructura de respuesta a incidentes.
10	Planes de continuidad del negocio.
11	Procedimientos de recuperación.
12	Resultados de acciones preventivas.
13	Resultados de supervisión y medición.
14	Resultados de la auditoría interna.
15	Resultados de la revisión por parte de la dirección.
16	Resultados de acciones correctivas.

TRANSICIÓN DE BS 25999-2:2007 A ISO 22301-2012

En la Figura Nº 3, se tiene una representación gráfica del proceso de transición del estándar BS 25999-2:2007 al ISO 22301:2012.

El United Kingdom Accreditation Service (UKAS) ha dado las pautas para la transición del BS 25999-2:2007 al nuevo modelo ISO 2301:2012. Como se puede apreciar en la Figura Nº 3, las empresas podrán certificarse al estándar BS 25999-2:2007 hasta noviembre de 2012. A partir de esa fecha el estándar desaparece y solo prevalecerá el ISO 22301:2012. Las empresas que obtuvieron la certificación al BS 25999-2:2007 tienen hasta mayo de 2014 para realizar la transición y realizar su ascenso al nuevo modelo. (Sharp, 2012).

PRINCIPALES ADICIONES AL ISO 22301:2012

El nuevo estándar tiene 106 requerimientos versus 56 que tiene el BS 25999-2:2007. El modelo tiene una serie de cláusulas adicionales que a continuación se detallan:

CLÁUSULA 4: CONTEXTO DE LA ORGANIZACIÓN

Esta cláusula introduce los requerimientos necesarios para establecer el contexto del SGCN tal como debe aplicar a los requerimientos y necesidades de la organización dentro de un alcance determinado.

La cláusula también requiere que la organización determine su apetito al riesgo, así como los aspectos legales y regulatorios que apliquen a la organización.

El ISO 22301 requiere que la organización determine qué será cubierto por la continuidad del negocio, así como también qué será excluido. La organización tiene la exigencia de comunicar a las partes, tanto internas como externas, el alcance del SGCN.

CLÁUSULA 5: LIDERAZGO

Esta cláusula hace un buen resumen de las exigencias a la alta gerencia de la empresa, en relación a su rol en el SGCN. Hay nuevos requerimientos para la alta gerencia, tales como:

1. ASEGURARSE QUE EL SGCN ES COMPATIBLE CON LA DIRECCIÓN ESTRATÉGICA DE LA ORGANIZACIÓN.
2. INTEGRACIÓN DE LOS REQUERIMIENTOS DEL SGCN EN LOS PROCESOS DE NEGOCIOS.
3. COMUNICAR LA IMPORTANCIA DE UNA EFICAZ GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

CLÁUSULA 6: PLANEACIÓN

Esta cláusula requiere que la organización claramente defina los objetivos de continuidad del negocio y desarrolle proyectos para alcanzarlos. Estos objetivos deben estar relacionados a la política de continuidad del negocio y deben ser conmensurables. Al establecer los objetivos se debe considerar el nivel mínimo de productos y servicios que serían aceptables para que la organización pueda alcanzar sus objetivos globales de negocio.

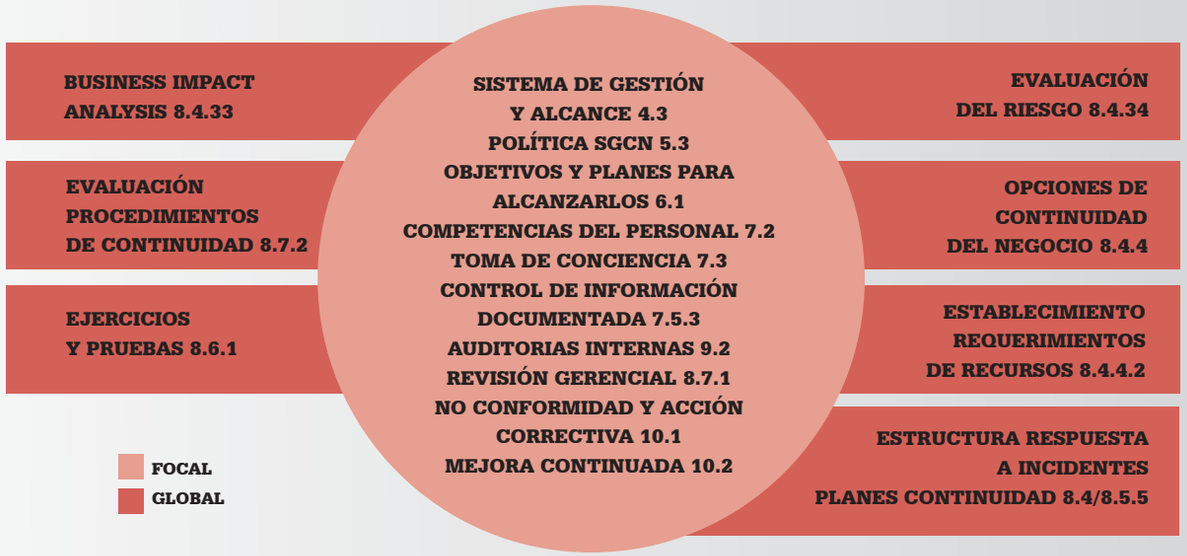
FIGURA Nº 3

PROCESO DE TRANSICIÓN

FIGURA Nº 4

CATEGORIZACIÓN DE LAS CLÁUSULAS EN GLOBALES Y FOCALES

ISO 22301:2012



CLÁUSULA 7: SOPORTE

La cláusula 7 detalla el soporte requerido para establecer, implementar y mantener un eficaz SGCN. Esto cubre los recursos requeridos, las competencias humanas, toma de conciencia y comunicaciones con partes interesadas, así como requerimientos para la gestión documentaria.

Esta sección, al cubrir toma de conciencia, es bastante específica ya que exige que todas las personas bajo el control de la organización estén conscientes de la política de continuidad del negocio, entender su contribución al logro de eficacia del SGCN y las implicancias de no tener conformidad con sus requerimientos. También, las personas deben conocer su rol en un momento de alteración.

La mayor adición en la cláusula 7 es el tema de comunicaciones. Este es un punto importantísimo al gestionar cualquier alteración en la organización.

CLÁUSULA 8: OPERACIÓN

Cláusula 8.1 La cláusula planificación operacional y control es nueva. Esta cláusula requiere que la organización asegure la existencia de procesos que hayan sido desarrollados para gestionar que los riesgos al SGCN estén correctamente implementados.

Cláusula 8.2.2 El *Business Impact Analysis*, introduce un nuevo término: "esquemas de tiempo priorizados". Este término se relaciona con el conocido *Recovery Time Objective* (RTO) y define el orden y los tiempos para la recuperación de actividades críticas que soportan los productos y servicios claves.

El término *Maximum Tolerable Period of Disruption (MTPD)*, el cual es definido en la sección 3 del estándar, no es usado en la norma. Pero en la cláusula 8.2.2 (c) plantea que la "organización debe establecer esquemas de tiempo priorizados para reanudar operaciones.

que apoyan los productos/servicios claves, en un nivel específico aceptable, tomando en consideración el tiempo en el cual, los impactos, de no reanudar operaciones se convertirían en inaceptables". Como se puede apreciar, el concepto del MTPD sigue vigente.

Cláusula 8.2.3 La evaluación del riesgo le presta atención de que ciertos aspectos "financieros y obligaciones gubernamentales" requieren de comunicación, a distintos niveles de detalle, de los riesgos que pudieran alterar las actividades priorizadas.

Cláusula 8.4.2 La estructura para respuesta a incidentes ha expandido sus requerimientos; específicamente la necesidad para "identificar impactos de amenazas que justifican la iniciación de una respuesta formal y la necesidad de utilizar la salvaguarda de vidas humanas como primera prioridad, al establecer comunicados internos y/o externos".

Cláusula 8.4.5 Recuperación es un nuevo requerimiento. El estándar plantea que la "organización debe tener procedimientos documentados para poder restablecer y retornar las actividades del negocio de medidas temporales creadas para soportar los requerimientos normales de la organización".

IMPLANTACIÓN DEL ISO 22301:2012

Cuando una organización desea iniciar la implantación del modelo ISO 22301:2012 siempre se genera la interrogante de ¿por dónde empezar? ¿Será conveniente iniciar con el *Business Impact Analysis*? ¿O con la estructura para responder a incidentes? En fin, hay una serie de opciones disponibles.

La manera adecuada es ir de lo general a lo particular. En la figura Nº 4, se han categorizado las cláusulas de la norma en "globales" y "focales". Para el inicio del proceso de implantación es recomendable atender primero a las cláusulas globales y luego iniciar las focales. Las cláusulas globales, permiten crear la plataforma inicial en la construcción del SGCN. Las cláusulas focales son la parte netamente técnica de la norma y requieren para su desarrollo de la infraestructura que desarrollan las globales.

El comité 223 de ISO está actualmente trabajando en la elaboración del Lineamiento 22313. Este documento consistirá en buenas prácticas y recomendaciones, indicando qué prácticas una organización debiera desarrollar para implementar un SGCN eficaz. Este documento podrá ser utilizado como guía para la implantación del modelo, o también para efectos de usarlo como autoevaluación. Se estima que este documento estará publicado a finales de 2012 o primer trimestre de 2013.

CONCLUSIONES

A nivel mundial, con las nuevas reglas de los mercados internacionales, las empresas tienen la obligación de poder demostrar que son proveedores confiables. Ante la presencia de cualquier evento alterador, de tener un SGCN implementado las empresas pueden, dentro de un tiempo estimado, reanudar sus operaciones y continuar ofreciendo sus productos y servicios. Un SGCN es la indicación que los proveedores son confiables.

El estándar ISO 22301:2012 engloba las distintas metodologías y buenas prácticas en continuidad del negocio generadas en los últimos casi 20 años.

Las empresas que hayan implementado y certificado el BS 25999-2:2007 tienen un límite de tiempo para realizar la migración al nuevo modelo.

Las organizaciones que estén implementando un SGCN bajo el esquema BS 25999-2:2007 deben iniciar la transición hacia el ISO 22301:2012.

Alberto Alexander Servat, Ph.D. por la University of Kansas, M.A. por la Northern Michigan University y Licenciado en Administración por la Universidad de Lima, tiene amplia experiencia académica en instituciones de posgrado peruanas e internacionales. Es auditor líder de Sistemas de Gestión de la Calidad ISO 9000, certificado por el International Register of Certificated Auditors (IRCA), Inglaterra.

También es auditor líder del ISO 14000, certificado ante el (EARA), Inglaterra y el (RAB), EE.UU., así como auditor líder del Modelo de Gestión de Seguridad de Información ISO 27001:2005 certificado ante Internacional Register of Certificated Auditors (IRCA), Inglaterra. Su más reciente publicación es "Diseño y Gestión de un Sistema de Seguridad de Información; Óptica ISO 27001:2005". Ha sido fundador y director gerente de la firma consultora Eficiencia Gerencial y Productvidad S.A., con sede en Venezuela. Actualmente, desempeña las mismas funciones para América Latina desde Perú.

Referencias Bibliográficas

Alexander, Alberto. Diseño y Gestión de un Sistema de Gestión de Seguridad de Información: Óptica ISO 27001:2005. Editorial Alfa Omega 2007. Colombia.

ISO 22301. Societal Security - Business Continuity Management Systems-Requirements 2012.

Sharp, John. The Route Map to Business Continuity management meeting the requirements. British Standards Institute, United Kingdom.