RISI 9(1), 91 - 110 (2012)
REVISTA DE INVESTIGACIÓN DE SISTEMAS E INFORMÁTICA
FACULTAD DE INGENERÍA DE SISTEMAS E INFORMÁTICA
UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS
ISSN 1815-0268 (VERSIÓN IMPRESA)
ISSN 1816-3823 (VERSIÓN ELECTRÓNICA)

Revisión de modelos de gestión de continuidad del negocio

Review of models of management of business continuity

Jesús Quevedo

Universidad Nacional Mayor de San Marcos
Facultad de Ingeniería de Sistemas e Informática

jesus.quevedouribe@gmail.com

RESUMEN

Eventos tales como el terrorismo, terremotos, fallas de la tecnología, entre otros, que pueden generar interrupciones en la entrega de productos y servicios, generan desde hace muchos años la necesidad de establecer lineamientos para la gestión de continuidad del negocio, que permitan a las empresas seguir entregando sus productos y servicios a un nivel aceptable. En el presente artículo se abordan los conceptos más relevantes respecto de la continuidad del negocio, se realiza una breve revisión de la literatura desde sus orígenes y se describen los modelos de gestión de continuidad del negocio más recientes.

Palabras clave: continuidad del negocio, modelo, impacto, riesgo.

ABSTRACT

Events such as terrorism, earthquakes, technology failures, among others, that can generate interruptions in delivery of products and services, generate since many years ago the need to establish a framework for business continuity management, that enable companies continue to deliver its products and services at an acceptable level. This article addresses the most relevant concepts of business continuity, presents a brief review of the literature from its origins and describes the latest business continuity management models.

Keywords: business continuity, model, impact, risk.

1. INTRODUCCIÒN

Las actividades terroristas, los climas extremos, la falla de las herramientas, la interrupción en la cadena de suministro y las pandemias son ejemplos de grandes eventos que pueden derivar en interrupciones y falla de las organizaciones que entregan productos y servicios [1]. Los terremotos, las erupciones volcánicas y las huelgas industriales, son sólo algunos de los incidentes que han llevado a una mayor sensibilización de las empresas sobre lo que significa la continuidad en toda América [2]. Como consecuencia de ello aparecieron los sitios de recuperación de desastres en EE.UU. a finales de los 70's y el concepto de Planeamiento de Recuperación de Desastres (Disaster Recovery Planning - DRP) [3]. El primer uso conocido del término "Continuidad del Negocio" fue hecho por Ron Ginn en 1986,

después de haber investigado el tema en los EE.UU. y de haber entrevistado a muchos destacados profesionales. Él escribió un libro titulado "Planificación de la Continuidad", que sugiere la aplicación de un conjunto de habilidades de DRP a un rango más amplio de riesgos de negocio e interrupciones operativas potenciales [3].Uno de los problemas iníciales fue la dificultad de convencer a la Alta Dirección de la justificación para hacer una importante inversión en algo que probablemente nunca iba a suceder. Esto llevó al concepto de Análisis de Impacto en el Negocio (BIA) para añadir más atención a los procesos de negocio [3]. En 1994 se fundó el BCI, como un grupo de trabajo encargado de definir el conjunto de habilidades para medir y juzgar la capacidad de aquellos que buscaban el reconocimiento como profesionales de continuidad del negocio [3].

En el 2003 el British Standard Institute (BSI) publicó la Guía para la Gestión de Continuidad del Negocio PAS56, que muestra las mejores prácticas en gestión de continuidad del negocio y que fue adoptado por muchas organizaciones alrededor del mundo [1]. En el 2006 PAS56 fue remplazada por el estándar británico BS 25999-1: Código de Prácticas, donde se establece el modelo para la gestión de continuidad del negocio; y en 2007 el BSI publicó la especificación para que las organizaciones puedan certificarse, llamada BS 25999-2 [1].

En algunos países se están implementando normas específicas sobre la gestión de la continuidad del negocio, como es el caso del Perú, en el cual la Superintendencia de Banca, Seguros y Asociación de Fondo de Pensiones (SBS), mediante Circular N° G-139-2009, aprueba las normas sobre gestión de la continuidad del negocio de manera obligatoria para las empresas del sector financiero [4].

Respecto de la gestión de continuidad del negocio se han desarrollado modelos derivados del estándar BS 25999, tales como el Modelo de Buenas Prácticas de implementación de Sharp [1], y el modelo para la implementación de prácticas globales de Gestión de Continuidad del Negocio [3]. Asimismo se han generado aquellos modelos orientados a un tipo de respuesta específico como el NIST[1] 800-34 Planeamiento de Contingencia para Sistemas de Información Federales – para la recuperación de desastres [5] –, el NFPA[2] 1600 Gestión de Emergencias y Desastres y Programas de Continuidad del Negocio – para la gestión de emergencias [6] –, el Modelo para el Planeamiento de Gestión de Crisis e Incidentes [7], o el Modelo de Madurez de Continuidad del Negocio [8]. En mayo de este año el estándar británico ha sido actualizado a través del estándar ISO 22301 Sociedad de Seguridad – Requerimientos para un Sistema de Gestión de Continuidad del Negocio [9], el cual brinda un mayor énfasis en la definición de los objetivos, el seguimiento, el rendimiento y la métrica; más claras expectativas sobre la gestión, y mejor y más cuidadosa planificación y preparación de los recursos necesarios para garantizar la continuidad del negocio [10].

Debido a que existen varios esfuerzos orientados a establecer un modelo para la gestión de la continuidad del negocio desde diferentes aspectos (organizacional, tecnológico, crisis, incidentes, emergencia) y que todos ellos son relevantes para las realidades en las cuales fueron creadas y han sido aplicadas (Reino Unido, EE.UU.), se hace necesario realizar la revisión detallada de dichos modelos y establecer sus puntos de convergencia y divergencia, así como las fortalezas de cada uno.

El artículo está organizado en cinco secciones: en la sección 2 se explica el marco teórico, en la sección 3 se

1 National Institute of Standards and Technology
2 National Fire Protection Association

realiza una breve revisión de los esfuerzos realizados sobre la continuidad del negocio desde sus orígenes, en la sección 4 se describen los modelos de gestión de continuidad del negocio más recientes, y finalmente en la sección 5 se tienen las conclusiones de la revisión.

2. MARCO TEÒRICO

2.1 Riesgo Operacional

El riesgo es la condición en la que existe la posibilidad de que un evento ocurra e impacte negativamente sobre los objetivos de la empresa [11].

La Gestión Integral de Riesgos es un proceso, efectuado por el Directorio, la Gerencia y el personal aplicado en toda la empresa y en la definición de su estrategia, diseñado para identificar potenciales eventos que pueden afectarla, gestionarlos de acuerdo a su apetito por el riesgo y proveer una seguridad razonable en el logro de sus objetivos [11].

Los riesgos pueden surgir por diversas fuentes, internas o externas, y pueden agruparse en diversas categorías o tipos como son: riesgo de crédito, estratégico, de liquidez, de mercado, operacional, de seguro, de reputación [11].

En el Acuerdo de Basilea II, emitido en el 2004 por el Comité de Basilea con el objetivo de establecer un marco que fortaleciera en mayor medida la solidez y estabilidad del sistema bancario internacional, se norma por primera vez el concepto de riesgo operacional, definido como el "riesgo de sufrir pérdidas debido a la inadecuación o a fallos de los procesos, el personal y los sistemas internos o bien a causa de acontecimientos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación" [12].

Los eventos de pérdida por riesgo operacional pueden ser agrupados de la siguiente manera: Fraude interno, Fraude externo, Relaciones laborales y seguridad en el puesto de trabajo, Clientes, productos y prácticas empresariales, Daños a activos materiales, Interrupción del negocio y fallos en los sistemas, y Ejecución, entrega y gestión de procesos [13].

2.2 Continuidad del Negocio

Es la capacidad estratégica y táctica de la organización para la planeación y respuesta a incidentes e interrupciones del negocio para continuar las operaciones del negocio a un nivel predefinido aceptable [14].

La Gestión de la Continuidad del Negocio – GCN, que forma parte de una adecuada gestión del riesgo operacional, es un proceso, efectuado por el Directorio, la Gerencia y el personal, que implementa respuestas efectivas para que la operatividad del negocio de la empresa continúe de una manera razonable, con el fin de salvaguardar los intereses de sus principales grupos de interés, ante la ocurrencia de eventos que pueden crear una interrupción o inestabilidad en las operaciones de la empresa [15].

Establece un marco de referencia estratégico y operacional para implementar proactivamente una resistencia organizacional ante la interrupción o la pérdida en la entrega de productos y servicios [16]. No deberían ser sólo medidas reactivas tomadas luego de un incidente que ha ocurrido. La GCN requiere el planeamiento a lo largo de muchas áreas de la organización, y su resistencia depende de manera equitativa de su personal administrativo y operacional, tanto como de la tecnología y el establecimiento de un programa de GCN [17].

Debido a que el riesgo operacional considera eventos de Interrupción del negocio y fallos en los sistemas, definido como pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas, la continuidad del negocio es parte de la gestión del riesgo operacional [12].

3. REVISIÒN DE LA LITERATURA

El primer uso conocido del término "Continuidad del Negocio" fue hecho por Ron Ginn (posteriormente Presidente del Instituto de Continuidad del Negocio - BCI) en 1986, después de haber investigado el tema en Estados Unidos y de haber entrevistado a muchos destacados profesionales. Él escribió un libro titulado "Planificación de la Continuidad", que sugiere la aplicación de un conjunto de habilidades de DRP a un rango más amplio de riesgos de negocio e interrupciones operativas potenciales [3].

El Concejo de Estándares NFPA, de Estados Unidos, estableció el Comité de Gestión de Desastres en enero de 1991, con la responsabilidad de desarrollar documentos relacionados a la preparación, respuesta, y recuperaciónde desastres resultados de eventos naturales, humanos o tecnológicos [6].

En 1994 se fundó en el Reino Unido el Instituto de Continuidad del Negocio (Business Continuity Institute –

BCI), como un grupo de trabajo encargado de definir el conjunto de habilidades para medir y juzgar la capacidad de aquellos que buscaban el reconocimiento como profesionales de continuidad del negocio, las cuales se desarrollaron en un esfuerzo cooperativo con el Instituto de Recuperación de Desastres (ahora DRII) [3].

En 1995 se realiza el lanzamiento de la Norma Británica para la Seguridad de Información BS 7799 y su posterior versión americana ISO/IEC 17799 Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. Esto incluye en sus principios básicos la necesidad de la GCN, que se define en términos de disponibilidad de datos. Esto añadió más confusión al debate y dio lugar a que muchos profesionales de TI afirmaran que la GCN era simplemente un subconjunto de seguridad de la información [3]. Ese año también se lanza el NFPA 1600 Prácticas recomendadas para la Gestión de Desastres, presentado en la Reunión Anual de los miembros en Estados Unidos [6].

Knight y Pretty de Templeton College, Oxford, realizaron una investigación en fines de los 90's que mostró que la falta de confianza en la habilidad de los directores para actuar rápida y profesionalmente en el momento de un desastre lleva a la reducción del valor de las acciones. La GCN efectiva integra la gestión de crisis/incidentes para asegurar que si un incidente mayor ocurre, la organización no está solo preparada para mantener la continuidad de sus operaciones, sino para asegurar a la comunidad que todo está bajo control [18].

En el 2000 el comité de NFPA incorpora en el NFPA 1600 la aproximación a la gestión de desastres/emergencias y programas de continuidad del negocio [6]. En el 2003 el BSI publicó la Especificación Disponible al Público PAS56 Guía para la Gestión de Continuidad del Negocio, que muestra las mejores prácticas en GCN, que fue adoptado por muchas organizaciones alrededor del mundo [17].

En el 2004 el comité NFPA actualizó la terminología y el formato del NFPA 1600 de acuerdo al Manual de Estilo para los documentos técnicos del NFPA emitido en el 2003 [6].

En el 2006 PAS56 fue remplazada por un nuevo estándar británico para la GCN: BS 25999-1. Este es un código de prácticas para la GCN e incorpora las mejores prácticas de PAS56, las guías de GCN que soporta el Acta de Contingencias Civiles del Reino Unido del 2004 [19] y otros recursos de todo el mundo [1]. En el 2007 el BSI publicó la segunda parte del nuevo estándar que es una especificación de GCN para las organizaciones que desean certificarse: BS 25999-2, Gestión de Continuidad del Negocio Parte 2 – Especificación [1]. Este último se basa en el ciclo de la ISO 9000 "Planear-Hacer-Verificar-Actuar" (Plan-Do-Check-Act – PDCA) [20], estableciéndose como el ciclo de vida de la continuidad del negocio las fases de: entendimiento de la organización, determinación de la estrategia, desarrollo e implementación de la respuesta, ejercicio, mantenimiento y revisión, y forjamiento de la cultura organizacional de continuidad del negocio [21]. El mismo año se actualiza el NFPA 1600, identificando la prevención como un aspecto adicional a la mitigación, preparación, respuesta y recuperación, identificado en versiones anteriores. Así mismo, reconoce la colaboración del Departamento de Seguridad interna de los Estados Unidos (DHS), IAEM[3] y NEMA[4] [22].

En el 2008, John Sharp, auspiciado por el BCI, elabora un libro para la implementación de la BS 25999-2, indicando lineamientos más específicos, casos y plantillas del cómo y quiénes implementan el SGCN [1].

En el 2010 se lanza la actualización de la norma NFPA 1600 de Gestión de Emergencias y Desastres y Programas de Continuidad del Negocio, alineada al ciclo PDCA. El capítulo Gestión del Programa fue expandido para enfatizar la importancia del liderazgo y el compromiso, incluyendo nuevos requerimientos para definir los objetivos de desempeño y gestión de registros. Se conforman otros cuatro capítulos de Planeación, Implementación, Pruebas y Ejercicios, y Mejora del Programa. El análisis de impacto al negocio y la evaluación de riesgos ahora están separados. En el capítulo de implementación se incluye una sección de asistencia al empleado y soporte [6]. Paralelamente, el NIST publica la Especificación Pública NIST 800-34 Rev. 1 Guía de Planificación de Contingencia para Sistemas de Información Federales, tomando en consideración los requerimientos del estándar FIPS 199 Categorización de Seguridad para Información Federal y Sistemas de Información [23], y de la publicación NIST 800-53 Controles de Seguridad recomendados para Sistemas

3 International Association of Emergency Managers
4 National Electrical Manufacturers Association

de Información y Organizaciones Federales [24]. Este estándar establece siete etapas del ciclo de vida del desarrollo del sistema de contingencias: desarrollo de la política, análisis de impacto al negocio, identificación de controles preventivos, creación de estrategias de contingencia, desarrollo de planes de contingencia, pruebas, entrenamiento y ejercicio del plan, y mantenimiento del plan [5].

En el 2011 la empresa Virtual Corporation publica la segunda versión del Modelo de Madurez de Continuidad del Negocio (Business Continuity Maturity Model – BCMM), publicado originalmente en 2003 para dirigir a la organización a que sean capaces de evaluar y mejorar su programa de continuidad del negocio, como un mecanismo de medición de la efectividad del mismo [8]. Ese mismo año Roberta Witty establece los componentes principales de un programa efectivo de gestión de crisis e incidentes, los cuales son: marco de referencia, equipo de gestión de crisis/incidentes, centro de operaciones de comando/emergencia, software de GCN, y ejercitación de los procedimientos de gestión de crisis [7].

En mayo de este año se publica la norma ISO/IEC 22301 Sociedad de Seguridad – Sistema de Gestión de Continuidad del Negocio – Requerimientos, en reemplazo de la BS 25999-2, que manteniendo el ciclo de vida del SGCN y alineado al modelo PDCA establece nuevas consideraciones y mejoras respecto a su predecesor. Esta norma es certificable [9]. Finalmente como complemento, John Sharp actualiza su libro de Mapa de Ruta, alineado en esta oportunidad a la ISO 22301 [25].

4. REVISIÒN DE MODELOS

4.1 Modelo Británico BS-25999 Sistema de Gestión de Continuidad del Negocio

El estándar creado por el Instituto Británico de Estandarización en el 2007 para la gestión de continuidad del negocio consiste en dos partes [1]:

BS 25999-1, Gestión de Continuidad del Negocio Parte 1 - Código de Prácticas [21]. Este documento toma la forma de guía de buenas prácticas y recomendaciones, indicando qué prácticas debe emprender la organización para implementar la GCN efectivamente. Las organizaciones deben escoger si siguen todo o parte del código de práctica. En ella se toma como referencias las normas ISO 9000 [20], ISO 20000 [26], ISO 27001 [14] y PAS77 [27].

BS 25999-2, Gestión de Continuidad del Negocio Parte 2 – Especificación [28]. Este documento indica lo que la organización debe hacer para implementar la GCN. Esto es para el uso de partes internas y externas, incluyendo organizaciones de certificación, para evaluar la habilidad de las organizaciones de cumplir con los requerimientos regulatorios y de clientes, y sus propios requerimientos. Contiene sólo requerimientos que pueden ser auditados objetivamente y la demostración de una implementación exitosa puede ser usada para asegurar a las partes interesadas que se cuenta con un Sistema de Gestión de Continuidad del Negocio – SGCN [1].

Este modelo establece el ciclo de vida de la GCN como un ciclo repetitivo y constante que se muestra en la Figura 1:

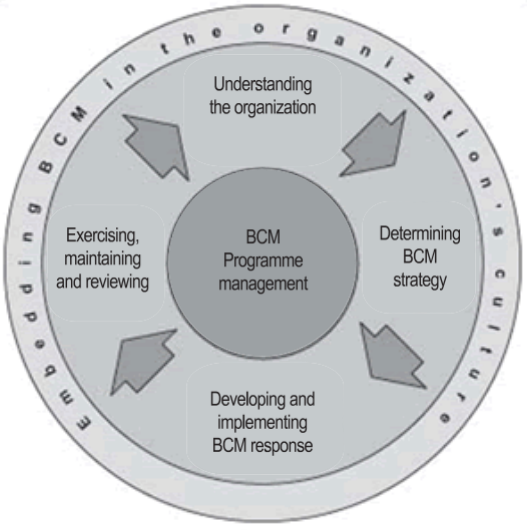


Fig. 1. Ciclo de Vida de la GCN [28].

A continuación se describen los componentes del ciclo de vida de la GCN:

4.1.1 Gestión del Programa de la GCN

Una gestión efectiva del programa establece la aproximación de la organización a la continuidad del negocio. La participación de la alta dirección es clave para asegurar que el proceso de GCN es correctamente introducido, adecuadamente soportado y establecido como parte de la cultura de la organización.

4.1.2 Entendimiento de la organización

Esta fase está constituida por:

Análisis de Impacto en el Negocio (Business Impact Analysis-BIA): determinar el impacto que pueda provocar las posibles interrupciones. Debe incluir:

- Actividades críticas para dar soporte a los procesos de negocio.
- Impacto que produce la interrupción de dichas actividades.
- Periodo Máximo Tolerable de Interrupción para cada actividad (tiempo máximo que la organización puede soportar sin que sus productos o servicios sufran un daño grave)
- Identificación de dependencias entre actividades.
- Identificación de proveedores de actividades críticas.
- Tiempo Objetivos de Recuperación para cada actividad, dentro del límite del Periodo Máximo Tolerable de Interrupción.

Evaluación de riesgos: para evaluar la probabilidad de ocurrencia de las posibles interrupciones identificadas en el BIA.

4.1.3 Determinación de la estrategia de continuidad del negocio

Deben definirse los procesos a seguir para que la organización recupere el funcionamiento de sus actividades críticas en un plazo de tiempo razonable, y que en la medida de lo posible no afecte a su suministro de productos o servicios. Se establece cuatro elementos:

- Desarrollo y documentación de una estructura de respuesta a incidentes.
- Determinar cómo la organización recuperará cada actividad crítica según el Tiempo Objetivo de Recuperación (Recovery Time Objective – RTO) y los recursos requeridos.
- Determinar cómo la relación con los interesados será administrada durante el tiempo de interrupción.
- Tener en cuenta las actividades no definidas como críticas.

4.1.4 Desarrollo e implementación de la respuesta de continuidad del negocio

- Estructurar la respuesta a incidentes: secuencia de operaciones a realizar una vez ocurrido un incidente.
- Desarrollo de los Planes de GCN: recuperación de las actividades interrumpidas.
- Desarrollo de los Planes de Gestión de Incidentes.

4.1.5 rcicios, mantenimiento y revisión

- Realización de ejercicios para validar los planes y procedimientos desarrollados, así como realizar su revisión y mantenimiento de forma periódica y en intervalos definidos.
- Acciones correctivas y preventivas como método para canalizar la mejora continua del sistema de gestión de la continuidad del negocio.

El estándar brinda una estructura para la generación de las diferentes etapas de la gestión de la continuidad del negocio, y es bajo este estándar que se desarrolló la circular SBS N° G-139 de continuidad del negocio, y que no indica el cómo desarrollar cada etapa. Si bien es cierto a nivel del estándar británico se complementa con la BS 25999-1, para su aplicación a la realidad del sector financiero se requiere de una mayor especificación, debido a la alta regulación de este sector y su enfoque por líneas de negocio según lo establecido en Basilea II.

4.2 Modelo de buenas prácticas para la implementación de los requerimientos de la BS 25999

John Sharp, alineado a la BS 25999, define las prácticas para implementar la gestión de continuidad del negocio [1], las cuales se muestran a continuación:

4.2.1 Entendimiento de la organización

Se define el proceso para determinar las actividades críticas que permitan a la organización cumplir con su misión, visión y objetivos de alto nivel, identificando productos y servicios claves, procesos, terceras partes, según se muestra en la Figura 2:

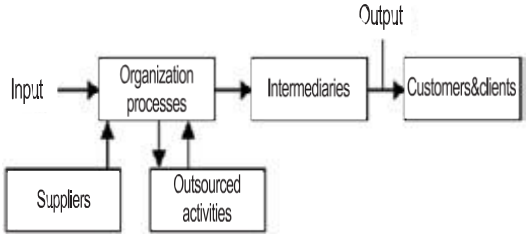


Fig. 2. La vista de entrega de extremo-a-extremo [1].

Las medidas de impacto pueden ser: pérdida financiera, impacto en la entrega del servicio, pérdida de reputación, amenaza a la seguridad del personal, infracción a la privacidad personal, falla en el cumplimiento de obligaciones regulatorias, y efecto en los objetivos de proyectos y cronogramas.

4.2.2 Determinación de las estrategias de continuidad de negocio

- Estructura de respuesta de incidentes (Incident Response Structure - IRS). El autor define cuatro elementos clave para un buen IRS: Evaluación de la situación, Activación del IRS, Capacidad de comunicación, y Proceso de toma de decisiones. El procedimiento tiene que ser apropiado para el tamaño y naturaleza de la organización y establecer las bases cuando ha ocurrido una interrupción, definiendo qué planes deben ser activados. La línea del tiempo para la respuesta se muestra en la Figura 3, que indica una implementación secuencial de los planes de incidentes, continuidad y recuperación, sin embargo, en algunos casos, los planes deben ser implementados en una sucesión rápida o simultáneamente.

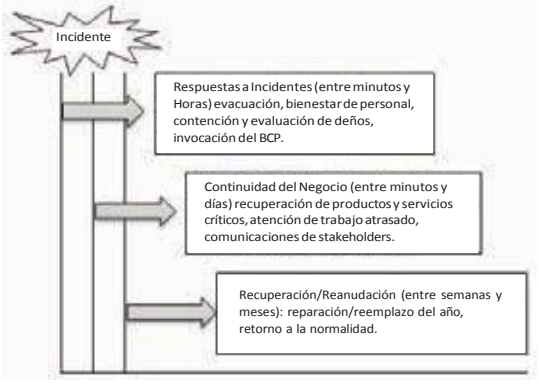


Fig. 3. Línea de Tiempo de Respuesta a Incidentes [1].

- Estrategias clave de recursos

• Personas: para mantener las habilidades y conocimiento se debe documentar cómo se desarrollan las actividades, entrenar al personal y proveedores, realizar separación de funciones y establecer un plan de sucesión.

• Locales: contar con locales alternativos que incluyan el desplazamiento de las actividades, locales alternativos provistos por otras organizaciones, provistos por especialistas o terceros, trabajo remoto y uso de fuerza de trabajo alternativo.

• Tecnología: dispersión geográfica de la tecnología (mantener la misma tecnología en diferentes locales), mantener equipamiento antiguo como reemplazo en una emergencia. Tener en cuenta los RTO, la distancia entre locales, el acceso remoto, la conectividad redundante y la naturaleza de la falla.

• Información: respaldo en un local seguro de manera física o virtual; teniendo en cuenta el punto de recuperación en el tiempo acordado con la alta dirección.

• Proveedores: acuerdos de entrega de stock en corto tiempo, proveedores alternativos, trasferencia de operaciones, acuerdos de niveles de servicio.

4.2.3 Desarrollo e implementación de una respuesta de GCN

El autor establece como contenido mínimo de los planes: propósito y alcance, roles y responsabilidades, invocación del plan, locales alternativos, planes de recuperación del sistema, detalles del contacto, prioridades, documentos y recursos vitales, listas de verificación y registros de auditoria, necesidades del personal, perfil público, retorno de la normalidad. Asimismo presenta el alcance que debe ser considerado para implementar las respuestas de GCN, el cual se muestra en la Figura 4:

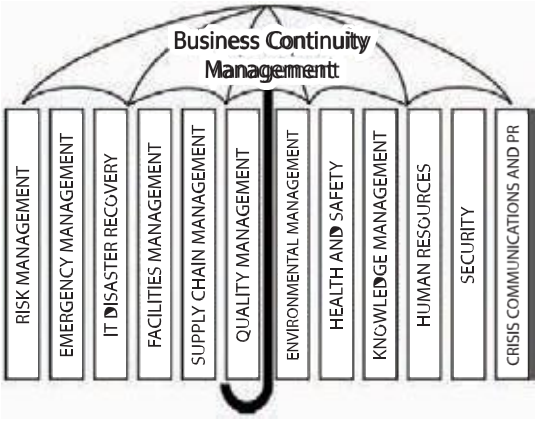


Fig. 4. Alcance del proceso de planeamiento [1].

4.2.4 Pruebas y mantenimiento

Se debe establecer un programa de pruebas y documentarlo. El autor propone un proceso para las pruebas como se indica en la Figura 5:

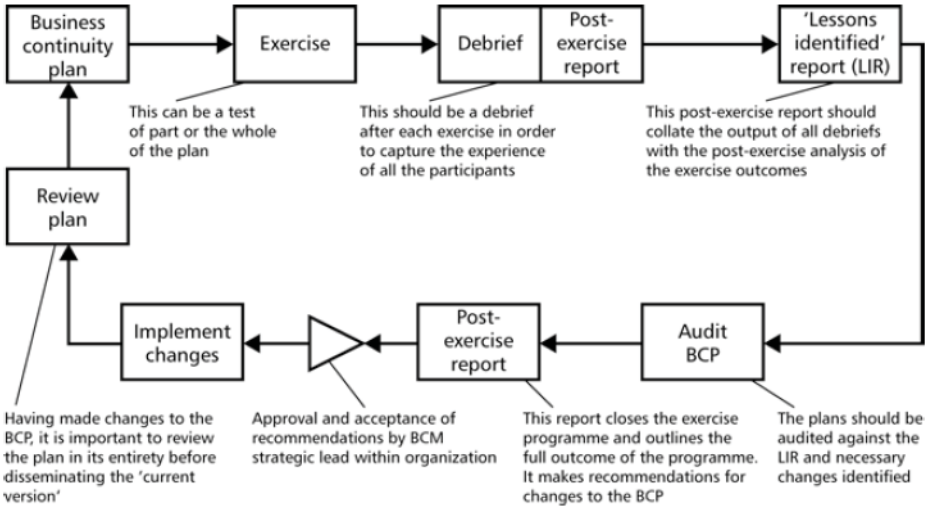


Fig. 5. El ciclo de ejercicio de la continuidad del negocio [1]

El autor muestra de manera más detallada lo que está estipulado en las normas BS 25999, pero de manera similar a su antecesor, el enfoque brindado es por procesos. Asimismo el autor continúa con la línea del estándar al abarcar cualquier tipo de empresa, siendo el sector de estudio motivo de la tesis el sector financiero peruano, el cual requiere de métodos y controles más enfocados.

4.3 Modelo NFPA 1600 Gestión de Emergencias y Desastres y Programas de Continuidad del Negocio

Este modelo brinda una herramienta para la autoevaluación de la NFPA 1600, de acuerdo al ciclo establecido para la Gestión de Emergencias/Desastres y Programas de Continuidad del Negocio que se muestra en la Figura 6:

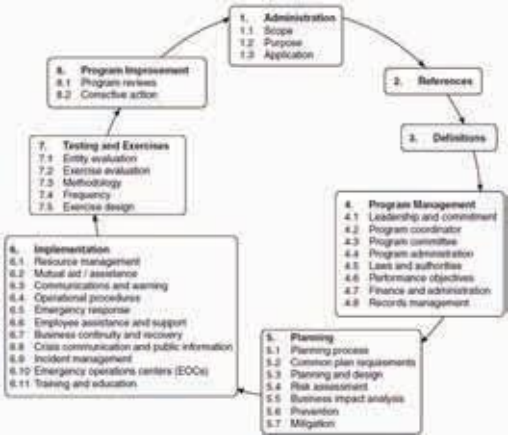


Fig. 6. Ciclo Planear-Hacer-Verificar-Actuar [6].

Este modelo se desarrolla en una lista de verificación resultado de la comparación con los modelos CSA Z1600-08 Gestión de Emergencias y Programas de Continuidad del Negocio [29] y las Prácticas Profesionales para los Profesionales de Continuidad del Negocio del DRII [30]. También toma como referencias las guías de gestión de recursos en emergencias de la ASTM E2640-10 [31]. Las fases del ciclo se especifican a continuación:

4.3.1 Gestión del Programa

- El compromiso de la dirección incluye políticas, planes, procedimientos, recursos, revisiones y evaluaciones, y correcciones.
- Se ha determinado un Coordinador del Programa para desarrollar, implementar, administrar, evaluar y mantener el programa.
- La documentación del programa consta de política, misión, visión, roles y responsabilidades, autoridades, alcance, metas, objetivos, método de evaluación, presupuesto y cronograma.
- Los objetivos de desempeño dependen de los resultados de la identificación de amenazas, la evaluación de riesgos, y el análisis de impacto al negocio.
- Se cuentan con procedimientos financieros, administrativos y de gestión de crisis para soportar el programa antes, durante y después del incidente.
- Se gestionan los registros: clasificación, confidencialidad e integridad, retención, almacenamiento,

archivo, destrucción, control de accesos y control de documentación.

4.3.2 Planificación

- El programa sigue un proceso de planificación que desarrolle la estrategia, gestión de crisis, prevención, mitigación, operación y respuesta a emergencias, planes de continuidad y de recuperación.
- Los planes identifican roles funcionales y responsabilidades, líneas de autoridad y sucesión, delegación de autoridad, soporte logístico y recursos, seguridad y salud de personal.
- La organización evalúa riesgos para identificar estrategias de prevención y mitigación y reúne información para desarrollar planes de respuesta, continuidad y recuperación.
- La entidad identifica amenazas y las monitorea. Se lleva a cabo un análisis de impacto respecto a la salud y seguridad de las personas, operaciones, activos, infraestructura, proveedores, servicios, ambiente, condición económica y financiera.
- El BIA identifica los procesos críticos y el punto en el tiempo cuando la interrupción se vuelve inaceptable. Se incluye la potencial pérdida de información en el tiempo.
- Se desarrolla una estrategia de prevención de incidentes que puedan amenazar la vida, propiedad y ambiente; y una estrategia de mitigación y medición para limitar o controlar las consecuencias.

4.3.3 Implementación

- La entidad conduce las necesidades de gestión de recursos basados en la identificación de amenazas, que debe incluir: recursos humanos, equipo, entrenamiento, herramientas, conocimiento experto, materiales, tecnología e información. Considera cantidad, tiempo de respuesta, capacidad, limitaciones, costo y responsabilidad cuando se utilizan los recursos.
- Se cuenta con procedimientos para localizar, adquirir, almacenar, distribuir, mantener, probar los recursos.
- Las comunicaciones y sistemas de alerta deben ser confiables, redundantes e inter-operativos.
- Se desarrolla procedimientos operacionales para soportar el programa, los cuales deben responder a las amenazas identificadas.
- Se cuenta con un centro de operaciones de emergencia y se cuenta con su procedimiento de activación, con planes de emergencia para proteger a las personas, con procedimientos de contacto, comunicación, desplazamiento y atención de empleados.
- Se han identificado dentro de los planes de continuidad: los stakeholders que necesitan ser notificados, las aplicaciones críticas, registros vitales, listas de contacto, procesos y funciones a mantener, personal, procedimientos y recursos para la recuperación.

4.3.4 Pruebas y Ejercicios

La entidad evalúa los planes, procedimientos y capacidades periódicamente a través de pruebas y ejercicios. Los ejercicios siguen una metodología estandarizada y se llevan a cabo con la frecuencia necesaria para mantener las capacidades, identificar deficiencias, validar cambios, esclarecer roles, obtener retroalimentación de los participantes y medir la mejora.

4.3.5 Mejoramiento del programa

Se mejora la efectividad del programa a través de la revisión de la gestión de las políticas, objetivos de desempeño, evaluación de la implementación del programa, y cambios resultados de las acciones correctivas y preventivas.

El presente modelo pone un mayor énfasis respecto a la gestión del programa y la planificación del mismo, y brinda una mayor especificación respecto a la gestión de la emergencia, que es una parte de un sistema de gestión de continuidad del negocio. Como tiene una estructura similar a otros modelos de gestión de continuidad del negocio, es posible usar el mismo para complementar con mayor detalle los planes de emergencia. Sin embargo, dado su punto de vista, hace referencia a la evaluación de riesgos con más significancia e incluso de manera precedente al análisis de impacto al negocio, puesto que al estar más enfocado en la emergencia, no busca una continuidad de procesos en sí, sino de la salvaguarda de personas y en el manejo de heridos, crisis, comunicaciones y recursos.

4.4 Modelo NIST Publicación Especial 800-34 Planeamiento de Contingencia para Sistemas de Información Federales

Este modelo ha sido desarrollado de manera alineada a los requerimientos del estándar FIPS[1] 199 Categorización de Seguridad para Información Federal y Sistemas de Información [23], tomando como referencia diferentes lineamientos del gobierno estadounidense, entre ellos la publicación NIST 800-53 Controles de Seguridad recomendados para Sistemas de Información y Organizaciones Federales [24], y otros [32] [33] [34] [35], estableciendo las siguientes etapas del ciclo de vida del desarrollo de un sistema de contingencia:

4.4.1 Desarrollar la política del plan de contingencia

Debe definir los objetivos globales de contingencia de la organización y establecer el marco de referencia y responsabilidades organizacionales para el planeamiento de sistemas de contingencia.

4.4.2 Llevar a cabo el BIA

Su objetivo es correlacionar los sistemas con los procesos críticos del negocio y servicios entregados, y con base a esa información, caracterizar las consecuencias de una interrupción, determinar los requerimientos del plan de contingencia y las prioridades de recuperación.

4.4.3 Identificar controles preventivos

En algunos casos los impactos del BIA deben ser mitigados o eliminados a través de controles preventivos que impidan, detecten o reduzcan el impacto en los sistemas. Donde es posible y efectivo en costos, los controles preventivos son preferibles, tal como grupos electrógenos, sistemas de aire acondicionado, sistemas anti incendios, detectores de humedad, entre otros.

4.4.4 Crear estrategias de contingencia

Las estrategias de contingencia son creadas para mitigar los riesgos, teniendo en cuenta respaldo y recuperación, almacenamiento externo, sitios alternos, remplazo de equipos, y consideraciones de costo.

4.4.5 Pruebas, entrenamiento y ejercicios del plan

Un plan de contingencia debe mantenerse en un estado de preparación, que incluye personal entrenado para asumir sus roles, y teniendo los sistemas y componentes de sistemas probados para asegurar su operatividad en el ambiente especificado en el plan [34].

4.4.6 Mantener el plan

Los sistemas de información están sometidos a cambios frecuentes debido a las necesidades del negocio, actualización de tecnología o nuevas políticas internas y externas. La revisión de los planesdeben enfocarse en los siguientes elementos: requerimientos operacionales, requerimientos de seguridad, procedimientos técnicos, información de contacto, tecnología, registros vitales o requerimientos alternos.

A través de este modelo los autores buscan ayudar a las organizaciones a entender el objetivo, proceso y formato para el desarrollo de un Plan de Contingencia de Sistemas de Información (Information System Contingency Plans – ISCPs) a través de guías prácticas y basadas en el mundo real. Mientras los principios establecen una línea base para conocer las necesidades de la mayoría de las organizaciones, es reconocido que cada organización puede tener requerimientos adicionales específicos a su propio ambiente operativo [5].

Deben considerarse varios enfoques alternativos cuando se desarrollan y comparan estrategias, incluyendo costos, tiempos de interrupción máximos, seguridad, prioridades de recuperación, e integración con planes de contingencia más amplios a nivel organizacional. Asimismo los autores muestran un resumen de criterios que pueden ser utilizados para determinar qué tipo de sitio alterno cubre las necesidades de la organización, considerando la seguridad del sistema, controles de administración y operativos compatibles con el prospecto de sitio alterno, firewalls, controles de acceso físico y requerimientos de seguridad de personal del grupo que soporta el sitio.

La Figura 7 identifica cinco componentes principales del plan de contingencia. La información de soporte y los anexos al plan proveen información esencial para asegurar un plan comprensible. Las fases de activación y notificación, recuperación y reconstrucción indican acciones específicas que la organización debe seguir frente a una interrupción del sistema o emergencia.

El modelo estudiado, al ser emitido cumpliendo con la ley Federal de Gestión de la Seguridad de Información

5 Federal Information Processing Standards

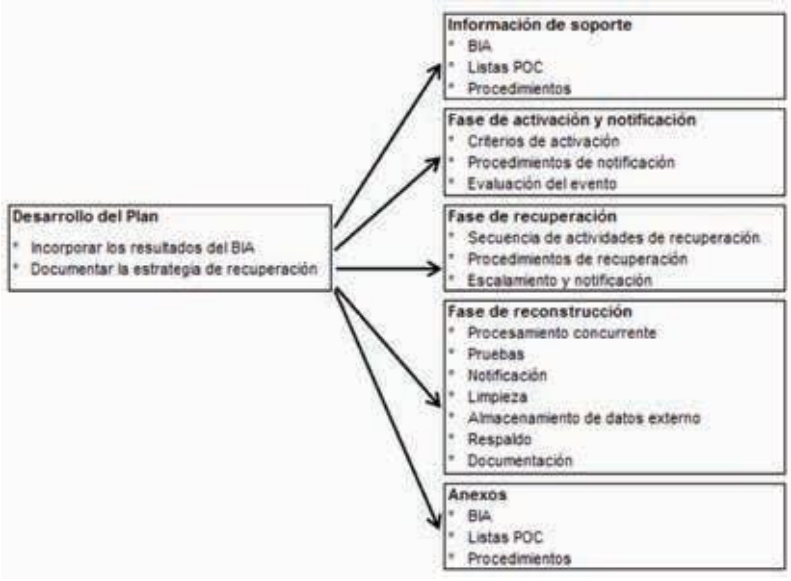


Fig. 7. Estructura del Plan de Contingencia [5].

(Federal Information Security Management Act – FISMA) emitida en el 2002 [36], el contenido del mismo se centraliza en la gestión de la información y tecnologías de información y comunicaciones y la generación de planes de contingencia y de gestión de incidentes tecnológicos, los cuales pueden complementar un modelo de gestión de continuidad empresarial, pero por sí solo. Resalta que a pesar de que no se evidencia en su contenido alguna referencia al estándar BS 25999, sus etapas son similares, lo cual favorece a su acoplamiento.

4.5 Modelo para la implementación de prácticas globales de Gestión de Continuidad del Negocio

Lyndon Bird, a través del BCI, establece una guía que cubre las seis fases de la GCN pero lo relaciona directamente a lo que ahora se define como Prácticas Profesionales (PP). Las seis PPs están subdivididas en dos Prácticas de Gestión y cuatro Prácticas Técnicas [3]:

4.5.1. Prácticas de Gestión

Políticas y Gestión del Programa

- Alineando la Política de GCN en la cultura de la organización: un programa de GCN necesita reflejar la estrategia, objetivos y cultura de la organización, para asegurar que el programa es relevante, efectivo y apropiado.
- Alcance del programa de GCN y selección de alternativas: definir qué productos y servicios se consideran dentro del programa y los criterios claves de éxito para su entrega. Asimismo la localización limita el alcance, incluye o excluye algunos sitios o locales. Si un producto o servicio se considera dentro del alcance, entonces todas las actividades que soportan su entrega deben ser incluidas en el programa. Las alternativas definen cómo la organización pretende proteger o no su habilidad para mantener la entrega.
- Desarrollar la política de GCN: el objetivo es comunicar a los stakeholders los principios de continuidad a los que la organización aspira, la cual debe ser corta, clara, precisa e ir al punto. Debe contener los objetivos, alcance, responsabilidades, métodos y estándares.
- Gestión del programa de GCN: los elementos clave son:
  - Asignación de responsabilidades: designar un responsable de la gestión y asignar un comité de apoyo, equipos de continuidad y de respuesta a incidentes.
  - Implementación de la GCN en la organización: procesos de iniciación, planeamiento, coordinación e implementación de los proyectos de GCN por cada fase.

- Gestión de proyecto: identificar proyectos requeridos para completar una implementación inicial del ciclo de vida de GCN.
- Gestión de continuidad del negocio en curso.
- Documentación de la GCN.

Integración de la GCN en la cultura de la organización

Tener un SGCN asegura que la organización pueda gestionar el programa eficientemente, se genera confianza de los stakeholders, incrementa la capacidad de respuesta a nivel táctico y estratégico, minimiza el impacto de interrupciones. El proceso es una iteración constante de:

- La evaluación de la actual cultura organizacional.
- Comprensión de a dónde quiere ir la organización.
- Evaluación e identificación de las diferencias entre ambas.

4.5.2 Prácticas Técnicas

Entendimiento de la organización

- Análisis de Impacto al Negocio (BIA): identifica, cuantifica y califica los impactos en el tiempo de una pérdida, interrupción o perturbación de las actividades de negocios en una organización a nivel estratégico, táctico y operativo; y proporciona los datos a partir de los cuales se pueden determinar estrategias de continuidad adecuadas. La decisión de qué productos y servicios están contenidos en el alcance del programa de GCN se realiza antes del BIA, y debe estar documentado en la política de GCN. Se debe determinar el Período Máximo Tolerable de Interrupción (MTPD), que es la duración después de que la viabilidad de una organización será irreparablemente dañada si la entrega no se puede reanudar.
- Análisis de requerimientos de continuidad: proveer la información de los recursos que permita determinar o recomendar estrategias adecuadas de recuperación, teniendo en cuenta que no siempre se requieren menos recursos durante las primeras horas, incluso en ocasiones se requiere más recursos de lo normal. Se debe determinar la pérdida máxima de datos aceptable, ya que la antigüedad de la data puede generar que la recuperación sea imposible.
- Evaluación de amenazas a través de evaluación de riesgos: identificar medidas que pueden ser implementadas para reducir la probabilidad de una interrupción de las actividades críticas de la organización. Los pasos clave son:
  - Hacer una lista de las amenazas conocidas que pudieran causar interrupción.
  - Determinar la evaluación del riesgo con base a su probabilidad e impacto.
  - Dar prioridad a las amenazas de mayor nivel e identificar áreas de riesgos inaceptables.
  - Recomendar las acciones que se pueden tomar para reducir la amenaza.

Determinación de estrategias de continuidad del negocio

- Identificar y seleccionar estrategias
  - Identificar el MTPD, y definir el RTO.
  - Si existen estrategias identificadas, realizar un análisis de brechas.
  - Identificar estrategias adecuadas que habilitarán el cumplimiento del RTO.
  - Analizar las estrategias por efectividad y costo.
  - Presentar a la alta dirección con recomendaciones.
- Identificar y seleccionar respuestas tácticas
  - Determinar el RTO y el RPO (Punto Objetivo de Recuperación) por cada actividad.
  - Identificar opciones tácticas por cada actividad.
  - Analizar las opciones por efectividad y costo.

Desarrollar e implementar las respuestas de GCN

Aunque el término Plan de Continuidad del Negocio (BCP) implica sólo un documento, en realidad cubre diferentes actividades que consiste usualmente en múltiples planes. El BCP puede existir en cualquier nivel organizacional y puede llevarse a nivel de detalle procedural. Hay cinco tipos de planes correspondientes a cinco etapas de respuesta, que son:

- Respuesta a la emergencia: como un plan de evacuación.
- Gestión de incidente: Plan de Comunicación de Crisis.

- Continuidad: respuesta inicial del negocio para asegurar que las actividades principales pueden continuar operando a un nivel mínimo aceptable.
- Recuperación: recuperar actividades a un nivel sostenible.
- Reanudación: reanudar operaciones a nivel normal.

Probar, Mantener y Revisar el SGCN

La capacidad del SGCN no puede ser considerada confiable hasta que sea probada. Esto verificará el trabajo adecuado de los equipos, procedimientos correctos, integración de procedimientos, cumplimiento del RTO y la capacidad del personal. Los tipos de pruebas son: de escritorio, simulación, unidad de prueba, unidad de ensayo, prueba punto a punto y ensayo total.

4.6 Modelo de Madurez de Continuidad del Negocio 2.0

El Modelo de Madurez de Continuidad del Negocio (Business Continuity Maturity Model – BCMM®) fue publicado originalmente en el 2003 por Virtual Corporation, para dirigir a la organización a que sean capaces de evaluar y mejorar su programa de continuidad del negocio, como un mecanismo de medición de la efectividad del mismo. Esta versión incorpora los requerimientos de BS 25999-1 [21] y 2 [28], NFPA 1600 [6] y ASIS SPC1 2009-1 [37], los cuales son evaluados a través de niveles de madurez, competencias corporativas y contenido del programa de continuidad del negocio (ver Figura 8):

4.6.1 Niveles de Madurez

Increasing Business Continuity Competency Maturity →

Maturity Model Levels	Level 1 Self-Governed	Level 2 Departmental	Level 3 Cooperative	Level 4 Standards Compliant	Level 5 Integrated	Level 6 Synergistic
Athlete Analogy	Able to Crawl	Able to Walk	Able to Run	"Fit" Runner"	Competitive Runner	Olympic Runner
Comparative Model	Organization "At Risk"		"Competent" Performer		"Best of Breed"	
Corporate Competencies	**Attributes of an Organization at Each Maturity Level**					
Leadership	VL	L	M	H	H	H
Employee Awareness	VL	L	L	M	H	H
BC Program Structure	VL	L	L	M	H	H
Program Pervasiveness	VL	VL	L	L	M	H
Metrics	VL	L	M	M	H	H
Resource Commitment	VL	L	M	H	H	H
External Coordination	VL	L	L	M	H	H
BC Program Content	**Attributes of Each BC Discipline at Each Maturity level**					
Incident Management	VL	L	M	H	H	H
Technology Recovery	VL	L	M	H	H	H
Business Recovery	VL	L	M	H	H	H
Security Management	VL	L	M	H	H	H

VL - Very Low L - Low M - Medium H - High

Fig. 8. Modelo de Madurez de Continuidad del Negocio [8].

- Nivel 1 Autogobernado: el estado de preparación es bajo y a través de la empresa, y reacciona a eventos de interrupción cuando ocurren.
- Nivel 2 Departamental: al menos una unidad de negocio o función corporativa ha iniciado esfuerzos para establecer conciencia de la importancia de la continuidad del negocio. El nivel de participación es bajo.
- Nivel 3 Cooperativo: las unidades participantes han instituido un programa de gobierno rudimentario, que cumplan con la limitada política de GCN. La alta dirección no ha comprometido a la empresa en el programa de GCN.
- Nivel 4 Cumplimiento de estándares: la alta dirección entiende y está comprometida con la importancia estratégica de un programa de GCN efectivo. Una política práctica y exigible y estándares asociados han sido adoptados, incluyendo métodos y herramientas para las cuatro disciplinas de continuidad. Se han identificado todas las funciones críticas y se han desarrollado los planes.
- Nivel 5 Integrado: todas las unidades han completado pruebas en todos los elementos de sus planes. Los métodos de actualización son efectivos. La alta dirección ha participado en los ejercicios de gestión de crisis. Un plan multianual se ha adoptado.

- Nivel 6 Sinergia: se han formulado y probado satisfactoriamente estrategias sofisticadas de protección del negocio. Los métodos de control de cambios y mejora continua de procesos mantienen a la organización en un nivel alto de preparación.

4.6.2 Competencias Corporativas

- Liderazgo: el compromiso y entendimiento demostrado por la alta dirección para asegurar la implementación apropiada del programa.
- Conciencia de empleados: la amplitud y profundidad del conocimiento y conciencia de la continuidad a través de todos los niveles incluyendo la consideración para la calidad y sostenibilidad del programa de concientización y entrenamiento.
- Estructura del programa de continuidad del negocio: la escala y oportunidad del programa implementado a través de la empresa, el grado de articulación con los casos de negocio.
- Penetración del programa: el nivel de coordinación entre departamentos, funciones y unidades de negocio. El grado en el cual las consideraciones de continuidad se han incorporado en iniciativas propias del negocio.
- Métricas: desarrollo y monitoreo de medidas apropiadas del desempeño del programa. El establecimiento y seguimiento de la línea base de competencia de continuidad.
- Compromiso de recursos: la aplicación de suficiente y apropiado entrenamiento de personal; finanzas y otros recursos para asegurar la sostenibilidad del programa.
- Coordinación externa: coordinación de los problemas y requerimientos de continuidad con la comunidad, incluyendo clientes, vendedores, gobierno, socios, bancos, acreedores, entre otros; asegurando que la cadena de provisión tenga una adecuado programa de BCM.

4.6.3. Contenido del programa de continuidad del negocio

Las competencias direccionan cómo la organización implementa las cuatro disciplinas centrales de continuidad:

- Gestión de incidentes: asegurar que todos los aspectos de respuesta a la emergencia, gestión de crisis y otras actividades relacionadas al mando, control y comunicación han sido establecidas.
- Recuperación de tecnología: asegurar que el hardware, software, redes y aplicaciones de sistemas de información críticas sean adecuadamente recuperadas de acuerdo a los tiempos objetivos.
- Recuperación del negocio: asegurar que las funciones críticas de negocios y recursos son adecuadamente recuperados de acuerdo a los tiempos objetivos.
- Gestión de Seguridad: asegurar que la seguridad física, seguridad de información y otras actividades asociadas a proteger la integridad de la información es apropiadamente dirigida.

4.7 Modelo para el Planeamiento de Gestión de Crisis e Incidentes

Según Roberta Witty, hay seis componentes principales en un programa de Gestión de Crisis/Incidentes (C/IM) efectivo [7]:

4.7.1 Marco de Referencia

Durante un evento, mantendrá la respuesta y evitará el riesgo de información extraña e irrelevante que se convierte en una distracción a los esfuerzos de respuesta. El marco recomendado se muestra en la Figura 9:

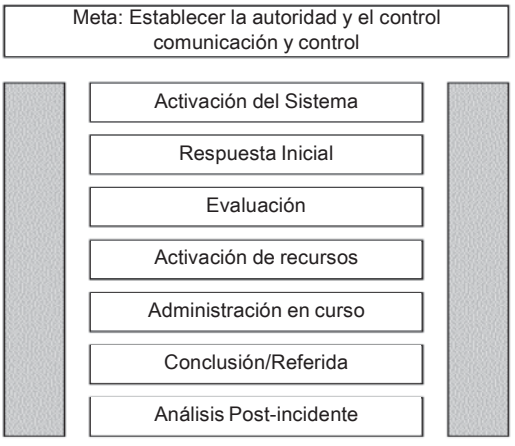


Fig. 9. Marco de referencia de un programa C/IM [38].

4.7.2 Equipo de gestión de crisis/incidentes

Conociendo quiénes en la organización están a cargo de las actividades de C/IM, y los roles de los integrantes del equipo, es clave para una ejecución exitosa de los procedimientos de C/IM.

4.7.3 Centrode operaciones de comando/emergencia

Sea un espacio físico, un salón virtual o la combinación de ambos, tener todos los roles críticos en un solo lugar es vital para asegurar que el evento está siendo monitoreado y manejado para la mejor capacidad de la organización.

4.7.4 Procedimientos de comunicaciones en crisis

Los mensajes bien direccionados son vitales para asegurar que la organización mantenga el control de la situación, y que el miedo, incertidumbre y rumores se mantengan al mínimo. Las relaciones públicas, comunicaciones corporativas, TI, áreas legales y médicas deben ser consultadas para asegurar que los mensajes enviados son apropiados para el evento. Los servicios de notificación masivos hacia proveedores, clientes y público en general pueden ayudar al objetivo.

4.7.5 Software de GCN

Usar las herramientas automatizadas correctas puede asistir a las organizaciones en la ejecución exitosa de los procedimientos de respuesta y recuperación. Aquí se incluye el software de creación, administración y prueba de planes de recuperación, software de planeamiento y de notificación masiva de emergencia.

4.7.6 Ejercitación de los procedimientos de gestión de crisis

Muchas organizaciones no enfrentan un desastre muy seguido, por lo que los planes y procedimientos de recuperación no son familiares para la mayoría de las personas en el momento que más lo necesitan. Es por ello que ejercitar es el único camino para asegurar que los planes son viables en el evento de un incidente real.

En este modelo si bien se establece un marco de referencia para la gestión de crisis, así como la necesidad de formación de equipos, no se indica quiénes deben mantener la responsabilidad de cada proceso del marco. Asimismo no se indica cuáles son las condiciones para la activación de cada paso del marco ni para la intervención de cada equipo, y no se considera la diferenciación en la gestión de crisis dependiendo de los escenarios enfrentados.

4.8 Modelo americano ISO/IEC 22301 Sociedad de Seguridad – Sistema de Gestión de Continuidad del Negocio – Requerimientos

En el 2012 la ISO emitió el estándar ISO 22301 Sociedad de Seguridad – Sistema de Gestión de Continuidad del Negocio – Requerimientos, que provee nuevos requerimientos y especificaciones para la GCN, y que se complementa con la nueva guía de la GCN aún en desarrollo, la ISO 22313 [25]. Los requerimientos especificados en este estándar internacional son genéricos e intentan ser aplicables a todas las organizaciones, o parte de las mismas, sin importar su tipo, tamaño o naturaleza [9]. Incorpora, entre otras, las definiciones de gestión de riesgos [39], las consideraciones para la preparación ante incidentes y continuidad operativa [40] y para la recuperación de servicios de tecnologías de información y comunicaciones [41].

A continuación se indican las fases que lo comprenden:

4.8.1 Contexto de la organización

- Entendimiento de la organización y su contexto. Se debe identificar y documentar: actividades, funciones, servicios, productos, socios, cadenas de suministro, relaciones con partes interesadas, y el impacto potencial relacionado a un incidente de interrupción. La relación entre la política, los objetivos de la organización y otras políticas, incluyendo su estrategia de gestión de riesgos y el apetito por el riesgo.
- Entendimiento de las necesidades y expectativas de las partes interesadas. Se debe entender a las partes interesadas relevantes para el SGCN y sus requerimientos. Tener en cuenta los requerimientos regulatorios de SGCN y otros que deban considerarse.
- Determinar el alcance del SGCN. Se debe establecer los requerimientos del SGCN, considerando la misión, metas, obligaciones internas y externas, responsabilidades legales y regulatorias. Asimismo identificar productos y servicios y todas las actividades relacionadas al alcance del SGCN, tomando en cuenta a las partes interesadas, como clientes, inversionistas, accionistas, cadena de suministro, necesidades del público.

4.8.2. razgo

La alta dirección debe demostrar su compromiso y liderazgo a través de:

- Compromiso de la dirección. Se debe asegurar que se establecen las políticas y objetivos del SGCN, y que son compatibles con la dirección

estratégica de la organización, que los recursos necesarios están disponibles, y que se logre los resultados previstos. Se debe comunicar al personal la importancia de la gestión de continuidad efectiva.

- Política. Debe ser apropiada a los propósitos de la organización y proveer un marco de referencia para establecer los objetivos de continuidad del negocio. Debe incluir el compromiso para satisfacer los requerimientos aplicables y para continuar mejorando el SGCN.
- Roles organizacionales, responsabilidades y autoridades. Asegurar que las responsabilidades y autoridades para los roles relevantes son asignados y comunicados a la organización.

4.8.3. Planeación

- Acciones para abordar riesgos y oportunidades. Determinar los riesgos y oportunidades necesarias para asegurar que el sistema de gestión puede alcanzar su estado deseado, y prevenir o reducir los efectos no deseados.
- Objetivos de continuidad del negocio y planes para lograrlos. Deben ser consistentes con las políticas de continuidad del negocio, tomar en cuenta el nivel mínimo de productos y servicios para lograr los objetivos, y ser medibles, monitoreados y actualizados como sea apropiado.

4.8.4. Soporte

- Recursos. La organización debe determinar y proveer los recursos necesarios para el SGCN.
- Competencia. Se deben determinar las competencias necesarias del personal para realizar su trabajo, y asegurarse que sean competentes.
- Concientización. El personal debe ser consciente de la política de continuidad, de su contribución a la efectividad del SGCN, las implicancias de no alinearse a los requerimientos, y su rol durante los incidentes de interrupción.
- Comunicación. Se deben establecer los procedimientos para la comunicación interna con partes interesadas y empleados, la comunicación externa con clientes, socios, comunidad, medios y partes interesadas; recibir, documentar y responder a comunicaciones de partes interesadas, y operar y probar la capacidad de comunicación a usar durante una interrupción.
- Información documentada. Debe ser adecuadamente identificada y descrita, formateada, almacenada, revisada y aprobada para su idoneidad y adecuación. Debe estar disponible donde y cuando se necesite, y estar adecuadamente protegida para evitar la pérdida de confidencialidad o integridad, o uso inapropiado.

4.8.5. Operación

- Análisis de impacto al negocio. Se debe identificar las actividades que soportan la provisión de productos y servicios, evaluar el impacto en el tiempo de no ejecutar dichas actividades, priorizar los plazos para la reanudación de las actividades a un nivel mínimo aceptable, considerando el tiempo en que el impacto de no reanudarlos se vuelve inaceptable, e identificar las dependencias y los recursos de soporte a dichas actividades, incluyendo proveedores, socios y otras partes interesadas.
- Evaluación de riesgos. La organización debe identificar y analizar los riesgos de interrupción para las actividades priorizadas de la organización, sistemas, información, personas, activos, socios y otros recursos que las soporten; e identificar tratamientos de acuerdo con el apetito.
- Estrategia de continuidad del negocio. La estrategia debe proteger las actividades priorizadas, establecer los requerimientos de recursos, e implementar las medidas para reducir los riesgos y los periodos de interrupción.
- Establecer e implementar los procedimientos de continuidad del negocio. Los procedimientos deben establecer los protocolos de comunicación interna y externa, indicar los pasos específicos a tomar durante una interrupción, ser flexible para responder a amenazas no anticipadas, y focalizarse en el impacto de los eventos.
- Estructura de respuesta a incidentes. Se identifican los umbrales de impacto que justifiquen una respuesta formal, evaluar la naturaleza y extensión del incidente y su potencial impacto, activar una respuesta apropiada de continuidad del negocio, tener procesos y procedimientos para la activación, operación, coordinación y comunicación de la respuesta.
- Planes de continuidad del negocio. Deben contener roles y responsabilidades definidos durante y después del incidente, un procedimiento para

activar la respuesta, detalle para salvaguardar el bienestar de las personas, opciones para responder a la interrupción, detalles de cómo y bajo qué circunstancias la organización se comunicará con los empleados y sus familiares; cómo la organización continuará o recuperará sus actividades priorizadas, y procedimientos para restaurar y retornar a la normalidad.

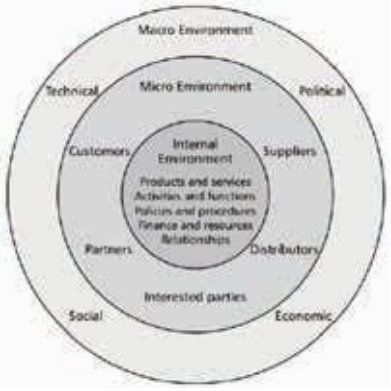
De manera similar al estándar BS 25999, se establece un modelo orientado a procesos y no a líneas de negocio, que sin embargo pone mayor énfasis en la definición de los objetivos y la participación de la alta dirección a través del liderazgo. Asimismo se mantiene general de manera que cualquier tipo de empresa pueda tomarlo de guía, pero indicando el qué y no el cómo.

4.9. Modelo de buenas prácticas para la implementación de los requerimientos de la ISO 22301

El autor [25] hace una explicación de la metodología PDCA en la cual se basa la ISO 22301 [9], el cual produce resultados de continuidad del negocio que hacen frente a los requerimientos y expectativas de las partes interesadas. A continuación se detalla el ciclo de vida de la GCN, que se mantiene similar al de la BS 25999 (ver Figura 1).

4.9.1 Contexto de la organización

- Entendimiento de la organización y su contexto. El ambiente que rodea e impacta en una organización puede ser dividido en tres áreas, las que se muestran en la Figura 10:



Fig, 10. Ambiente que rodea e impacta a una organización [25].

- Entendimiento de las necesidades y expectativas de las partes interesadas. Una técnica sugerida por el autor para identificar a los stakeholders y sus expectativas es reunir un grupo de directivos y conseguir que hagan una lista de los grupos de interés y sus expectativas, y luego clasificarlos en orden de importancia para la organización. Debería hacerse especial hincapié en las expectativas de los clientes en el momento de la interrupción.
- Determinar el alcance del SGCN. Se debe documentar áreas, productos, servicios y actividades que serán y no serán incluidas en el SGCN.

4.9.2 Liderazgo

- Política. Debe ser breve y apropiada para la organización, teniendo en cuenta su naturaleza, tamaño, complejidad, geografía y actividades críticas. Debe reflejar la cultura, dependencias y ambiente operativo.
- Roles organizacionales, responsabilidades y autoridades. Estos se reflejan en una estructura sugerida por el autor a través de la Figura 11:

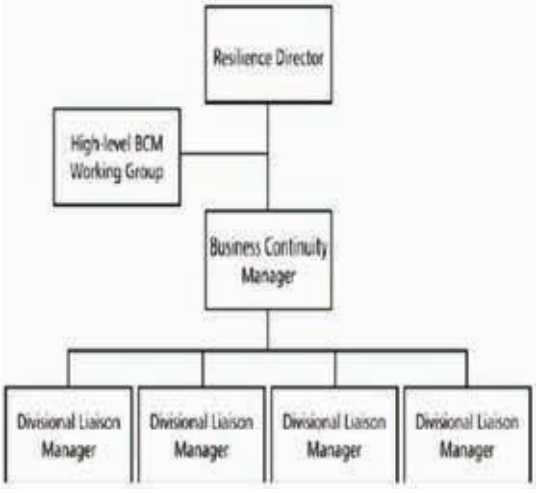


Fig. 11. Posible estructura de GCN [25].

4.9.3 Planeación

Acciones para abordar riesgos y oportunidades. Tratar de no hacer mucho la primera vez o desarrollar un SGCN muy complicado y exhaustivo. Acordar expectativas realistas con la alta dirección, dando el tiempo suficiente para la fase de diseño. Los esfuerzos iniciales deben ser percibidos como útiles y con legitimidad organizacional. La alta dirección debe reconocer el tiempo y esfuerzo que se requiere para desarrollar e implementar el SGCN.

4.9.4 Soporte

- Recursos. Se pueden definir costo de oportunidad como: costo de ventas perdidas si la producción se interrumpe más de X horas, penalidades si no se puede entregar el producto o servicio, o por no cumplir con regulaciones, y pérdida de clientes si la interrupción dura más de X días.
- Concientización. Una organización se beneficiará de una cultura positiva de GCN si desarrolla un programa de GCN, inspira confianza en las partes interesadas en su habilidad de manejar las interrupciones, incrementa su resiliencia en el tiempo y minimiza la probabilidad e impacto de interrupciones.
- Comunicación. Contar con material preparado que pueda ser rápidamente adaptado cuando se requiera puede salvar tiempo, que incluya una declaración e información general de la organización. Tener en cuenta medios como Facebook o Twitter para comunicarse rápidamente y de manera más accesible. Las instalaciones alternativas deben ser de conocimiento incluso de los proveedores.
- Documentación. Contexto, necesidades y expectativas de las partes interesadas, requerimientos regulatorios y legales, alcance y exclusiones, compromiso de la alta dirección, política, roles y responsabilidades, objetivos y planes, procedimientos, BIA y evaluación de riesgos, estrategias, pruebas.

4.9.5 Operación

La ISO 22301 no indica en qué orden debe emprenderse el BIA y la evaluación de riesgos. Para ello se deben identificar los productos y servicios clave. Para ello una opción es obtener la opinión de la gestión operacional respecto de los que considera importante para la organización, priorizando las actividades de reanudación, siendo el riesgo de que cada jefe vea sus propias operaciones como importantes. La segunda opción es contar con un equipo de alta dirección que priorice los productos y servicios, así como el MTPD y RTO.

Luego de identificar los productos y servicios críticos, se debe mapear las actividades críticas. Una forma es entrevistarse con la persona que realiza la actividad y usando notas adhesivas por actividad a manera de diagrama de flujo, indicar la información y recursos asociados. Finalmente, se obtiene como resultado un mapeado similar al de la Figura 12:

Figura 12. Mapeado de recursos de las actividades críticas [25].

La evaluación de riesgos ahora puede realizarse sobre los recursos identificados. Se deben determinar los puntos individuales de falla (Single Points of Failure - SPoF), como un miembro crítico del equipo, un local o un proveedor.

4.9.6 Estrategias de continuidad del negocio

Determinar cómo se usarán los recursos críticos: personas, locales, herramientas, equipos, artículos de consumo, tecnologías de información y comunicaciones, transporte, finanzas, proveedores e información.

Se recomienda el desarrollo de estrategias para cuatro escenarios: denegación de acceso a los locales, escasez de personal, falla de la tecnología, y falla del proveedor o socio clave. Los ejemplos de soluciones serían: oficinas alternas equipadas, proveedores alternativos, jefes interinos, contratos de reciprocidad con empresas similares.

4.9.7 Establecer e implementar procedimientos de continuidad del negocio

Al definir la Estructura de Respuesta a Incidentes (Incident Response Structure – IRS) debe tener cuatro elementos: evaluación de la situación, activación del IRS, capacidad de comunicación, y proceso de toma de decisión. Asimismo debe considerar la formación de un equipo de respuesta, el cual se sugiere tenga un líder, representantes de salud y seguridad, comunicaciones corporativas, recursos humanos, legal, operaciones, coordinador y administrador de equipo.

4.9.8 Respuesta a incidentes y planes de continuidad del negocio

El autor presenta una plantilla de evaluación para los planes, de manera que se verifique que cumpla requisitos mínimos.

5. CONCLUSIONES

Se observa que los modelos de gestión de la continuidad del negocio que han sido desarrollados a la fecha se han basado principalmente en el estándar británico BS 25999, con algunos modelos especializados desarrollados por instituciones estadounidenses que pueden considerarse como complementarios.

Asimismo se verifica que estos modelos derivados utilizan el enfoque por proceso, y no una estructura por línea de negocio como se establece en el Acuerdo de Basilea II.

Finalmente, se verifica que a pesar de que se cuenta con modelos detallados de cómo implementar ciertos aspectos de la continuidad, éstos requieren ser adaptados a las necesidades de un sector y realidad específicas, como es el sector financiera peruano.

REFERENCIAS

[1] J. Sharp, "The route map to Business Continuity Management – Meeting the requirements of BS 25999"; British Standards Institution, Londres-Reino Unido, 2008.

[2] V. Varshney, J. Hernández, "Raising BCM awareness in Latin America", Continuity Magazine, Business Continuity Institute, Edición 01, Reino Unido, Enero 2012.

[3] L. Bird, "Good Practice Guidelines – A Management Guide to Implementing Global Good Practice in Business Continuity Management", Business Continuity Institute, Berkshire-Reino Unido, 2010.

[4] Superintendencia de Banca, Seguros y Asociación de Fondo de Pensiones, "Memoria Anual 2009", http://www.sbs.gob.pe/repositorioaps/0/0/jer/pub_memorias/memo2009(2_06_2010).pdf, Lima-Perú, 2009.

[5] M. Swanson, P. Bowen, A. Wohl Phillips, D. Gallup, D. Lynes; "Contingency Planning Guide for Federal Information Systems – Special Publication 800-34 Rev. 1", National Institute of Standards and Technology – NIST, EE.UU., 2010.

[6] D. Schmidt, "NFPA 1600 – Standard on Disaster/ Emergency Management and Business Continuity Programs", National Fire Protection Association, EE.UU., 2010.

[7] R. Witty, "Pre-planning for plan invocation, Continuity Magazine", ISSN 1460-1451, Páginas 19-20, 2011.

[8] V. Corporation, "Business Continuity Maturity Model 2.0", EE.UU., 2011.

[9] International Organization for Standardization, "ISO 22301:2012 Societal Security – Business Continuity management systems – Requirements", Primera Edición, Suiza, 2012.

[10] R. St-Germain, F. Aliu, E. Lachapelle, P. Dewez, "Whitepaper: Societal Security – Business Continuity Management Systems", Proffesional Evalution and Certification Board – PECB, Nueva York-EE.UU., 2012.

[11] Superintendencia de Banca, Seguros y Asociación de Fondo de Pensiones, "Resolución SBS N° 037-2008 Reglamento de la Gestión Integral de Riesgos", Lima-Perú, 2008.

[12] Basel Committee on Banking Supervision, "Convergencia Internacional de Medidas y Normas de Capital", Press & Communications, Basilea-Suiza, 2006.

[13] Superintendencia de Banca, Seguros y Asociación de Fondo de Pensiones, "Resolución SBS N° 2116-2009 Reglamento para la Gestión del Riesgo Operacional", Lima-Perú, 2009.

[14] International Organization for Standardization, "ISO/IEC 27001, Information Technology–Security Techniques-Information Security Management Systems", Suiza, 2007.

[15] Superintendencia de Banca, Seguros y Asociación de Fondo de Pensiones, "Circular Nº G-139-2009 Gestión de la continuidad del negocio", Lima-Perú, 2009.

[16] International Organization for Standardization, "ISO 22300: 2012 Seguridad de la Sociedad – Terminología", Primera Edición, Suiza, 2012.

[17] British Standards Institution, "PAS 56:2003, Guide to business continuity management", Londres-Reino Unido, 2003.

[18] R.F. Knight, D.J. Pretty, "El impacto de las catástrofes en el valor de las acciones", Oxford, Templeton College, Universidad de Oxford, Inglaterra, 2000.

[19] UK Cabinet Office, "Emergency Preparedness, Guidance on Part 1of the Civil Contingences Act 2004", HM Government, Londres-Reino Unido, 2005.

[20] British Standards Institution, "BS EN ISO 9001:2000, Quality management systems – Requirements", Londres-Reino Unido, 2000.

[21] British Standard Institute, "BS 25999-1 Gestión de Continuidad del Negocio Parte 1 – Código de Prácticas", Reino Unido, 2006.

[22] D. Schmidt,"Implementing NFPA 1600 National Preparedness Standard", National Fire Protection Association, EE.UU., 2007.

[23] National Institute of Standards and Technology, "Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems", EE.UU., 2004.

[24] National Institute of Standards and Technology, "NIST SP 800-53, Rev.3, Recommended Security Controls for Federal Information Systems and Organizations", EE.UU., 2009.

[25] J. Sharp, "The route map to Business Continuity Management – Meeting the requirements of ISO 22301"; British Standards Institution, Segunda Edición, Londres-Reino Unido, 2012.

[26] International Organization for Standardization, "ISO/IEC 20000 (both parts), Information Technology–Service management", Suiza, 2005.

[27] British Standards Institution, "PAS77 IT Service Continuity Management", Londres-Reino Unido, 2006.

[28] British Standard Institute, "BS 25999-2 Gestión de Continuidad del Negocio Parte 2 – Especificación", Reino Unido, 2007.

[29] Canadian Standards Association, "CSA Z1600, Emergency Management and Business Continuity Programs", Canadá, 2008.

[30] Disaster Recovery Institute International, "Professional Practices for Business Continuity Practitioners", Nueva York-EE.UU., 2008.

[31] ASTM International, "ASTM E2640-10, Standard Guide for Resource Management in Emergency Management and Homeland Security", EE.UU., 2010.

[32] Federal Continuity Directive (FCD), "Federal Executive Branch National Continuity Program and Requirements", EE.UU., 2008.

[33] National Institute of Standards and Technology, "NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems", EE.UU., 2002.

[34] National Institute of Standards and Technology, "NIST SP 800-84, Guide to Test, Training and Exercise Programs for Information Technology Plans and Capabilities", EE.UU., 2006.

[35] National Institute of Standards and Technology, "NIST SP 800-37, Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems", EE.UU., 2010.

[36] National Institute of Standards and Technology, "Federal Information Security Management Act – FISMA, Public Law 107-347", EE.UU., 2002.

[37] American National Standards Institute, "ASIS SPC1 2009-1 Organizational Resilience: Security, Preparedness, and Continuity Management Systems – Requirements with Guidance for use", EE.UU., 2009.

[38] Gartner Group, http://blogs.gartner.com/business-continuity/, 2010.

[39] International Organization for Standardization, "ISO/IEC Guide 73, Risk management — Vocabulary", Suiza, 2002.

[40] International Organization for Standardization, "ISO/PAS 22399, Societal security — Guideline for incident preparedness and operational continuity Management", Suiza, 2007.

[41] International Organization for Standardization, "ISO/IEC 24762, Information technology — Security techniques — Guidelines for Information and communications technology disaster recovery services", Suiza, 2008.

Jesús Quevedo. Ingeniera de Sistemas de la Universidad Nacional Mayor de San Marcos, con ocho años de experiencia en el sector financiero peruano: en el Banco de la Nación como analista de Seguridad de Información, en EDPYME Raíz como Jefe de Ingeniería de Procesos, en Caja Rural Prymera como analista de procesos, en Banco Falabella como analista de Seguridad de Información, y actualmente en Financiera TFC como Jefe de Riesgo Operacional y Oficial de Seguridad de Información y Continuidad del Negocio. Miembro de ISACA y representante de Financiera TFC en los comités de riesgo operacional, seguridad de información y continuidad del negocio de la Asociación de Bancos del Perú – ASBANC.