Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Modelo para asegurar el involucramiento de la Seguridad de la Información en la implementación de la Continuidad del Negocio

Autora: Ing. Scarlett Villalba

Tutor: Mg. Gustavo Díaz

Año 2012

Cohorte 2011

DECLARACIÓN JURADA DE ORIGEN DE LOS CONTENIDOS

Por medio de la presente la autora manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e internacional de propiedad Intelectual.

Firmado,

Scarlett Josefina Villalba Harry

DNI: 94724821
Pasaporte: 012799754

RESUMEN

El presente trabajo de investigación presenta una síntesis de las bases teóricas, elementos fundamentales, estándares y normativas que subyacen en la Gestión de Continuidad del Negocio (Business Continuity Management/BCM). Tomando en consideración que la continuidad del negocio, se apoya en diferentes aspectos dentro de los cuales destaca la Seguridad de la Información (SI), se propone un modelo para asegurar el involucramiento de la Seguridad de la Información en la implementación de la Gestión de Continuidad del Negocio. Este trabajo ofrece un constructo que contribuye al abanico de discusión sobre la implementación del BCM y las consideraciones que éste debe tener con respecto a la SI. Para ello se empleó como estrategia metodológica, el análisis del ciclo de vida del BCM, algunos estándares y mejores prácticas más utilizadas en seguridad de la información para procurar la supervivencia de una Organización.

Palabras claves: Gestión, continuidad del negocio, contingencia, incidentes, seguridad de la información, mejores prácticas.

ÍNDICE

INTRODUCCIÓN

Los reportes emitidos por diferentes organismos, revelan que ninguna Organización está exenta de sufrir eventos extraordinarios que comprometan la continuidad del negocio y en particular lo relacionado con los activos informáticos. El riesgo de interrupción de operaciones y la posible pérdida de reputación de una Organización, imprime una dinámica particular a este tipo de situaciones, y en consecuencia se toman decisiones y se generan procesos apoyados en la contingencia, lo que implica que se dejen de lado las estrategias de Gestión de continuidad del Negocio (BCM) ya previstas. Esto además de generar un desfase entre lo importante y lo urgente, también ocasiona que se confundan los roles entres las áreas de Tecnología de la Información (TI) y Seguridad de la Información (SI) al momento de implementar el BCM.

Lo antes expuesto resalta la necesidad de generar un modelo operativo, que presente acciones para el involucramiento, delimitación de responsabilidades y participación del área de SI en la implementación del BCM. En este sentido, para guiar el curso de la investigación se plantearon las siguientes interrogantes:

¿Qué tipo de normativas, mejores prácticas ó estándares de seguridad de la información, se deben considerar para la implementación del BCM?

¿Cuál es el rol del área de Seguridad de la Información en el BCM?

¿Cómo involucrar el área de Seguridad de la Información (SI) en la implementación del BCM?

Para dar respuesta a las interrogantes planteadas y como propuesta de solución ante la necesidad antes expuesta, a continuación se presentan los objetivos de investigación.

Objetivos de la investigación

Objetivo General

Desarrollar un modelo para asegurar el involucramiento de la Seguridad de la Información en la implementación de la Continuidad del Negocio.

Objetivos específicos

- ✓ Analizar las normativas, mejores prácticas y estándares de seguridad de la información, a fin de que identificar aquellas que inciden en la implementación del BCM.
- ✓ Definir estrategias de involucramiento del área de SI en la implementación del BCM en una Organización.
- ✓ Establecer el rol de las áreas de Seguridad de Información en el BCM.

Alcance de la investigación

El modelo propuesto para asegurar la participación del SI en la implementación del BCM, toma como referente principal las normas ISO/IEC 27002 y BS 25999. Este modelo incluye la estructuración del rol de SI en el ciclo de vida del BCM. El alcance de la investigación no contempla la implementación del modelo.

Estructura de la investigación

La investigación está compuesta por tres capítulos: El primero se denomina **Marco Teórico;** y presenta las bases teórico-conceptuales relacionadas con el objeto de estudio. El segundo capítulo lleva por nombre **Descripción del Modelo Propuesto;** en él se describe las estrategias que constituyen el modelo propuesto. Finalmente se presenta el cuarto capítulo titulado **Conclusiones;** como su nombre lo indica presenta las conclusiones a las que llegó la autora al finalizar la investigación.

Enfoque y Relevancia de la Investigación

El enfoque metodológico utilizado para el desarrollo de la investigación es de tipo descriptivo. Así mismo se empleó operaciones lógicas de análisis,

síntesis y abstracción, a partir de la revisión teórico-conceptual y antecedentes investigativos del tema objeto de estudio.

La razón por la cual se justifica esta investigación, responde a la necesidad de contar con un instrumento escrito en un lenguaje sencillo y concreto, que sugiera qué y cómo hacer para involucrar la Seguridad de la Información en la implementación del BCM. Según los reportes de instituciones y asociaciones como; BCI[1] (Business Continuity Institute), ISACA[2] y ALAPSI[3] entre otros, coinciden en que, una de las dificultades presentes durante la implementación del BCM es la falta de documentación y coordinación entre el plan de continuidad y el involucramiento del recurso humano.

De allí que la relevancia y aporte fundamental de la investigación, consiste en el desarrollo de un modelo que presenta estrategias prácticas para asegurar el involucramiento del área de Seguridad de la Información en el proceso de implementación de la Gestión de Continuidad del Negocio.

[1] BCI: El Instituto de Continuidad de Negocios se creó en 1994 para permitir a sus miembros obtener orientación y soporte en relación a las actividades profesionales vinculadas con la Continuidad del Negocio.

[2] ISACA (Information Systems Audit and Control Association): Fundada en el año 1977, con el objetivo de difundir conocimientos técnicos, en el área de la Auditoría en Informática.

[3] Asociación Latinoamericana de Profesionales en Seguridad de Información (ALAPSI); Fundada en 2005, su finalidad es la de capacitar y concientizar a profesionales y organizaciones en materia de SI.

CAPITULO I

MARCO TEÓRICO

A continuación se presenta el estado del arte a partir del cual se analizan las normativas, mejores prácticas ó estándares de seguridad de la información que se deben considerar para la implementación del BCM.

Seguridad de la Información

Ante los actuales, diversos y demandantes escenarios de negocios, las organizaciones reconocen la información como parte fundamental de sus activos, por lo que han concientizado que la continuidad de sus operaciones y el aprovechamiento de las oportunidades del mercado, depende en gran medida de la "disponibilidad", "confidencialidad" e "integridad" de la información asociada a sus actividades y procesos críticos; estos tres parámetros constituyen la Seguridad de la Información

Según la ISO/IEC 2700-2:

> La Seguridad de la Información es la protección de la información contra una amplia gama de amenazas para asegurar la continuidad del negocio, minimizar los daños al negocio y maximizar el retorno de las inversiones y las oportunidades de negocio. [8]

Como corolario los activos de información están seguros cuando se mantiene preservada su:

> **Confidencialidad:** Garantía de que a la información solo puedan acceder las personas debidamente autorizadas.
> **Integridad:** Se protege la exactitud y totalidad de la información, así como los métodos de procesamiento.
> **Disponibilidad:** los usuarios autorizados deben tener acceso a la información y a los recursos asociados con la misma en el momento que lo requieran. [16]

Dependiendo de las necesidades del negocio también deben considerarse los parámetros de:

> **Autenticidad**: Busca asegurar la validez de la información en tiempo, forma y distribución. También, se garantiza el origen de la información, mediante la validación del emisor para evitar suplantación de identidades.

> **Auditabilidad**: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
> **Protección a la duplicación**: Consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
> **No repudio**: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
> **Legalidad**: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
> **Confiabilidad de la Información**: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones. [16]

Es importante diferenciar el concepto Seguridad de la Información del concepto Seguridad Informática, el alcance de esta última se deriva en la protección de las infraestructuras que soportan los recursos de Tecnología de la Información y la Comunicación. Por su parte la Seguridad de la Información es un proceso más amplio que absorbe la Seguridad Informática.

Gestión de Continuidad del Negocio

El escenario organizacional, se ve impactado por diferentes circunstancias tales como; nuevas tecnologías, estrategias de mercado, tendencias de competitividad, infraestructura, condiciones geográficas, meteorológicas y naturales. Las fallas, debilidades o eventos inesperados de cualquier índole, implica que la actividad organizacional sea reducida y en el peor de los casos interrumpida.

De allí la importancia de disponer de marcos de acción para garantizar la Continuidad del Negocio. A partir del interés e importancia que se le adjudico a nivel mundial a este tema, a mediados de los años 1980 creció la investigación y desarrollo de estos framework para Gestionar la Continuidad del Negocio. Impulsado por la relevancia de la mencionada temática el BCI, define la Gestión de Continuidad del Negocio ó Business Continuity Management (BCM) como:

> Proceso de gestión holístico que identifica potenciales impactos que amenazan la Organización y provee una estructura para la aumentar la resistencia y la capacidad de respuesta de manera efectiva que salvaguardan los intereses de las partes interesadas, su reputación, marca, valor y las actividades que aportan valor al negocio. [1]

Este proceso para la Gestión de Continuidad del Negocio centra sus estrategias en la planificación para la reducción de riesgos y el restablecimiento de las actividades del negocio ante situaciones inesperadas (Disaster Recovery), no obstante para alcanzar esa resiliencia, se requiere asumir el BCM como un sistema.

Así pues la Continuidad del Negocio se concibe desde un concepto interdisciplinario que abarca de forma transversal todas las áreas, actividades y elementos de la organización.

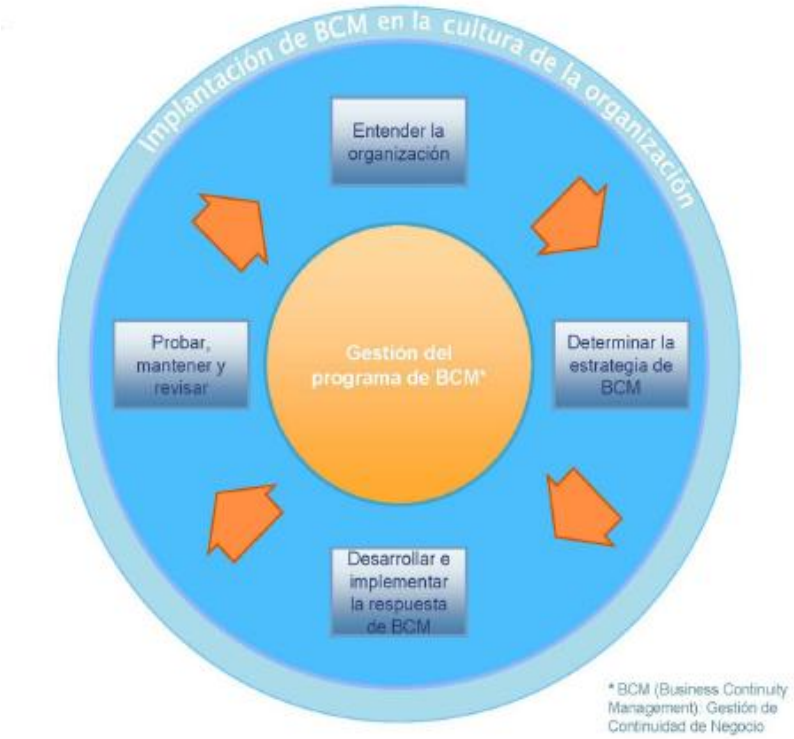
¿Dónde se ubica la Continuidad del Negocio?

La continuidad del negocio no es un proceso aislado y/o particular conformado por las actividades de alguno de los elementos que integran una organización; contrario a esto el trabajo integrado, organizado y progresivo es la mejor herramienta para vencer alguna eventualidad que comprometa la consecución normal de los procesos en cualquier organización.

En este sentido es pertinente distinguir lo urgente de lo importante, así como tener presente el alcance y funcionamiento del BCM dentro de la organización. La norma BS25999 resume lo antes planteado a través de un esquema que denomina; Ciclo de Vida del BCM, éste ofrece una orientación sobre el funcionamiento continúo de la Gestión de continuidad del Negocio (BCM) y las medidas apropiadas ante la restauración de las actividades del negocio.

El Ciclo de Vida del BCM constituye cinco etapas, que se resumen en: Entender la organización, Determinar las estrategias de continuidad y/o recuperación del negocio, Desarrollar e implementar las respuestas de BCM, Pruebas, mantenimiento y revisión, e Implantar la cultura de BCM en la organización [2]:

Figura 1. Ciclo de vida del BCM



Fuente: http://scc2008.webs.com/Desarrollo/BS%2025999.docx

A continuación se describen las etapas del ciclo de vida del Software, según lo planteado en la BS25999 [2]:

✓ **Entender la organización:** Durante esta etapa se identifican los procesos y elementos críticos de la organización, así como el análisis del impacto que pueda generar cualquier interrupción de las actividades propias del negocio. La BS25999 plantea que:

> Debe existir un método definido, documentado y apropiado para determinar el impacto de toda interrupción de las actividades que dan soporte a los principales productos y servicios [3]

Este análisis de impacto al negocio (BIA)[4] diligencia la toma de decisiones sobre el tratamiento que se destine ante la causa de la interrupción, ya sea; la aceptación, mitigación ó trasferencia del riesgo que origine la posible

[4] BIA (Busiess impact analysis): Es un proceso esencial para respaldar la continuidad del negocio, cuyo objetivo es determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto

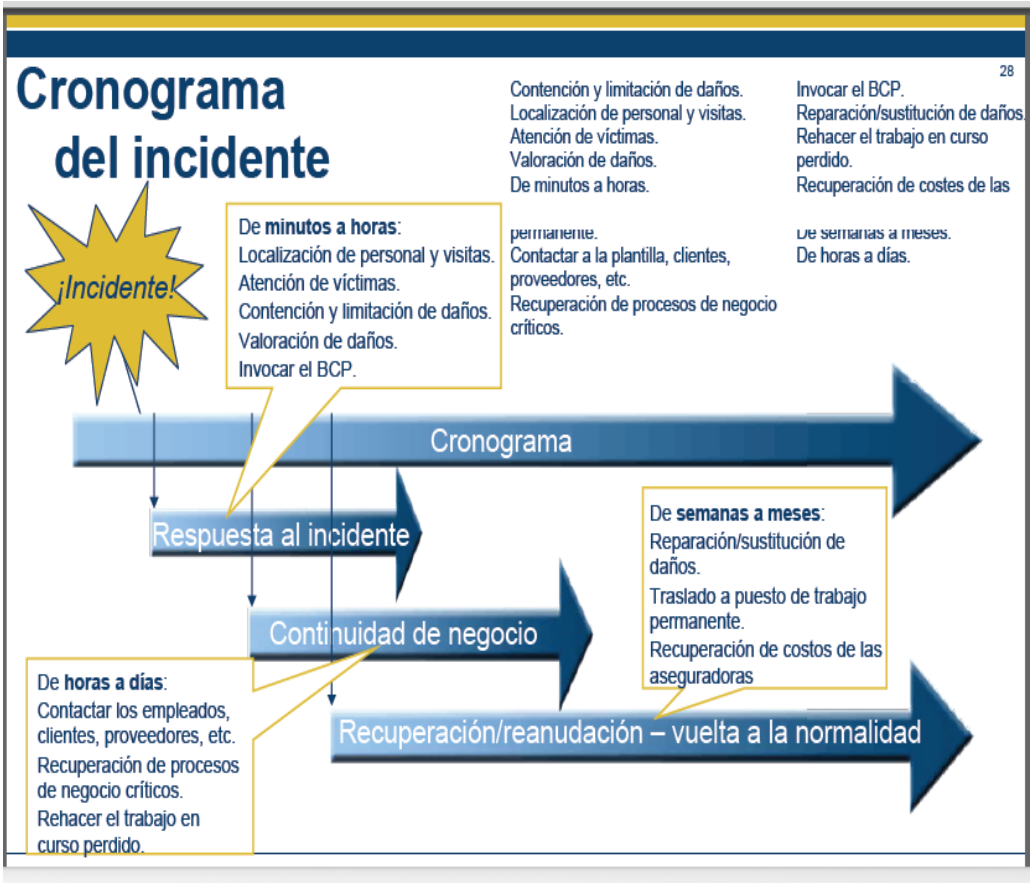
interrupción, también forma parte de estas alternativas, la finalización de la actividad comprometida.

✓ **Determinar las estrategias de continuidad y/o recuperación del negocio:** La definición de etas estrategias, estriba en; el período de tolerancia de interrupción, las consecuencias que deban afrontarse en caso de no ejecutar alguna acción y los recursos que se invertirán en la implementación de medidas, en este particular la Bs BS25999 define estos recursos a nivel de:

> 1. Personas: El recurso humano como elemento más importante de una organización, puede representar una de las vulnerabilidades más significativas. Por ende entre las estrategias de continuidad y/o recuperación del negocio, deben enmarcarse en el desarrollo de habilidades, conocimiento y concientización de las personas; a través de la documentación, formación y segregación de actividades claves.
> 2. Locales: Estas estrategias persiguen disminuir el riesgo por inaccesibilidad, en este caso se pueden implementar medidas como; disponibilidad de locales alternativos, propiciar el trabajo remoto y disposición de un equipo de personal emergente.
> 3. Tecnología: Este punto se apoya en la disponibilidad de recursos tecnológicos necesarios para activar las actividades críticas en tiempo de emergencia.
> 4. Información: El objetivo de estas estrategias deben centrarse en garantizar la disponibilidad, confiabilidad e integridad de la información crítica de la organización, según los tiempos mínimos determinados en el BIA.
> 5. Suministros: Se trata de garantizar la disponibilidad de los suministros que sustentan las actividades vitales. Para ello es necesario: incrementar el número de proveedores, mantener un stock de emergencia en almacenes, identificar proveedores de suministros alternativos, establecer acuerdos con proveedores para abastecimiento ante contingencias.[3]

✓ **Desarrollar e implementar las respuestas de BCM:** Esta etapa se despliega a partir de entender la organización y consiste en definir una estructura de respuesta ante incidentes, a través de la elaboración e implementación de los diferentes planes que permitan gestionar una interrupción de cualquier índole.

Figura 2. Delimitación de períodos ante la respuesta de incidentes



Fuente: http://scc2008.webs.com/Desarrollo/BS%2025999.docx

La figura anterior representa la delimitación de tres períodos relacionados con la ocurrencia y los planes a implementar ante un incidente. El enfoque de estos planes dependerá de la naturaleza del negocio, entre los más utilizados en lo que respecta a información se puede mencionar; Plan de Gestión de Incidentes, Plan de Continuidad del Negocio y la reanudación de planificación de negocios.

El contenido de estos planes según la Bs BS25999 debe contemplar como mínimo:

a) Las actividades críticas deben ser recuperadas y bajo que situaciones debe aplicarse el plan.
b) Las actividades críticas priorizadas y enmarcadas por los periodos de tiempo, y niveles de recuperación necesarios.
c) Roles y responsabilidades durante el incidente.
d) Procedimientos para la activación de la gestión de incidentes, continuidad del negocio o recuperación.

e) Datos de contacto de las personas clave implicadas en cada plan.
f) Responsable de la actualización de cada plan. [3].

✓ **Pruebas, mantenimiento y revisión:** Como lo indica el enunciado esta fase está conformada por tres casos, que van desde la implementación de pruebas, mantenimiento, hasta la revisión de planes y estrategias de continuidad. En el primer caso; la validación de cada uno de los planes que conforman la Gestión de Continuidad del Negocio, proporcionan la fiabilidad, afianza el conocimiento y desarrolla las habilidades requeridas para hacer frente a situaciones de contingencia.

Con respecto al mantenimiento, es importante que cada uno de los mencionados planes y estrategias estén acorde con las características y necesidades vigentes del negocio, una vez implementadas las pruebas se identifican los aspectos a mejorar y se incorporan nuevos elementos que se hayan desestimado en las versiones originales. Forman parte del mantenimiento los mecanismos de comunicación de mejora, los sistemas de control de cambios y los planes de actualización y concientización del personal.

Así mismo es necesaria la revisión periódica mediante procesos de auditorías, a partir de la revisión de los estándares e indicadores de buenas prácticas en la Gestión de Continuidad del Negocio. En este caso es recomendable implementar las siguientes técnicas: auto evaluación, auditoria forense, cumplimiento de auditoría, diligencia de auditoría, viabilidad de auditoría, control de auditoría y mejor valor auditado [2]

Fases de la Gestión de Continuidad del Negocio

La implementación de políticas, mejores prácticas y estrategias de Continuidad del Negocio estriban en la cultura organizacional, naturaleza y alcance de la organización, en este sentido es recomendable considerar los estados que contribuyen a la madurez del proceso de BCM, a propósito de esto, la norma BS25999 plantea diez fases [2], las cuales están enmarcadas en el ciclo de vida del BCM:

1. Inicio y gestión del proyecto: Esta fase constituye el punto de partida, ya que su objetivo principal consiste en explicar e instaurar la

necesidad de desarrollo del BCM, así como lograr el compromiso, apoyo de los directivos y demás miembros de la organización (recurso humano y proveedores externos). En relación con el ciclo de vida del BCM, esta fase se corresponde con la primera etapa, denominada “Entender la Organización”.

2. Evaluación y control del riesgo: Implica la identificación, clasificación y documentación de amenazas y riesgos, tanto a nivel interno como externo a la organización. Se ubica en la primera etapa del ciclo de vida del BCM.

3. Análisis de impacto del negocio (BIA). El BIA se circunscribe en la primera etapa del ciclo de vida del BCM. Para el desarrollo de esta fase es necesario esgrimir una visión holística de la organización. El BIA sienta sus bases en el Recovery Time Objetive (RTO)[5] y el Recovery Point Objetive (RPO)[6].

4. Desarrollo de estrategias para la Continuidad del Negocio: Constituye la segunda etapa (Determinar Estrategias) del ciclo de vida del BCM. Durante esta fase se definen los diferentes escenarios de posibles estrategias para la recuperación de las operaciones del negocio, dentro de un marco de tolerancia de tiempo de interrupción (este tiempo es identificado durante la fase de análisis de impacto del negocio). El desarrollo de estrategias involucra los siguientes elementos:

1. La identificación de requerimientos de la organización.
2. Comparar el nivel de compatibilidad de las estrategias con los resultados del BIA.
3. Análisis costo-beneficio de las estrategias de continuidad.
4. Comprensión de los términos contractuales de los servicios de la continuidad del negocio. [2]

5. Respuesta ante emergencias: Se circunscribe en la etapa de desarrollo e implementación de respuesta, del ciclo de vida del BCM (tercera etapa). Constituye la elaboración e implementación de las estrategias y planes para la recuperación de las actividades del negocio ante una interrupción incidental. Durante esta fase resalta la necesidad de identificar e implementar los procedimientos de control de emergencias y de autoridad. Este control de

[5] **RTO:** Tiempo entre el punto de interrupción y el punto en el cual las actividades críticas, con respecto al tiempo, deben estar restablecidas.
[6] **RPO:** Punto de interrupción de las actividades del negocio.

autoridad se refiere a la designación de responsabilidades y atribuciones de los elementos de la organización, ante situaciones de emergencia.

6. Desarrollo e implementación del BCM: Se inserta en la tercera etapa del ciclo de vida del BCM. Esta fase está conformada por el diseño, desarrollo e implementación de los planes de continuidad del negocio, en correspondencia con lo señalado en el RTO y RPO. Para desarrollar e implementar acertadamente es sustancial:

1. Identificar los requerimientos para el desarrollo de los planes.
2. Definir requerimientos de control y administración de la continuidad.
3. Definir procedimientos de gestión de crisis y continuidad del negocio.
4. Definir las estrategias de evaluación de daños y reanudación de actividades.
5. Desarrollar la documentación de los equipos de operación del negocio y la recuperación tecnológica de la información.
6. Desarrollar el sistema de comunicaciones y los planes de los usuarios finales.
7. Implementar planes.
8. Establecer los procedimientos de control y distribución de los planes. [2].

7. Programa de concientización y capacitación: Las acciones entorno a la mitigación de los riesgos, así como la recuperación de las actividades del negocio luego de un incidente, generan una ambiente de incertidumbre que afecta a las personas involucradas con la organización. La puesta en marcha de los planes y estrategias ante cualquier contingencia se puede ver afectada por la resistencia al cambio, por lo que es necesario, capacitar a los involucrados para disminuir la incertidumbre por desconocimiento.

Así mismo es importante gestar una cultura organizacional en el marco del BCM, esto se logra mediante políticas de concientización. Esta fase guarda relación con la etapa de implantación del BCM en la cultura de la organización (dentro del ciclo de vida del BCM).

8. Mantenimiento y ejercicio del BCM: Esta fase, como se explica anteriormente en el ciclo de vida de BCM (cuarta etapa: probar, mantener y revisar), testifica que los planes entorno a la Gestión de Continuidad del Negocio permanezcan efectivos con respecto a la gestión de crisis, mitigación de riesgo, tiempos y puntos de recuperación.

9. Comunicación de crisis: Es necesario contemplar un plan de comunicación en situación de crisis, para que el entorno organizacional este

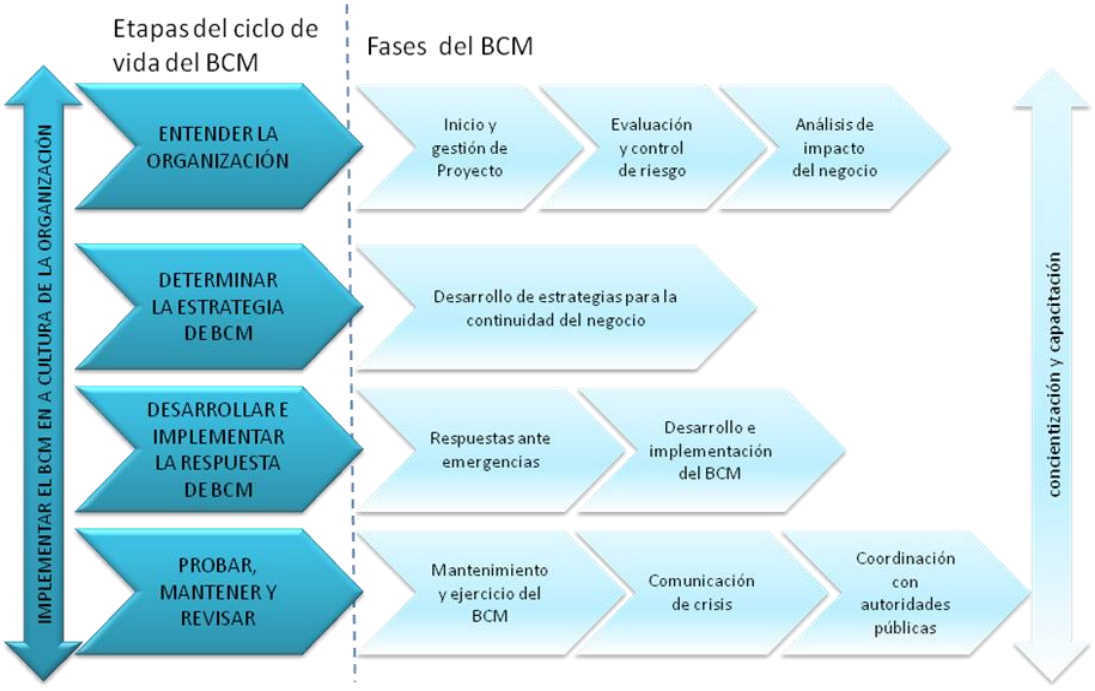
informado y en consecuencia reaccione según lo estipulado y en función de minimizar los costos de interrupción. La comunicación de crisis se inserta en la cuarta etapa del ciclo de vida del BCM

10. Coordinación con Autoridades públicas: Enmarcada en la cuarta etapa del ciclo de vida del BCM, esta etapa la conforman la documentación de políticas y planes de continuidad, las cuales son de carácter imprescindible y deben ser oficializadas ante las instancias correspondientes. Durante este proceso es necesario:

a) Revisión de políticas vigentes.
b) Consultar profesionales externos a la organización.
c) Identificar, actualizar y modificar las políticas de BCM existentes.
d) Documentarse sobre los códigos actuales de buenas prácticas de BCM, implementados en otras organizaciones.
e) Conformas equipos de trabajos multidisciplinarios.
f) Someter a discusión los borradores de nuevas políticas de BCM. [2]

Como se ha mencionado en lo antes descrito, estas diez fases de la Gestión de la Continuidad del Negocio se insertan dentro de las etapas del ciclo de vida del BCM. A continuación se muestra una representación gráfica, con el objeto de conceptualizar de manera resumida esta interacción:

Figura 3. Fases de la gestión de continuidad del negocio en las etapas del ciclo de vida del software



Fuente: elaboración propia (2012)

¿Qué tipo de normativas, mejores prácticas ó estándares de seguridad de la información, se deben considerar para la implementación del BCM?

Familia de normas ISO/IEC 27000. Seguridad de la Información

La serie ISO[7]/IEC[8] 27000 constituye un conjunto de normas que ofrecen un estándar internacional, que proporcionan un marco para la gestión de la Seguridad de la Información. Esta serie está conformada por las normas bases ISO/IEC 27000-1 e ISO/IEC 27000-2 y otras normas complementarias, aunque alguna de ellas aun se encuentran en desarrollo, o no han sido publicadas se mencionan a continuación:

ISO 27003: Presenta una guía de implementación de SGSI[9] e información acerca del uso del modelo PDCA (Plan, Do, Check, Act) y de los requerimientos de sus diferentes fases.
ISO 27004: Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.
ISO 27005: Guía de técnicas para la gestión del riesgo de la Seguridad de la Información y sirve de apoyo a la ISO 27001 y a la implantación de un SGSI.
ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de Sistemas de Gestión de Seguridad de la Información.
ISO 27007: Consiste en una guía de auditoría de un SGSI.
ISO 27011: Consiste en una guía de gestión de seguridad de la información específica para telecomunicaciones.
ISO 27031: Consiste en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.
ISO 27032: Consiste en una guía relativa a la ciberseguridad.
ISO 27033: Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.
ISO 27034: Consiste en una guía de seguridad en aplicaciones. [6]

ISO/IEC 27000-1

Fue publicada el 15 de octubre de 2005 y es la norma principal de la serie, establece los requisitos para desarrollar, implantar, controlar, revisar, mantener y mejorar un SGSI sustentado en los riesgos del negocio de una

[7] **ISO** (International Organization for Standardization) la Organización Internacional para la Estandarización, es el encargado de promover el desarrollo de normas internacionales, así como la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional, en todas las áreas industriales a excepción del ramo eléctrico y electrónico.
[8] **IEC** Comisión Electrónica Internacional, es una comisión normalizadora en los campos eléctricos y electrónicos.
[9] **SGSI:** Sistema de Gestión de la Seguridad de la Información.

organización. Según lo expresa su publicación, esta norma específica los requisitos para la implantación de los controles de seguridad hechos a medida de las necesidades de organizaciones individuales o partes de las mismas [7].

Los puntos focales de esta norma se pueden resumir en dos elementos; "gestión de riesgo" y "mejora continua". ISO/IEC 27000-1 se apoya en el ciclo de Deming ó también conocido como modelo PDCA[10], este modelo se puede poner en práctica para todos los procesos del SGSI, además impulsa a los usuarios de este sistema para que asuman la importancia de:

a) Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
b) Implementar y operar controles para manejar los riesgos de la seguridad de la información.
c) Monitorear y revisar el desempeño y la efectividad del SGSI.
d) Mejoramiento continuo en base a la medición del objetivo. [7]

La ISO/IEC 27000-1 está estructurada de la siguiente manera:

Fase de Planificación (PLAN); Consiste en establecer el SGSI en cuanto a objetivos, políticas, procesos y procedimientos relativos a la gestión de riesgo y mejora de la seguridad de la información.
Fase de Ejecución (DO); contempla la implementación y gestión del SGSI de acuerdo a su política controles y procesos.
Fase de Seguimiento (Check); se centra en la medición y revisión de las prestaciones de los procesos del SGSI.
Fase Mejora (ACT); adoptar acciones preventivas y correctivas basadas en auditorias y revisiones internas a fin de procurar la mejora continua del SGSI. [7]

ISO/IEC 27000-2

El 01 de julio del año 2001 la norma ISO 17799:2005 adoptó el nombre de ISO/IEC 27000-2; esta es una guía de buenas prácticas que se basa en objetivos de control y controles para la SI, los cales deben implementarse en base a los resultados de la evaluación de riesgo. Esta no es una norma certificable, su fin principal consiste en definir los aspectos operativos de la implementación del SGSI.

[10] El ciclo **PDCA**, o "Círculo de Deming" (de Edwards Deming), es una estrategia de mejora continua de la calidad en cuatro pasos: **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar).

Esta Norma puede servir como recomendación práctica para desarrollar normas de seguridad de la organización y una práctica efectiva de la gestión de la misma, así como ayudar a construir confianza en las actividades entre organizaciones [17].

Esta norma está estructurada en 11 dominios, 39 objetivos de control y 133 controles. Los objetivos de control recogen aquellos aspectos fundamentales que se deben analizar para conseguir un sistema seguro en cada área de la organización, para alcanzar estos objetivos es necesario cumplir con los controles, por cada control la norma incluye una guía de implementación [7].

Figura 4. Distribución de los dominios de ISO/IEC 27000-2

Fuente: http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf

Norma Británica BS25999

Se trata de la primera norma certificable, fue publicada por el British Standards Institute (BSI), es de origen Británico y plantea la estandarización de los procesos, buenas prácticas y terminologías para la Gestión de Continuidad del Negocio. Tiene como objetivos principales:

- ✓ Proporcionar una base para entender la Gestión de Continuidad del Negocio.
- ✓ Proporcionar un medio de medida que sea coherente y reconocido.
- ✓ Proporcionar un sistema basado en buenas prácticas establecidas [12]

La norma BS25999 se divide en dos partes; la primera parte es un código de buenas prácticas, publicado en el año 2006 conocido como BS25999-1, que sirve de guía general para la definición del alcance y desarrollo del plan de continuidad del negocio. Así mismo esta primera parte presenta los lineamientos y requisitos para obtener la certificación de continuidad del negocio. Este código de buenas prácticas de la continuidad del negocio define los siguientes elementos:

- ✓ Alcance del plan de continuidad del negocio.
- ✓ Definición de las políticas de continuidad en la organización.
- ✓ Identificación de las actividades Críticas del negocio.
- ✓ Desarrollo y gestión de un plan de continuidad del negocio.
- ✓ Validación, mantenimiento y ejercicio del plan de continuidad del negocio.
- ✓ Permear la continuidad del negocio en la cultura organizacional. [18]

La segunda parte de esta norma, publicada en el año 2007, contiene las especificaciones de los requisitos que debe cumplir cualquier organización para alcanzar la certificación. Este documento estableces los indicadores para los procesos de auditorías externas.

La Bs25999-2 concibe la continuidad del negocio como un sistema cuya creación y mantenimiento incluye cuatro secciones principales; la planificación, implementación y operación, supervisión y medición, manteamiento y mejora del Sistema de Gestión de Continuidad del Negocio [4].

Código de buenas prácticas BS25999-1

Su contenido recorre el ciclo de vida del BCM a través de sus controles basados en buenas prácticas. A continuación se resume las diez secciones que conforman el BS25999-1:

Sección 1. Ámbito de aplicación y aplicabilidad; Esta primera sección presenta el alcance y describe las mejores prácticas, las cuales deben ser adaptadas a las condiciones de cada organización.
Sección 2. Términos y Definiciones. Puntualiza los términos y definiciones presentes en toda la norma.
Sección 3. Información general de la gestión de la continuidad del negocio. Describe de manera general la vinculación entre procesos, gestión de riesgos y justificación para la puesta en marcha de la Gestión de Continuidad del Negocio.
Sección 4. El negocio de gestión de la continuidad política. Describe el escenario para la aplicación de la Continuidad del Negocio, basado en la definición de políticas y recursos necesarios

Sección 5. BCM Gestión de Programas. Define el enfoque de la Gestión de Continuidad del Negocio.
Sección 6. Conocimiento de la organización. Plantea la comprensión de las actividades críticas del negocio, así como la disponibilidad de recursos, vulnerabilidades y riesgos, con el objeto de definir e implementar las estrategias adecuadas para la continuidad del negocio.
Sección 7. Determinación de las estrategias de BCM. Trata de la definición de las estrategias de BCM, esta sección depende directamente de lo planteado en la sección 6.
Sección 8. Desarrollar y aplicar una respuesta BCM. Abarca las estrategias de BCM, gestión de incidentes y planes de continuidad del negocio.
Sección 9. El ejercicio, el mantenimiento, auditoría y autoevaluación de la cultura de BCM. Establece la necesidad de validar la efectividad del BCM, a partir de la implementación de pruebas a partir de las cuales se puedan definir las modificaciones necesarias. **Sección 10. Adherido a BCM en la cultura de las organizaciones.** Trata de la importancia de permear el BCM en la cultura organizacional. [12]

Este código de bunas prácticas Bs25999-1, sirve de apoyo para la implementación de la Continuidad del Negocio, surgió como reemplazo a PAS 56:2003[11] y abarca relaciones B2B (Negocio a Negocio) y B2C (del Negocio al Consumidor) en cualquier sector, tipo y tamaño de organización.

Especificaciones de la BS25999-2

La BS25999-2 presenta la especificación de requerimientos para que cualquier organización alcance la certificación en materia de Continuidad del negocio, a través de seis secciones:

Sección 1. Ámbito de aplicación de la Gestión de continuidad del Negocio. Define el ambiente de aplicación de la norma, así como los requisitos para la implementación de un sistema documentado de la continuidad del negocio.
Sección 2. Términos y Definiciones. Esta sección define los términos y definiciones utilizadas en el cuerpo de la norma.
Sección 3. Planificación de la Continuidad del Sistema de Administración de Empresas (Plan). Esta segunda parte de la BS25999 eta basada la estrategia de mejora continua, conocida como el círculo de Demimg “Plan-Do-Check-Act”.
Sección 4. Implementación y funcionamiento de la BCMS (DO) de aplicar en la práctica los planes. Esta sección está totalmente basada en la BS25999-1 pero se aborda desde el punto de vista de la implementación evaluación.
Sección 5. Seguimiento y revisión de la BCMS (Check). Estable las comprobación y control del BCM a partir de auditorías internas, así como la revisión de la Gestión del la Continuidad del Negocio.

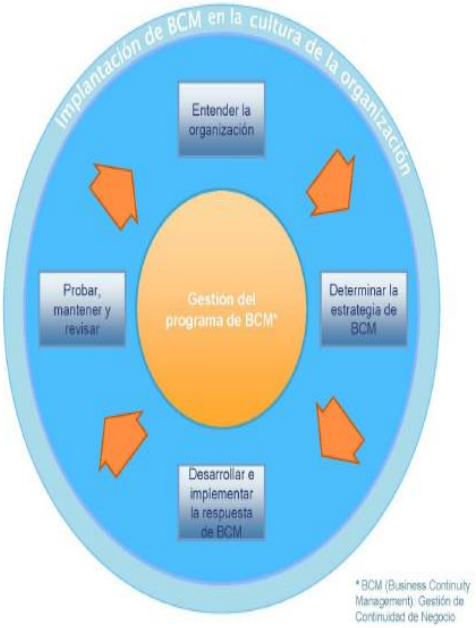
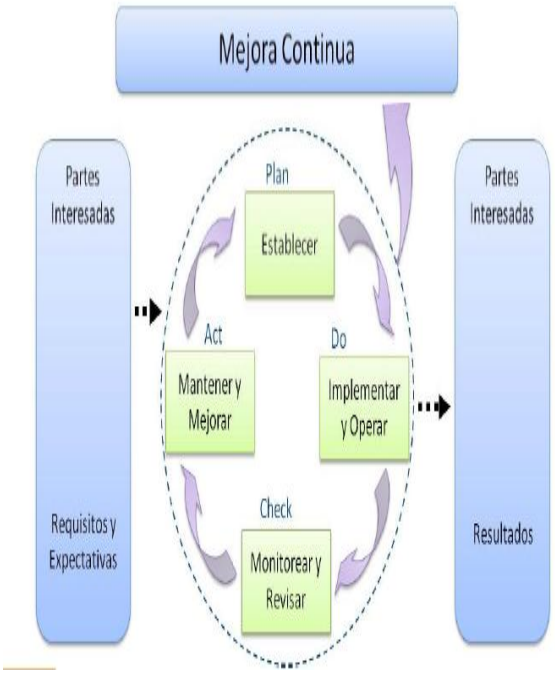
[11] PAS 56:2003 es una guía publicada por el BSI en colaboración con el BCI que establece el proceso fundamental, los principios y la terminología referente a la Gestión de Continuidad de Negocio, incluyendo una serie de buenas prácticas en lo relativo a anticipación a incidentes y respuesta a los mismos. No constituye en sí un estándar o norma certificable.

Sección 6. Mantenimiento y Mejora de la BCM (ACT). Esta sección propone la mejora continua del BCM a través de las acciones preventivas y correctivas del BCM. [12]

BS25991- Vs BS2599-2

La diferencia entre estas dos partes que conforman la estructura de la BS25999 se ve reflejada en su ámbito de aplicación y en los elementos que sustentan a cada una de ellas, la BS25999-1 está apoyada sobre el ciclo de vida del BCM, mientras que la BS25999-2 toma como referente el ciclo de mejora continua. Eta diferenciación se refleja en la figura que se presenta a continuación:

Figura 5. BS25991- Vs BS2599-2

BS25999-1; Basado en el Ciclo de Vida del BCM	**BS2599-2;** Basado en el ciclo de mejora continua PDCA
	

Fuente: http://sas-origin.onstreammedia.com/origin/isaca

ASIS SPC 1-2009. Resistencia Organizativa: Sistemas de Gestión de la Seguridad, Disposición y Continuidad

Es una norma desarrollada por ASIS[12] Internacional y está orientada hacia la resiliencia de las organizaciones, se centra en los componentes asociados al control, mitigación y gestión de riesgos, así como a los aspectos reactivos propios de la Continuidad del Negocio. La norma incluye una guía que sirve de apoyo para la evaluación de riesgos y el desarrollo de estrategias que permitan a la organización y las personas prevenir y dar respuestas ante situaciones inesperadas.

ASIS SPC 1-2009 proporciona a cualquier organización un marco de referencia para:

- ✓ Crear una estrategia equilibrada para la gestión, reducción y prevención de riesgos e incidentes.
- ✓ Establecer, implantar, mantener y mejorar un sistema de gestión organizativa para la resistencia ante situaciones críticas.
- ✓ Demostrar la capacidad para la recuperación y la continuidad de la actividad, de cara al cumplimiento de acuerdos contractuales.
- ✓ Asegurar la conformidad con las políticas declaradas, sobre la capacidad real de recuperación de los procesos organizativos.
- ✓ Aplicar un modelo de enfoque maduro, para optimizar y rentabilizar el coste de los procesos generados de cara a la resistencia de la organización.
- ✓ Potenciar la optimización de recursos invertidos en la implantación de otras normas del sistema ISO (ISO 9001, ISO 14001, ISO 27001, ISO 28000, etc) para mejorar la seguridad, los niveles de preparación, la disposición de medios organizativos, humanos y materiales, y la gestión de la continuidad de la actividad corporativa.
- ✓ Integrar todas las responsabilidades en materia de gestión de riesgos, asumidas por las diferentes unidades de negocio o de servicio, dentro de un único sistema corporativo desarrollado de conformidad con la norma ISO 31000, de gestión integral del riesgo. [15]

[12] Es una asociación que impulsa la profesionalización en seguridad y protección. Fundada en 1955, ASIS se dedica a aumentar la eficacia y la productividad de los profesionales de la seguridad mediante el desarrollo de programas y materiales educativos que se ocupan de los intereses generales de seguridad.

NFPA 1600-2010. Gestión de Desastres, Emergencias y programas de Continuidad del Negocio

Esta norma publicada por la NFPA[13], ha evolucionado desde su primera edición en el año 2000. En la actualidad se edita una presentación 2013, no obstante la que se encuentra vigente es la versión 2010 la cual establece los procedimientos y terminología para la Gestión de Emergencias, Desastres y continuidad del Negocios, a partir del reordenamiento de los cinco principios fundamentales de la NFPA 1600-2007; prevención, preparación, respuesta, recuperación y mitigación de las emergencias.

Esta norma está concebida para organizaciones de cualquier índole y es aplicable todo tipo de incidentes, ya sean causados por el hombre o por desastres naturales. Entre los aspectos mas resaltantes de esta norma destaca su capítulo cinco, el cual hace referencia a la comunicación de las crisis y la información pública. Este capítulo define:

> La necesidad de la planificación y comunicación ante eventos de crisis, estableciendo procedimientos para proveer información al ámbito interno y externo de manera adecuada (incluyendo a los medios de comunicación), mediante la definición de interlocutores pertinentes para evitar el caos y el pánico generalizado [14]

ISO 22301. Seguridad de la Sociedad: Sistemas de Continuidad del negocio

El borrador final de esta normativa será publicado para el segundo trimestres del año en curso (2012) [10], se estima que se suscite una transición entre la BS25999 y la ISO22301. La ISO define esta norma como:

> La estandarización en el área de seguridad de la sociedad, orientada a incrementar las habilidades en gestión de crisis y continuidad del negocio; por ejemplo, a través de mayor interoperatividad técnica, humana, organizativa y funcional, como también concienciación situacional compartida entre todas las partes interesadas [14]

Aunque la ISO 22301 no es correlativa por cada uno de los elementos de la BS25999, presenta similitud ya que su contenido está basado en las

[13] National Fire Protection Association, es una organización internacional cuyo objetivo lo constituye el desarrollo de normas para la reducción incendios y otros riesgos.

buenas prácticas de BCM y también estará constituida en dos partes. En la ISO 22301 los planes de recuperación y el análisis de impacto del negocio están puntualizados de manera más amplia, además presenta otras diferencias:

- ✓ En la ISO 22301, el modelo Planificación-Implementación-Verificación-Mantenimiento (PDCA, por sus siglas en inglés), en comparación con la BS 25999-2, está desarrollado con menos claridad.
- ✓ La ISO 22301 Pretende acercar la continuidad del negocio a la forma de pensar de la alta dirección; pare ello enfatizará el establecimiento de los objetivos, así como la verificación del rendimiento.
- ✓ La ISO 22301 solucionará una de las falencias de la BS 25999-2 y demandará una planificación y preparación de recursos para asegurar la continuidad del negocio mucho más detallada ya que esos requisitos ahora son más extensos y están estructurados con mayor claridad.
- ✓ La ISO 22301, por ser una norma internacional, implica que las entidades de certificación serán mucho más exigentes, por lo cual obtendrá más reconocimiento con mayor rapidez. [14]

CAPITULO II

DESCRIPCIÓN DEL MODELO PROPUESTO

El modelo propuesto en la presente investigación surge a partir del análisis de diferentes guías, manuales, modelos y mejores prácticas para la implementación de la Gestión de Continuidad del Negocio (BCM). Esta propuesta puede aplicarse en cualquier organización y tipo de negocio.

El objetivo de este modelo se enmarca en un conjunto de estrategias que aseguren el involucramiento del área de Seguridad de la Información en la implementación de la Gestión de Continuidad del Negocio (BCM), el conjunto de acciones que conforman dicho modelo se justifica en lo planteado por INTECO[14], este instituto sostiene que:

> Uno de los principales inconvenientes o barreras a las que se enfrenta una Organización cuando decide abordar cualquier tipo de iniciativa relacionada con la continuidad de negocio es la falta de conocimiento y de instrucciones claras y concisas que detallen por dónde empezar y qué aspectos deben tenerse en cuenta para garantizar el éxito [9].

Tomando como referencia la cita anterior, las estrategias que constituyen el modelo propuesto contemplan desde la definición de las funciones del área de SI, hasta su nivel de participación en la ya mencionada implementación del BCM.

Estructura del Modelo para asegurar el involucramiento de la Seguridad de la Información en la implementación de la Continuidad del Negocio

Las estrategias propuestas para este modelo son de elaboración propia, para ello la autora realizó un compendio de:

1. Los códigos de buenas prácticas contenidos en la norma ISO/IEC 27000-2 [6] [8] [17] y la norma Británica BS25999-1 [1] [2] [4] [11]
2. La guía elaborada por INTECO titulada “cómo implantar un plan de continuidad del negocio” [9]

[14] INTECO: Instituto Nacional de Tecnologías de la Comunicación, con sede en León España. Su misión principal es reforzar la confianza en los Servicios de la Sociedad de la Información.

3. Guía para la recuperación de desastres, desarrollada por Vision Solutions[15] [10]
4. Las Políticas de seguridad de la información de la Universidad Tecnológica nacional de Buenos Aires [16]

Así mismo se consideró diferentes opiniones y experiencias de las empresas que prestan servicios de BCM y recuperación de información; como es el caso de Deloitte, Open-Se y Expertia Continuity. También se consulto diversos extractos de congresos, publicaciones y noticias publicadas de manera electrónicas a través de; Infosecurity, Segu-Info, Usuaria, ASIS, entre otras.

Es importante destacar que el contenido del modelo propuesto no cita de manera rígida y estructurada las publicaciones antes mencionadas, simplemente es el resultado del análisis, síntesis y abstracción de la información referida.

El modelo está conformado por dos fases y el conjunto de acciones que la conforman se circunscribe en los elementos del Ciclo de Vida de la Gestión de Continuidad del Negocio.

1. Primera Fase: Deontología e Integración Organizacional

Esta fase está compuesta por dos elementos; el primero de ellos se titula "Comprender el negocio", el segundo se denomina "documentación y Socialización". El objetivo de esta fase es consolidar el sentido de identidad y compromiso entre el área de Seguridad de la Información (SI) y la Organización. Sienta sus bases en la etapa primera etapa (Comprender la Organización) del Ciclo de vida del BCM. A continuación se describe en qué consiste cada elemento que constituye esta primera fase:

[15] Vision Solutions es un proveedor a nivel mundial de software para disponibilidad y recuperación de información.

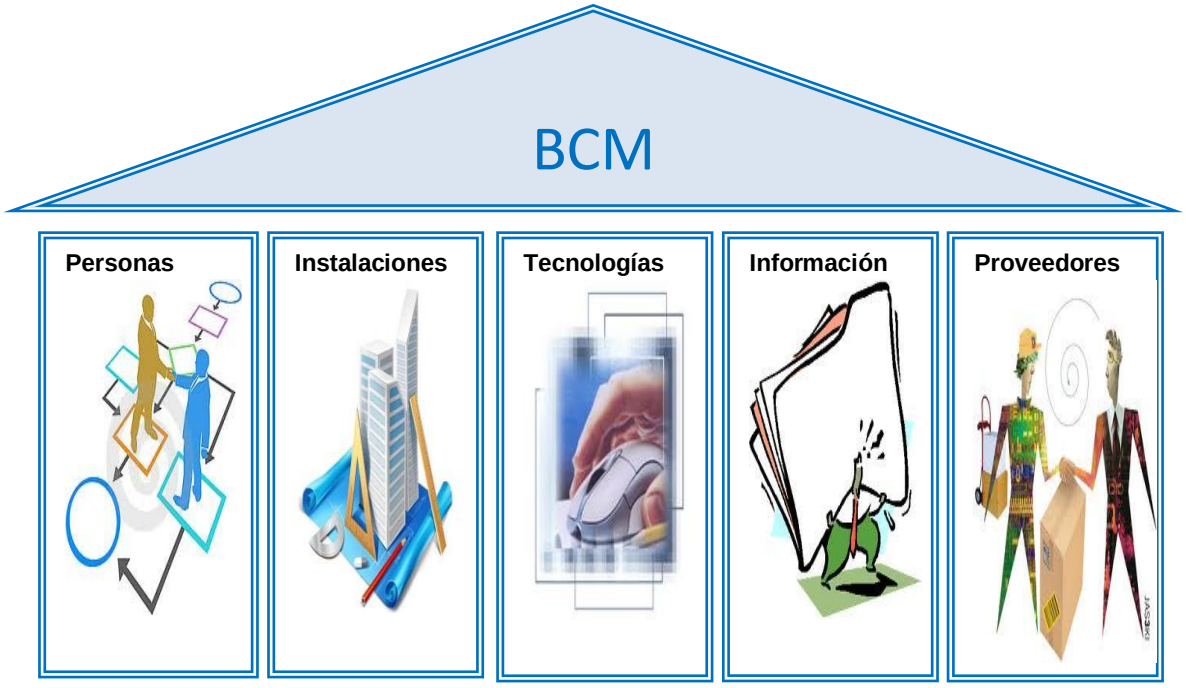
1.1 Comprender el Negocio

Uno de los errores más comunes en materia de BCM se encuentra en la priorización de las actividades propias del negocio. Esto resalta la necesidad de conocer y comprender la razón de ser del mismo y su relación directa con la información más relevante, sobre este particular el BCI sugiere plantearse las siguientes interrogantes:

¿Cuáles son los objetivos de la Organización?
¿Cómo se obtienen los objetivos del negocio?
¿Cuáles son los productos / servicios de la Organización?
¿Quién está involucrado (a nivel interno y externo) en la entrega de productos / servicios?
¿Cuáles son los imperativos de su tiempo de entrega? [1]

Estas interrogantes congregan los diferentes recursos organizacionales que subyacen en el modelo de negocio tales como; personas, instalaciones, tecnologías, información y proveedores.

Figura 6. Recursos organizacionales subyacentes en el BCM



Fuente: Guía práctica: cómo implantar un Plan de Continuidad de Negocio [9]

Acciones

Las acciones sugeridas para comprender el negocio están estrechamente ligadas con el reconocimiento; para llevar a cabo esta acción de **reconocer el negocio**, se listan las siguientes tareas, las cuales permitirán conciliar los objetivos del negocio con los objetivos del área de SI:

- ✓ Análisis del flujo de información asociado a los procesos y actividades del negocio. Para ello se recomienda realizar un flujograma, ó en caso de que las características técnicas de los sistemas informáticos lo permiten, analizar el tráfico de información.
- ✓ Identificación de la información crítica y su relación con las unidades y equipos de trabajo vinculados directamente con la misma. En este aspecto es necesario la cooperación de los responsables de procesos claves por cada área.
- ✓ Ajustar los procedimientos propios de la Seguridad de la Información (SI), a los procesos, actividades e información crítica del negocio.

1.2 Documentación y Socialización

Luego de comprender y reconocer los objetivos del negocio, así como la interrelación de sus áreas involucradas. Es necesario, concientizar, involucrar e informar a la directiva de las conclusiones que surgieron, para ello es pertinente documentar cada actividad.

Acciones

- ✓ Elaborar manuales de procedimientos para situaciones críticas, los cuales deben estar sujetos al plan de Continuidad del Negocio e involucrar a las diferentes áreas y entes (internos o externos) al negocio.
- ✓ Informar, concienciar y lograr el apoyo de la directiva al respecto de las funciones y prioridades de SI en la implementación de BCM
- ✓ Establecer de manera frecuente, canales de comunicación con las diferentes áreas de la Organización para mantener vigente las necesidades relacionadas con la seguridad de la información. En este

particular es oportuno llevar un registro de acuerdos, para ello se sugiere utilizar una bitácora de reuniones y acuerdos.

2. Segunda Fase: El rol del área de SI en la implementación de la Gestión de Continuidad del Negocio

Esta segunda fase la integran tres (3) elementos, enmarcados en las acciones que vinculan de manera operativa la SI con la Gestión de Continuidad del Negocio.

2.1 Impacto de los riesgos en la información

Es importante mantener vigente el analizáis de riesgos. Cuando se trata de información se incurre en el error de extremar las decisiones, ya sea sobreestimando el valor de la misma o restando importancia. En un proceso de BCM el tiempo de interrupción asociado a la información debe recibir el nivel de prioridad y criterio de uso en correspondencia con la interacción crítica sobre los objetivos del negocio. El enfoque de SI que propone el presente modelo ante esta identificación de riesgos no se centra en las metodologías para el análisis de riesgos, sino en aportar los datos pertinentes para que el equipo especializado pueda realizar un buen análisis de riesgos.

Acciones

Este conjunto de acciones se enmarcan en la **Identificación de los riesgos en la información**; estas están dirigidas al momento previo al proceso de análisis de riesgo, donde el rol del área de SI constituye un apoyo fundamental, a partil de cual los datos aportados desde esta instancia permiten agilidad, precisión y facilidad para la identificación y clasificación de los riesgos. Y por otra parte contribuye a la toma de decisiones en torno a aceptar, reducir, evitar o trasferir del riesgo.

Las actividades que conforman este grupo de acciones para la identificación de riesgos, dependen del cumplimiento de la primera fase y consideran:

✓ Clasificar los procesos críticos tomando como indicadores, la cultura organizacional, los objetivos, las estrategias y las áreas involucradas.

✓ Documentar todas las situaciones de riesgos, desastres e incidentes que afecten la información, bajos los controles de integridad, disponibilidad y confidencialidad. Para facilitar el relevamiento de estos datos se pueden considerar los siguientes aspectos:

a) Naturaleza de amenazas y vulnerabilidades.
b) Registro estadístico de ocurrencia de incidentes.
c) Tiempo de interrupción por causa de incidentes.

✓ Documentación y clasificación de acciones de respuestas para la recuperación de incidentes o desastres.

2.2 Recursos

Otro aspecto importante al momento poner en marcha el BCM es el control del recurso humano, tecnológico y económico, así como el tiempo estimado para la recuperación del negocio. En este punto es oportuno tomar conciencia sobre la disponibilidad de los recursos y del empleo efectivo de los mismos.

Acciones

2.2.1 Gestión de recurso humano: El involucramiento del área de SI en la Gestión de Continuidad del Negocio depende en gran medida del recurso humano. En este orden de idea es necesario:

- ✓ Designar un coordinador de Seguridad de la Información para la Continuidad del Negocio, cuya función será planificar, coordinar y supervisar las actividades necesarias para que el área de SI, se involucre de manera activa y pertinente en el BCM.
- ✓ Asignar responsabilidades para cada miembro del equipo de SI, tomando en consideración los siguientes indicadores:

a) Perfil profesional y competencias individuales.

b) Intereses particulares de cada individuo para desarrollar una actividad.
c) Interrelación y desempeño en tareas grupales.

- ✓ Generar políticas de capacitación y concientización entorno al BCM, etas deben gestarse de manera interna (del área de SI) y externa (diferentes unidades y entes involucrados). El desarrollo de estas políticas estará sujeto al modelo de negocio, no obstante se puede enmarcar en:

a) Selección de cursos de formación y mejoramiento profesional.
b) Actividades de integración, comunicación e intercambio de experiencias entre las diferentes unidades.
c) Protocolos para simulacros de riesgos.

2.2.2 Gestión del recurso tecnológico: Este es precisamente uno de los aspectos que generan confusión en lo que se refiere a límites de responsabilidades, particularmente entre las áreas de TI y SI. En algunas organizaciones esta línea diferenciadora entre TI y SI es imperceptible por motivos asociados a; estructuras de funcionamiento, espacio físico, presupuesto y decisiones Gerenciales.

El presente modelo propone partir de las siguientes premisas relacionadas con rol de SI en el BCM:

- ✓ Coordinación de esfuerzos entre los responsables del manejo de información de las diferentes áreas y especialmente con TI.
- ✓ Definir claramente los niveles de responsabilidad del área de SI en el BCM.
- ✓ Establecer políticas de control sobre:

a) Servicios de mensajería interna y externa.
b) Dispositivos de almacenamiento de información.
c) Backup.

La siguiente tabla propone la diferenciación de los niveles de responsabilidad del área de SI en la implementación del BCM:

Tabla1. Diferenciación de los niveles de responsabilidad del área de SI en la implementación del BCM

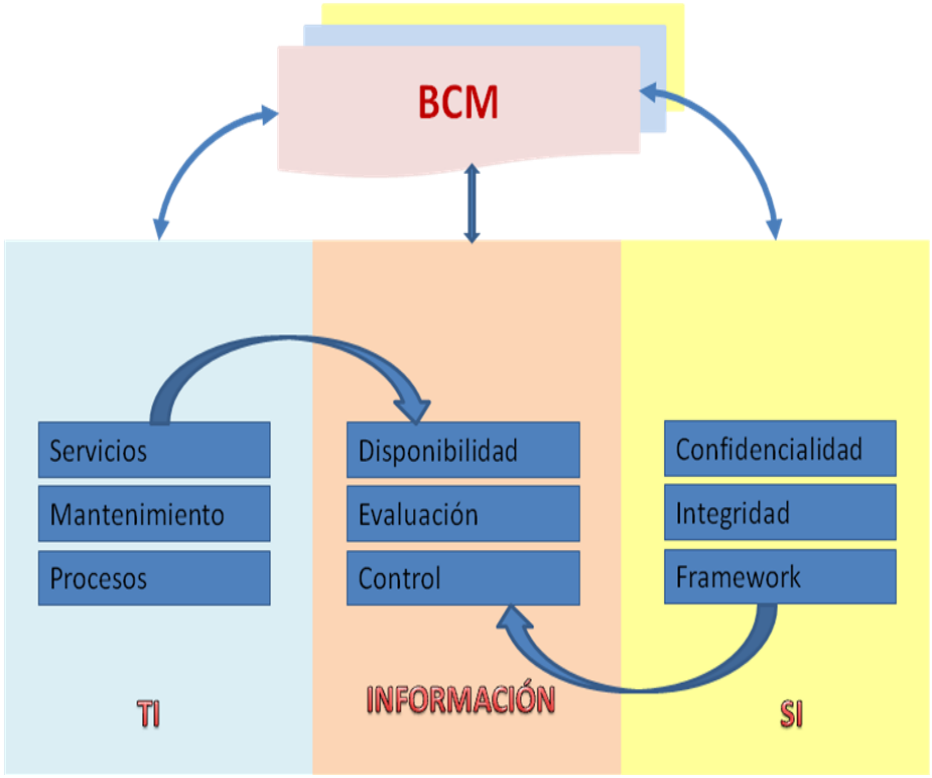
Rol de TI **Responsable de los procesos para prestar Servicios**	Rol de SI **Responsable de la gestión y control de la Información**
✓ Control de la infraestructura tecnológica. ✓ Gestión de servicios tecnológicos (mensajería, backup, sistemas informáticos, recursos, etc.). ✓ Soporte técnico. ✓ Restablecimiento de servicios tecnológicos.	✓ Framework de seguridad para infraestructura tecnológica. ✓ Políticas de control y estándares de acceso a los servicios de TI. ✓ Control de riesgos internos en SI. ✓ Control de riesgos en SI, asociados a servicios tercerizados. ✓ Programas de comunicación y concientización para la prevención y manejo de incidentes. ✓ Políticas de restablecimiento de servicios tecnológicos.

Fuente: Elaboración propia (2012)

El proceso de Gestión de Continuidad del Negocio, involucra cada uno de los recursos organizacionales, y por consiguiente su implementación demanda interoperabilidad entre las diferentes áreas, unidades y departamentos que conforman la organización. En relación al manejo y tratamiento de la información, los niveles de comunicación y trabajo en consonancia de las áreas de TI y SI, diligencian el involucramiento de esta última (SI) en el BCM.

El esquema que a continuación se presenta, resume los procesos más significativos que involucran responsabilidades compartidas entre TI y SI en el BCM.

Figura 8. Proceso compartidos entre TI y SI



Fuente: Elaboración propia (2012)

2.2.3 Gestión del recurso económico: La asignación del recurso económico es imprescindible para el desarrollo de los objetivos y actividades propias de cada una de las unidades, áreas y departamentos que conforman la organización. No obstante en lo que respecta al área de SI, lograr la asignación de este recurso representa una de las tareas que requieren mayor habilidad, estrategia y vanguardia, ya que los directivos concentran su interés en el tiempo estimado para recuperar la inversión (ROI) en lugar de invertir en algo que tal vez no sucederá.

En este orden de ideas y considerando el involucramiento de la Seguridad de la Información en el BCM, el presente modelo sugiere:

- ✓ Promover la creación de un comité para la seguridad de la información[16], con el objeto de establecer alianzas estrategias principalmente con las áreas que manejan información critica, para lograr el apoyo del cuerpo directivo de la organización. El área de SI estará representada ante este comité por el coordinador de Seguridad de la Información para la de Continuidad del Negocio.
- ✓ Alineación de los proyectos, planes y actividades del área de SI con las de TI; a fin de presentar ante la directiva una visión más completa sobre las iniciativas de seguridad.
- ✓ Proyectar las actividades de SI bajo un esquema de planificación por proyectos (PP); esto facilitara la gestión y control del recurso económico, evitando los excesos por extensión de tiempo. Así mismo dicho esquema de PP permite presentar informes de resultado al cuerpo directivo.

2.3 Implantación del BCM y la SI en la cultura organizacional

Como ya se ha expuesto en el capítulo I de la presente investigación, la Continuidad del Negocio se sustenta en la capacidad estratégica, táctica y operativa de la organización para planificar y responder ante incidentes e interrupciones del negocio y continuar sus operaciones a un nivel aceptable y predefinido [3].

Tomando en consideración que las organizaciones están conformadas principalmente por personas, lo antes expuesto implica, que del desarrollo e implementación del BCM depende de las decisiones, aptitudes y actitudes humanas dentro y en todos los niveles de la organización; este fenómeno se resume en la cultura organizacional. La cultura organizacional es la forma característica de pensar y hacer las cosas en una organización [13]

> La cultura se desarrolla en torno a los problemas que los grupos afrontan en los procesos de adaptación externa e integración interna durante su

[16] Un comité de la Seguridad de la información, según la oficina Nacional de Tecnologías de la Información (ONTI), es un cuerpo integrado por representantes de todas las áreas fundamentales de la organización.

> gestación y florecimiento, y una de sus tareas es solucionarlos en pos de asegurar la adecuación y posterior supervivencia de la organización [5].

Involucrar la seguridad de la información en el BCM, requiere implantar acciones desde dos escenario de la cultura organizacional; uno orientado hacia un estado normal y otro en situación de emergencia.

Acciones

2.3.1 En estado Normal: En este momento la cultura de la organización, alrededor de la SI debe estar orientada hacia:

- ✓ **Mantenimiento y revisión;** es necesario mantener los planes de continuidad y protocolos de emergencia, ajustados a los objetivos actuales de la organización y a las exigencias del negocio. En este punto es relevante la participación del Comité de Seguridad para consensuar las propuestas de las diferentes áreas que conforman la organización.
- ✓ **Aprender de los incidentes ocurridos;** no solo dentro de la organización, también es importante mantenerse atento a los diferentes reportes de incidentes que afectan la SI y que ocurren a nivel mundial. La idea no es crear un clima de tensión alrededor de estos eventos, sino de informar, reflexionar y hacer copartícipe al recurso humano en tomar iniciativas para minimizar las áreas vulnerables en cada estación de trabajo.
- ✓ **Prevención;** esto se logra no solo implementado políticas para respaldo de información y uso de servicios tecnológicos, sino también fomentando la socialización y compromiso en las responsabilidades en materia de SI.
- ✓ **Manejo de situaciones difíciles;** es importante que los simulacros de incidentes incluyan pruebas para el manejo y control de la SI, que trasciendan más allá de los procedimientos operativos y considere aspectos como, el desarrollo de habilidades para la toma de decisiones bajo presión.

- ✓ **Comprender y conocer;** se refiere al nivel de respuesta en SI, que se requiere ante la ocurrencia de incidentes y desastres[17].

2.3.2 En estado de Emergencia:

> Una emergencia es un suceso grave, repentino e importante, donde se producen amenazas serias e imprevistas. Evitar las emergencias es imposible, lo que debemos hacer ante ellas es tratar de paliar sus efectos y limitar sus riesgos, previniendo en la medida de lo posible, sus consecuencias [16].

Así pues, ante un estado de emergencia la continuidad del negocio esta signada por la cultura de la organización, en este sentido la SI debe:

- ✓ **Garantizar la supervivencia del negocio;** a través de la implementación de los planes dispuestos para cada caso particular.
- ✓ **Coordinación y asignación de responsabilidades;** a los grupos de contingencia, cuya participación e implementación de planes estará sujeta al impacto de la emergencia.
- ✓ **Cierre del estado de emergencia;** una vez restablecida la Continuidad del Negocio, el área de SI, debe ser la encargada de definir el momento de normalidad en relación con la información. En este punto es preciso realizar un análisis retrospectivo de los sucesos ocurridos.

Como aspecto final del modelo para asegurar el involucramiento de la Seguridad de la Información en la implementación del BCM, se presenta un cuadro resumen de los elementos y acciones que conforman el citado modelo:

[17] Un incidente es un evento que si no se controla conducirá a múltiples impactos. Un desastre es un evento no predecible, desastroso, no planificado y súbito que causa un gran daño o pérdida o también cualquier evento que crea una incapacidad de una parte de las organizaciones para proporcionar funciones de negocios críticas [5]

Figura 9. Resumen del modelo propuesto

Fuente: Elaboración propia (2012)

CAPÍTULO III

CONCLUSIONES

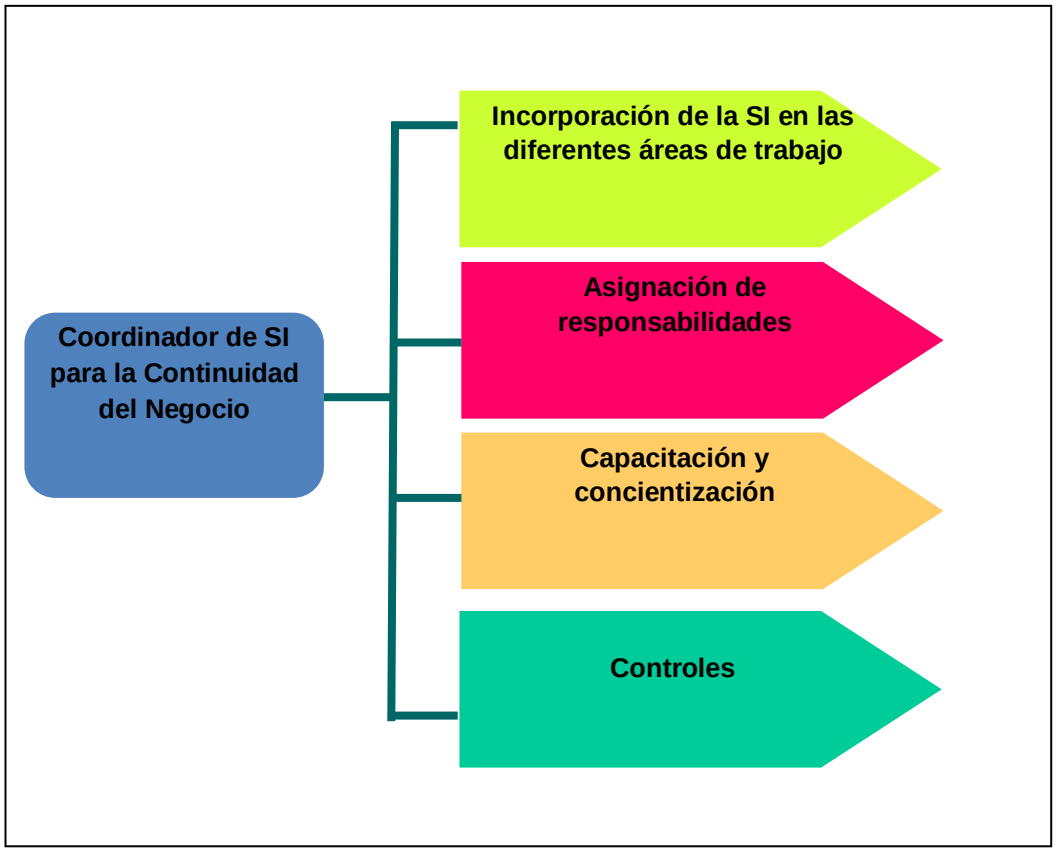
A partir de la importancia que representa hoy en día la Seguridad de la Información, como elemento neurálgico para la Continuidad del Negocio, se despliega la necesidad de marcos de referencia que definan las condiciones de necesarias para que los elementos que forman parte de la organización sean coparticipe de la Seguridad de Información en la implementación de la Gestión de la Continuidad del Negocio.

De allí que el aporte fundamental de la presente investigación se refleja principalmente el capítulo II, a través de un modelo sencillo que sirve de apoyo para hacer más expedito el involucramiento de la Seguridad de la Información en la Continuidad del Negocio. Si bien este modelo no plantea estrategias revolucionarias, ni se realizó pruebas o estudios de mercados para su elaboración; es destacable que su contenido emplea un lenguaje que puede ser fácilmente asimilado, facilitando su interpretación.

El modelo está dirigido desde el punto de vista procedimental al área de Seguridad de la Información (SI) y sirve como referente funcional para los directivos. No obstante no desvincula las diferentes áreas que conforman la organización. En este sentido es importante resaltar que el recurso humano constituye el aspecto más relevante en cuanto a la implementación de la propuesta, para ello se recomienda una secuencia de tareas basadas en el conjunto de acciones del punto 2.2.1 denominado **Gestión del recurso humano.**

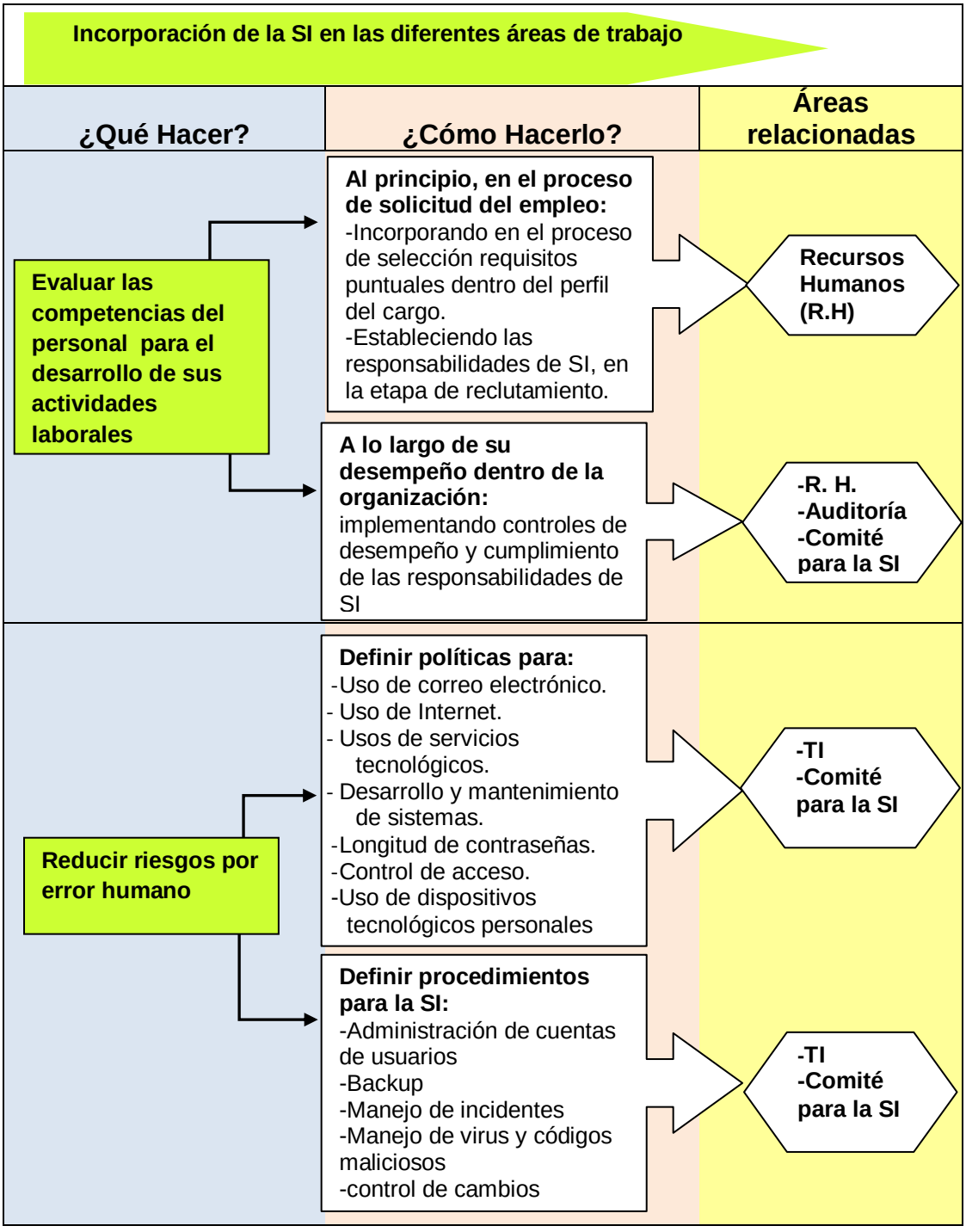
El responsable de esta implementación será el coordinador de SI para la Continuidad del Negocio. La autora ha decidido definir estas tareas a través de cinco (5) esquemas para mejor visualización:

Figura 9. Esquema para la Implementación del Modelo para asegurar el involucramiento de la Seguridad de la Información en la continuidad del Negocio



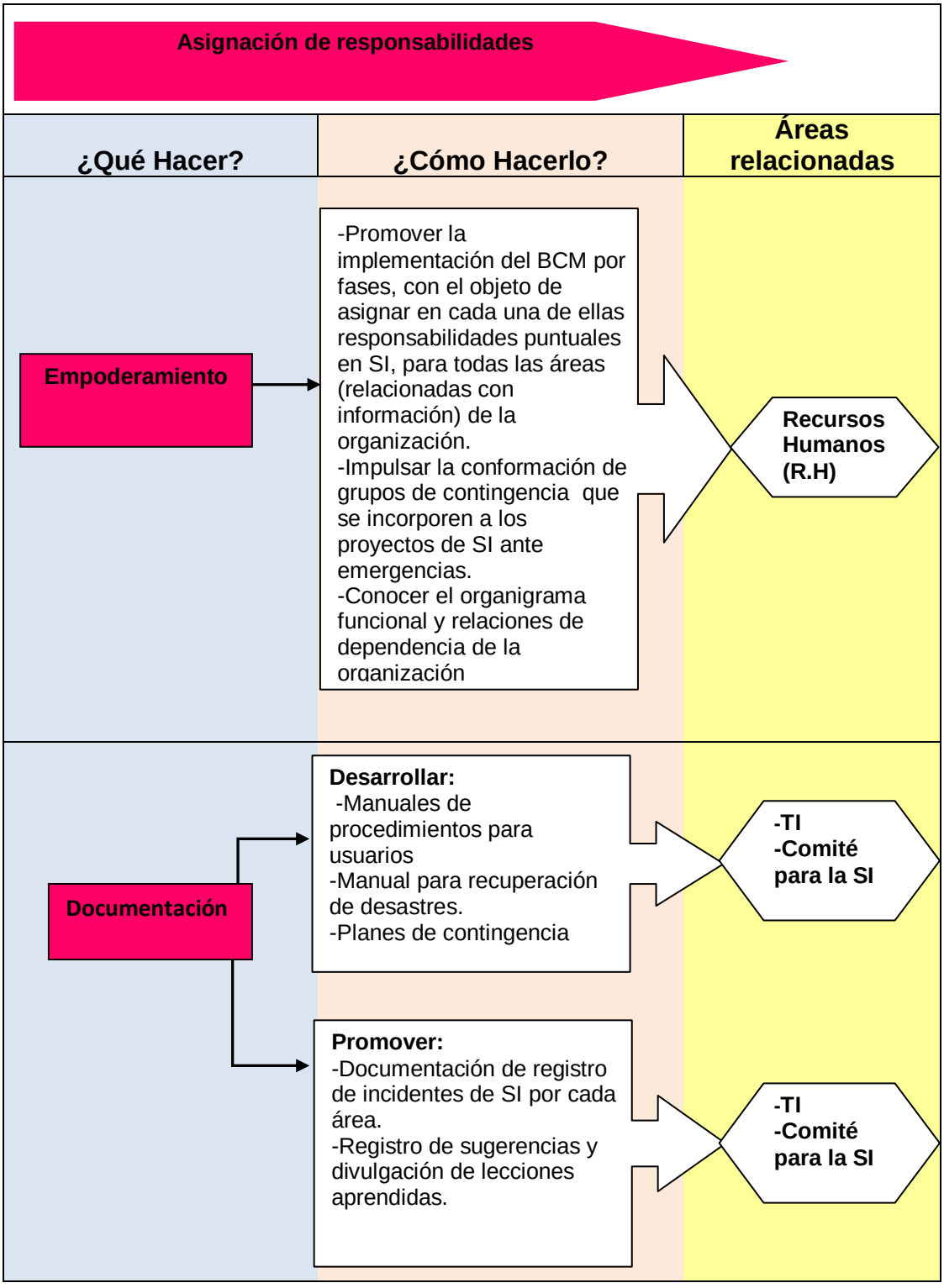
Fuente: Elaboración propia (2012)

Figura 10. Implementación del Modelo para asegurar el involucramiento de la Seguridad de la Información en la continuidad del Negocio / incorporación de la SI en la diferentes áreas de trabajo



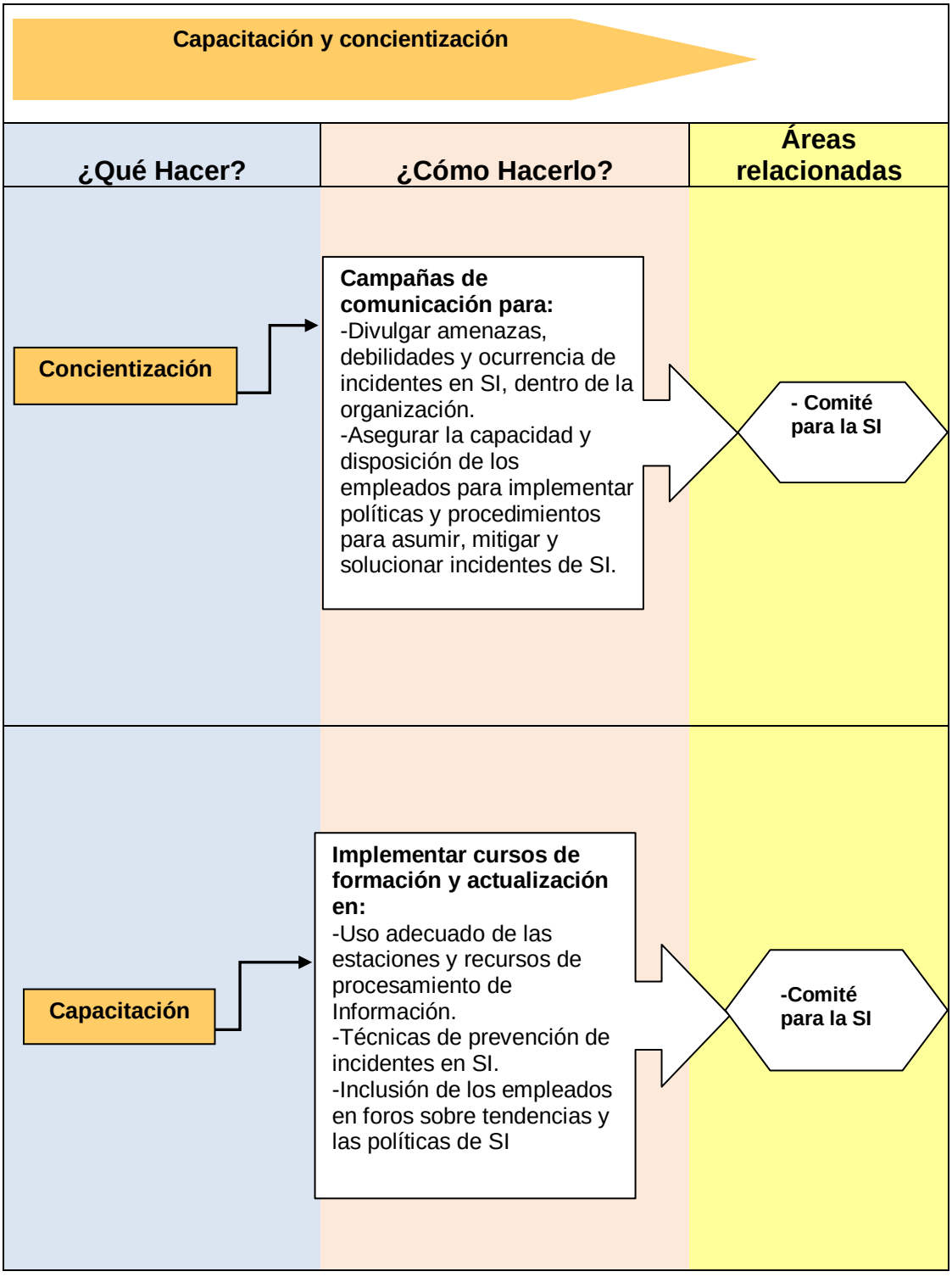
Fuente: Elaboración propia (2012)

Figura 11. Implementación del Modelo para asegurar el involucramiento de la Seguridad de la Información en la continuidad del Negocio / Asignación de responsabilidades



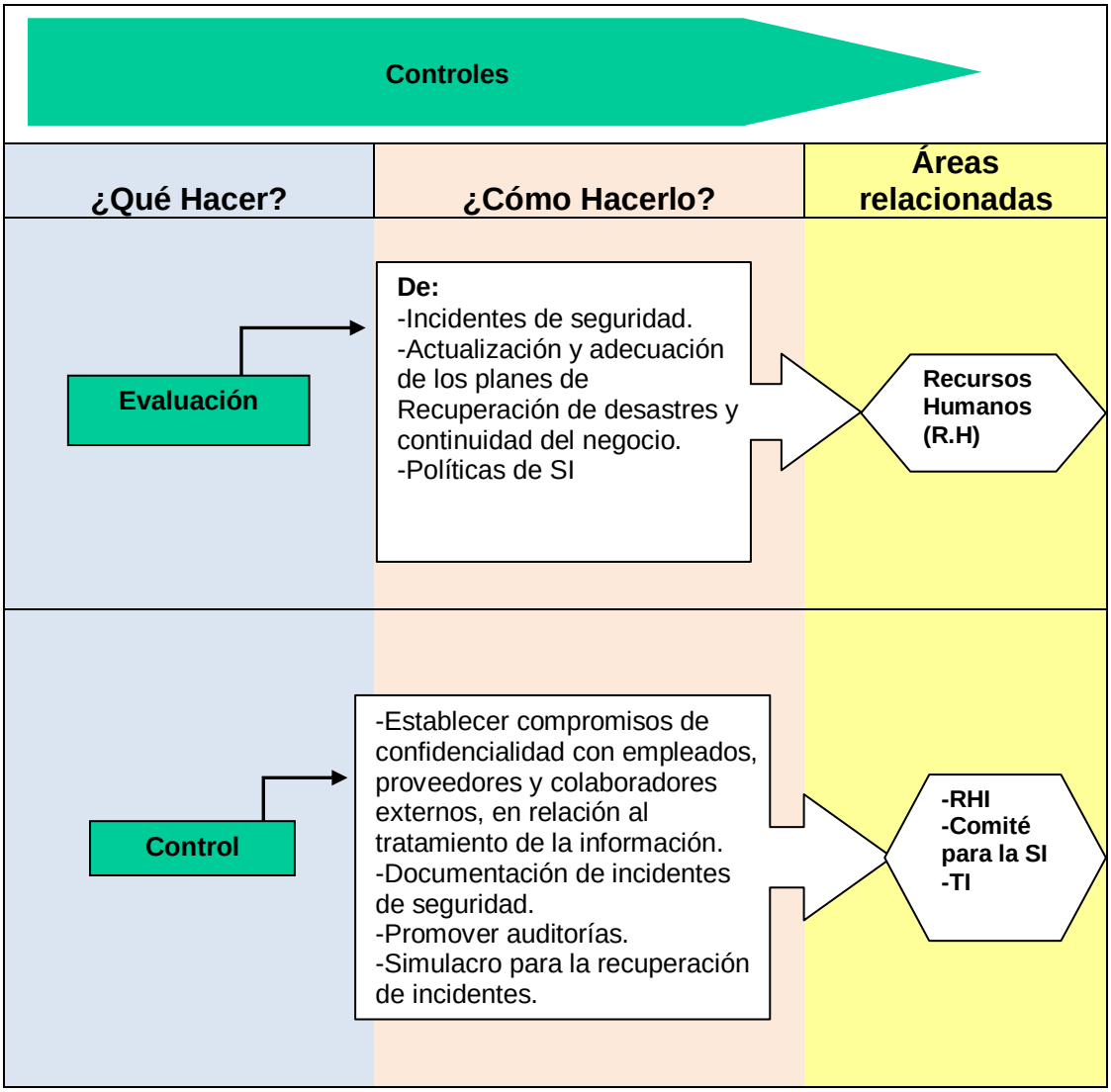
Fuente: Elaboración propia (2012)

Figura 12. Implementación del Modelo para asegurar el involucramiento de la Seguridad de la Información en la continuidad del Negocio / Capacitación y concientización



Fuente: Elaboración propia (2012)

Figura 13. Implementación del Modelo para asegurar el involucramiento de la Seguridad de la Información en la continuidad del Negocio / Controles



Fuente: Elaboración propia (2012)

Con la implementación del modelo propuesto se pretende:

- ✓ Que la organización este consciente de sus prioridades a nivel de información, así como de los tiempos de tolerancia para la recuperación de las actividades sensibles del negocio
- ✓ Que la organización comprenda de qué manera deben coaccionar los recursos organizacionales durante la implementación del BCM en función de la seguridad de la información.

- ✓ Que el recurso humano de las diferentes áreas de la organización, coadyuven para involucrar la SI en el BCM.
- ✓ Que se establezcan las atribuciones y responsabilidades de las diferentes áreas de trabajo de la organización, especialmente entre TI y SI.

BIBLIOGRAFÍA ESPECÍFICA

[1] BCI. Guía de Buenas Prácticas, www.thebci.org/gpg/GPG_Pocket_2009_Spanish.doc (consultada el 27/10/2011).

[2] BS 25999. Norma de Continuidad de Negocio. Resumen realizado por BSI, autosystem2010.wikispaces.com/file/view/Compilacion+BCM.pdf (consultada el 22/9/11).

[3] BS 25999-1 Gestión de la Continuidad del Negocio. http://www.marblestation.com/?p=650. (Consultada el 29/01/2012)

[4] BRITISH STANDARDS BS25999-2 Business Continuity Management – Part 2: Specification. United Kingdom, http://shop.bsigroup.com/en/ProductDetail/?pid=000000000030169700 (Consultada el 29/01/2012)

[5] Cultura Organizacional. http://manuelgross.bligoo.com/content/view/479296/Cultura-Organizacional-Definiciones-y-Tipologias.html#content-top. (Consultada el 11/11/11).

[6] Estándares y normas de seguridad. http://ccia.ei.uvigo.es/docencia/SSI/normas-leyes.pdf (consultada 11/11/11)

[7] Estándar de seguridad ISO/IEC 27000-1. http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf. (consultada 11/11/11)

[8] Estándar de seguridad ISO/IEC 27000-2. http://profesores.is.escuelaing.edu.co/asignaturas/sypi20071/FOLLETOS%20Y%20MATERIAL%20DE%20ESTUDIO/Introducci%F3n%20a%20los%20conceptos%20de%20Seguridad.pdf (consultada 11/11/11)

[9] Guía práctica: cómo implantar un Plan de Continuidad de Negocio, http://www.inteco.es/Seguridad/Observatorio/guias/guia_continuidad (consultada el 03/10/2011).

[10] Guía fundamental para la recuperación de desastres. http://www.eventosti.net/wp-content/uploads/2011/05/Guia-recuperacion-desastres.pdf (consultada el 03/10/2011).

[11] Gestión de Continuidad del Negocio. De BS25999 a ISO 22301. http://www.bsigroup.es/upload/NEWS/2012/PREGUNTAS%20FRECUENTES%20DE%20BS2599%20A%20ISO%2022301-v5.pdf (consultada 11/11/11)

[12] Gonzales, Vásquez, Reyes, Ramírez, Arias (2009). Gestión de la Continuidad del Negocio. http://scc2008.webs.com/Desarrollo/BS%2025999.docx (consultada el 20/09/11)

[13] Identidad Corporativa. http://www.rrppnet.com.ar/culturaorganizacional.htm (Consultada el 11/11/11).

[14] La Norma ISSO 22301 reemplazará a La BS25999-2 http://blog.iso27001standard.com/es/tag/iso-22301-es/ (consultada 11/11/11)

[15] Organizational Resilience: Security, preparedness, and continuity Management systems-requirements with guidance for use. http://www.asisonline.org/guidelines/ASIS_SPC.1-2009_Item_No._1842.pdf (consultada el 13/12/11)

[16] Plan de Intervención ante Situaciones de Emergencia. http://www.minsa.gob.pe/dgiem/cendoc/pdfs/Evacuaciones1.pdf. (Consultada el 20/03/2012).

[17] Proyecto de norma Mercosur ISO/IEC, Asociación Mercosur de Normalización, 24, (2007) pp. 10-19.

[18] Torres J. (2010). BCM Business continuity management, BS 25999, BCI. Compilación bibliográfica de la universidad de Caldas. http://autosystem2010.wikispaces.com/file/view/Compilacion+BCM (consultada el 12/08/11).

BIBLIOGRAFÍA GENERAL

Análisis de la Continuidad del Negocio en Situaciones de Crisis. http://www.conectronica.com/Seguridad/An%C3%A1lisis-en-torno-a-la-gesti%C3%B3n-de-la-continuidad-de-negocios-en-situaciones-de-crisis.html. (Consultada el 15/12/11).

Business Impact Analysis. http://www.sisteseg.com/files/Microsoft_Word_-_BIA_BUSINESS_IMPACT_ANALYSIS.pdf (consultada 10/02/2012)

NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Programs. http://www.nfpa.org/assets/files/pdf/nfpa16002010.pdf (Consultada el 20/03/2012)

NIST Sp800-34. Contingency Planning Guide for Federal Information Systems http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf (consultada 07/01/12)

Políticas de seguridad de la información. Plan de acción 2009. Universidad Tecnológica Nacional. Buenos Aires

Ureña C. (2011).Sistema de Gestión de la Continuidad del Negocio BS25999. http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/133.pdf (consultada 12/11/11)