Metodología para la Gestión de la Continuidad del Negocio

Por: Rodrigo Ferrer V.

Año: 2015

Resumen

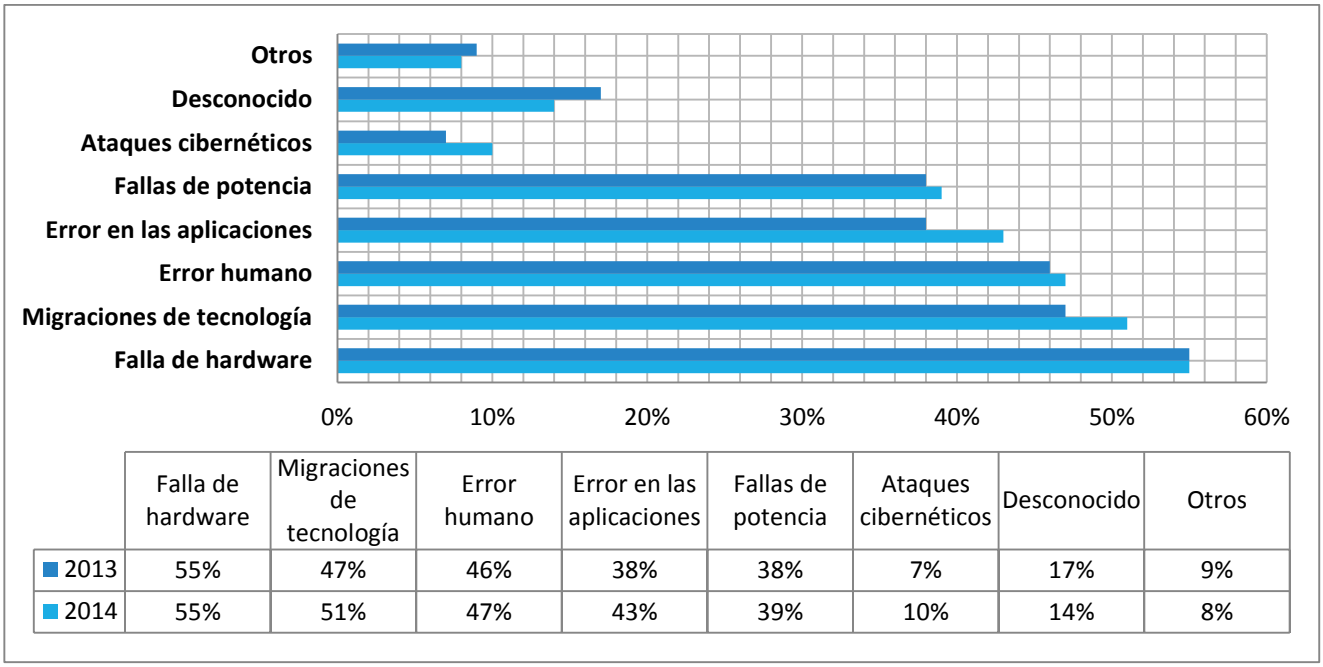
Este artículo, busca exponer los pasos requeridos para diseñar e implementar un proceso de Gestión de la Continuidad del Negocio, BCM (Business Continuity Management), por sus siglas del inglés, orientado a diversas organizaciones en Colombia. La metodología propuesta a continuación está basada en los estudios realizados por el Business Continuity Institute (BCI) y el Disaster Recovery Institute International (DRII) los cuales han sido las organizaciones líderes a nivel mundial en esta campaña de formación en los temas relacionados con la continuidad del negocio ante diferentes tipos de incidentes. La Gestión de la Continuidad del Negocio (de ahora en adelante GCN) es una parte fundamental del Gobierno y de la gestión del riesgo y se debe considerar también como un proceso permanente dentro de la organización; este proceso debe poseer una fase de planeación (Planear), seguida por la fase de implementación (Hacer), luego la verificación (Verificar) y, por último, se deben realizar mejoras sobre todo el sistema (Actuar), conformando así el conocido ciclo PHVA. La gestión de la continuidad del negocio debe ser un aspecto importante a considerar en nuestra sociedad moderna, globalizada, interconectada, con tecnologías novedosas, más complejas y, además, con una alta presencia de riesgos que en cualquier momento podrían llegar a materializarse. Por último, el BCM ha sido estandarizado en el año 2012 bajo la norma internacional ISO 22301; esta norma es hoy en día certificable y también ha servido de consulta permanente e indispensable para la realización de este artículo.

Introducción

En los últimos años, algunas entidades a lo largo del territorio nacional, han concedido una importancia creciente a la implementación de planes, procedimientos y estructuras que garanticen la continuidad de sus productos y servicios críticos del negocio ante incidentes de diversas categorías y diferentes niveles de impacto. Estos factores, junto con una legislación cada vez más exigente, (Circulares de la Superintendencia Financiera y el Marco de Referencia de Arquitectura de TI, entre otros) en lo relacionado a la confiabilidad y seguridad en la prestación de estos productos y servicios, hacen necesario en la actualidad que se cuente con una GCN, con el objetivo de lograr una sociedad cada vez más comprometida con la protección del talento humano, de la disponibilidad de los procesos del negocio, de la información (ISO 27001:2012) y del conocimiento, de la tecnología, al igual, que con el incremento de la productividad, la agilidad, la efectividad y la eficiencia.

En un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, pero las consecuencias derivadas de sucesos como el terrorismo, la inestabilidad política, las pandemias, la pérdida de empleados claves y el ciberterrorismo[1], han mostrado la necesidad de incorporar nuevas amenazas en la GCN con el fin de garantizar la continuidad de las operaciones ante un escenario cada vez más dinámico en lo relacionado con el tipo de riesgos al que se está expuesto. De acuerdo con la firma Continuity Software de los Estados Unidos, las fallas a nivel de hardware en los diferentes dispositivos que conforman los sistemas de información, por dos años consecutivos, ha permanecido en el primer lugar de acuerdo al 55% de los encuestados, le siguen migraciones de tecnología con el 51%; en el 2014, el error humano alcanzó un 47% y las fallas a nivel de las aplicaciones un 43%. Para mayor información, en la Figura No. 1, se presentan los resultados completos de la encuesta tanto para el año 2013 como para el año 2014.

[1] EL BCI Horizon Scan, evaluó 760 organizaciones a nivel mundial y comprobó que el (82%) de los líderes de continuidad temen por un ciberataque inminente. Estos ataques pueden generar unas pérdidas de alrededor de $7.6 millones de dólares por empresa y con un crecimiento anual de 10.4% en el número de estos ataques.



	Falla de hardware	Migraciones de tecnología	Error humano	Error en las aplicaciones	Fallas de potencia	Ataques cibernéticos	Desconocido	Otros
2013	55%	47%	46%	38%	38%	7%	17%	9%
2014	55%	51%	47%	43%	39%	10%	14%	8%

Figura No. 1. Causas de activación del BCM en porcentaje (fuente: Continuity Software).

¿Qué es la Gestión de la Continuidad del Negocio?

La GCN busca sostener en niveles previamente definidos y aceptados, los productos y servicios críticos del negocio a través de la estructuración de procedimientos, tecnología e información, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre, con el fin de proteger los intereses de las partes interesadas, la reputación, las finanzas, los activos críticos y otros aspectos generadores de valor.

La GCN está principalmente relacionada con las actividades que se evidencian en la siguiente figura:

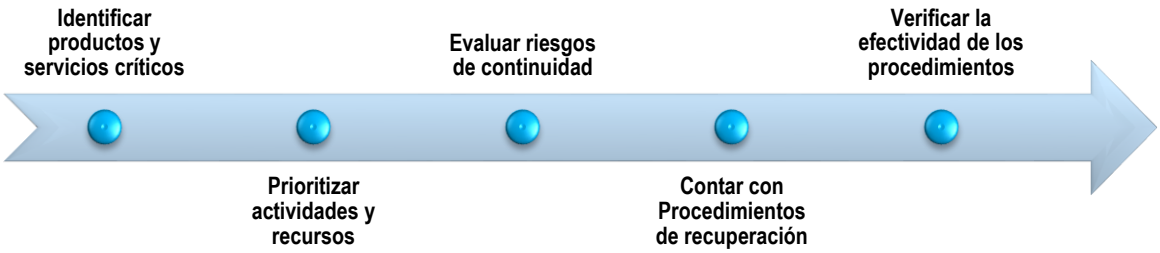


Figura No. 2. Actividades principales en el GCN.

Del análisis cuidadoso de la figura anterior, se puede afirmar que una de las actividades principales de la GCN, es la identificación de los productos y servicios críticos, ya que ellos son la razón de ser de toda organización productiva. A través de la GCN, la organización será capaz de reconocer qué necesita ser protegido para garantizar la prestación de los servicios y la entrega de sus productos. El talento humano, las edificaciones, la tecnología, la información, los proveedores, las partes interesadas y la reputación, son algunos de los elementos que deben ser considerados en las estrategias de

continuidad. La organización tendrá así la habilidad de diseñar las estrategias óptimas de recuperación cuando una disrupción se presente y, de esta manera, controlar el impacto como consecuencia de la materialización de un determinado riesgo. De modo que comprender a la organización es una parte fundamental cuando se trata de avanzar en un proyecto de GCN. En la siguiente figura siguiente, se puede observar los componentes de una organización, resaltando los elementos que deben ser considerados cuando se trata de entender el propósito y la razón de ser de una organización.

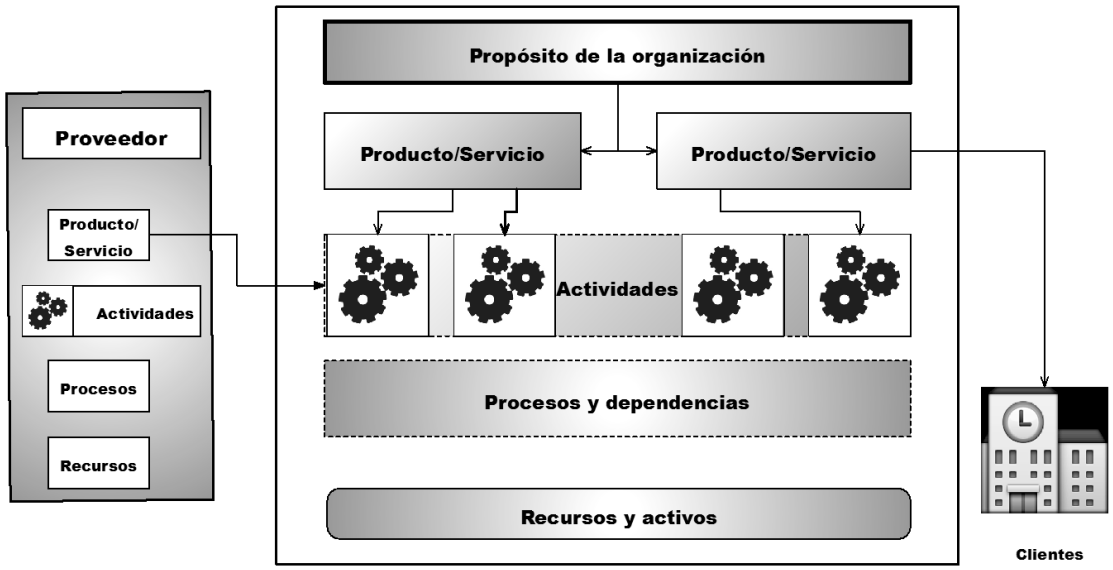


Figura No. 3. Entendiendo la organización.

Planes adicionales a la GCN

Entre los planes adicionales a la GCN, la siguiente figura, basada en la publicación especial del National Institute of Standards and Technology, NIST, SP800-34, se observa una versión holística de los diferentes tipos de planes relacionados con la atención de desastres, incidentes y emergencias, que se interrelacionan con la GCN, la complementan y la apoyan:

Figura No.4. Planes complementarios al GCN.

Del análisis inicial de la figura anterior, se puede observar la eventual conveniencia de que la GCN, se complemente con una serie de planes adicionales con funciones específicas. Sin embargo, debido a la carencia de definiciones estandarizadas para estos tipos de planes, en algunos casos, el alcance y su implementación pueden variar entre las diferentes organizaciones. Por ello, se considera conveniente, como se hará a continuación, contar con una definición precisa de cada uno de estos planes complementarios e importantes a la GCN.

- **Plan de comunicación de crisis**: este documento debe describir los procedimientos y comunicados de prensa que las organizaciones deben preparar para responder ante un incidente de manera correcta. Este plan debe estar coordinado con los otros planes de la organización para asegurar que sólo comunicados previamente revisados y aprobados sean divulgados y que solamente el personal autorizado, designado con anterioridad, sea el responsable de responder a las diferentes inquietudes que se generen y de diseminar los reportes de estado a los empleados y al público en general.

- **Planes de evacuación por edificio**: estos planes, contienen los procedimientos que deben seguir los ocupantes de una instalación o facilidad en el evento en que una situación se convierta en una amenaza potencial a la salud y a la seguridad del personal, al ambiente o la propiedad. Tales eventos podrían incluir fuego, terremoto, huracán, ataque criminal o una emergencia médica. Estos planes son normalmente desarrollados a nivel de instalación, específicos a la localización geográfica y al diseño estructural de la construcción.

- **Plan de respuesta a ciberincidentes**: este plan establece los procedimientos para responder a los ataques en el ciberespacio contra los sistemas de información de una organización. Estos planes son diseñados para permitirle al personal de seguridad identificar, mitigar y recuperarse de incidentes de cómputo maliciosos tales como: acceso no autorizado a un sistema o información, negación del servicio, cambios no autorizados a hardware, software, entre otros. Ejemplos de elementos que pueden generar incidentes de seguridad se tienen: la lógica maliciosa, los virus, los gusanos, los troyanos. Estos planes normalmente pueden pertenecer o estar integrados al Sistema de Gestión de la Seguridad de la Información (SGSI).

- **Plan de recuperación de desastres (PRD)**: este plan es conocido como DRP (Disaster Recovery Plan), por sus siglas en inglés, está orientado a responder a eventos importantes, usualmente catastróficos, que puedan afectar la prestación de los servicios de información. Frecuentemente, el DRP se refiere a un plan enfocado en TI, diseñado para restaurar la operatividad de los sistemas, aplicaciones y bases de datos, además, se cuenta generalmente con un sitio alterno en donde se realizarían las operaciones que fueron interrumpidas por el incidente en el sitio principal. El alcance de un DRP puede confundirse con el de un Plan de Contingencia de TI; sin embargo, el DRP es menos amplio en alcance y no cubre interrupciones menores que no requieren reubicación.

- **Planes de contingencia**: Según el NIST, los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y a recuperar los servicios críticos de TI después de una emergencia en un tiempo mínimo. Es posible en algunos casos contar con múltiples planes de contingencia, uno por cada componente, sistema o servicio crítico. Los planes de contingencia son de rápida activación y se puede asumir un RTO (Recovery Time Objective: Tiempo Objetivo de Recuperación), muy cercano a cero. Los planes de contingencia son típicos en los canales de comunicaciones, de tal manera que ante la falla de uno de estos canales, otro, entrará en operación muy rápidamente y en muchos casos de manera automatizada.

Metodología

La metodología recomendada en este artículo para el desarrollo de la GCN (apoyada en ISO 22301:2012), propone un proceso comprendido desde el inicio del proyecto hasta la definición de la estructura de respuesta ante incidentes. La siguiente figura presenta las fases de la metodología que se procederá a explicar:

Figura No. 5. Fases de la metodología.

Inicio del Proyecto

Esta fase se realiza con el propósito de estructurar el proyecto para la GCN, de forma tal que éste se encuentre adecuadamente organizado y controlado durante su ejecución para cumplir los objetivos estipulados de previamente. Es fundamental definir el alcance del proyecto, teniendo en cuenta los requerimientos y las capacidades del negocio. De igual manera es importante identificar las partes interesadas con el fin de considerar sus requerimientos en todo el desarrollo de la GCN.

Definir la política de continuidad

La GCN debe estar apoyada en una política claramente definida, precisa y posteriormente aprobada de manera formal. La política debe estar orientada a los propósitos de la organización, a proveer un marco de referencia para establecer los objetivos del negocio y debe incluir un compromiso para la mejora continua de la GCN; por otra parte, esta política debe ser comunicada al interior de la organización; debe estar disponible para las partes interesadas y debe ser revisada a intervalos definidos con el fin de garantizar su relevancia en relación con los objetivos del negocio.

Compromiso de la alta gerencia

Una vez se realice la aprobación de la política por parte de la alta gerencia para la realización del proyecto, se debe también validar la existencia de los recursos financieros, humanos y logísticos requeridos tanto para la etapa de diseño como para la etapa de implementación de la GCN; así como velar porque se logren los objetivos definidos al decidir implementar este proyecto. También la alta gerencia debe promover la mejora continua de todo el Sistema de la Gestión de la Continuidad del Negocio (SGCN) una vez esté implementado.

Contexto de la organización

Antes de realizar el Análisis de Impacto al Negocio (Business Impact Analysis, BIA, por sus siglas del inglés), siguiendo las recomendaciones de la norma ISO 22301:2012, la organización debe documentar e identificar los siguientes aspectos:

- Las actividades, funciones, productos, asociaciones y proveedores, además del impacto a incidentes que afecten la continuidad del negocio
- Los enlaces entre la política de continuidad y la gestión de riesgos
- Se debe determinar el apetito al riesgo de la organización y de sus líneas de negocio
- Estimar las expectativas de las partes interesadas
- Analizar el ambiente regulatorio que rodea a la organización
- Con base en lo anterior se debe actualizar el alcance de la GCN

Análisis de impacto al negocio

El Análisis de Impacto al Negocio tiene como función principal determinar los productos y servicios críticos de la organización y el impacto relacionado con su interrupción. Se recomienda realizar tres tipos de BIA, los cuales se explican en la siguiente tabla:

Tipos de BIA	Definición

BIA estratégico	Identifica y prioriza los productos y servicios más urgentes y determina los tiempos de recuperación y el impacto a la disrupción desde un punto de vista estratégico.
BIA táctico	Se determinan los procesos requeridos para la entrega de los productos y servicios críticos y se analizan los impactos por interrupciones.
BIA operacional	Se identifican y se priorizan las actividades en los procesos determinados como críticos y se determinan los recursos requeridos.

Tabla No. 1. Tipos de BIA.

De manera resumida, las principales actividades que se realizan durante el BIA son:

- Evaluar el impacto potencial de un incidente disruptivo
- Identificar las actividades que soportan la prestación de los productos y servicios
- Evaluar el impacto en el tiempo de no realizar las actividades propias del negocio
- Especificar los tiempos de recuperación
- Identificar dependencias y recursos

En la siguiente figura, se presentan los tiempos determinados como parte del BIA. El MTPD (Maximum Tolerable Period of Disruption, por sus siglas del inglés), o el Máximo Período Tolerable de Disrupción, el cual, en base a las entrevistas que se realicen, ayuda a estimar los tiempos máximos en que un producto o servicio puede estar fuera de su operación normal sin afectar la supervivencia del negocio. El RTO (Recovery Time Objective, por sus siglas del inglés), es el Tiempo Objetivo de Recuperación, el cual debe ser menor que el MTPD, y se aplica tanto para productos, procesos y recursos. Por último, se tiene el RPO, (Recovery Point Objective, de sus siglas del inglés) Punto Objetivo de Recuperación, el cual determina la máxima información que se puede perder, sin afectar la continuidad del negocio, desde que ocurre un incidente.

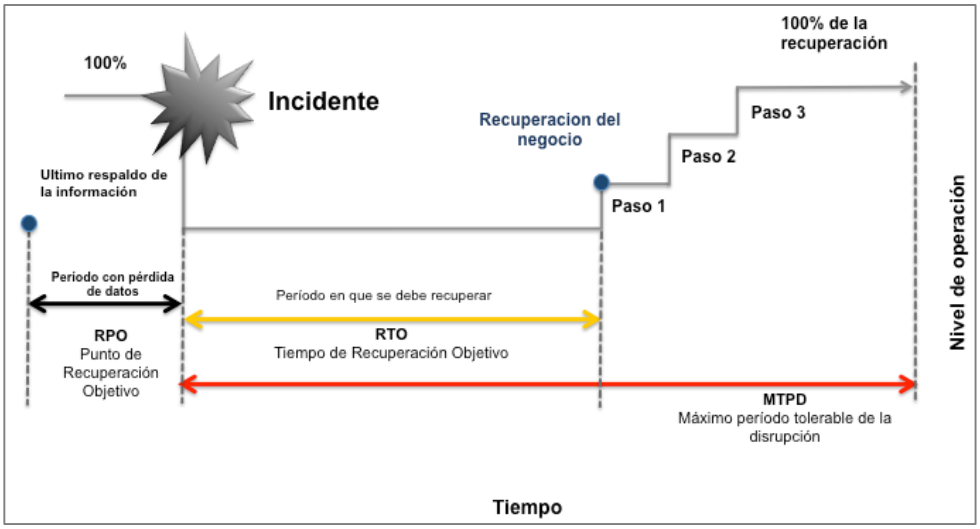


Figura No. 6 Tiempos de recuperación.

Gestión de riesgos

La fase de gestión de riesgos tiene como objetivo principal establecer, implementar y mantener un proceso de evaluación de riesgos que sistemáticamente identifique, analice y evalúe los riesgos asociados a los incidentes disruptivos en la organización. Este proceso puede ser realizado siguiendo las recomendaciones de la ISO 31000, por ejemplo, para implementar un sistema de gestión de riesgos.

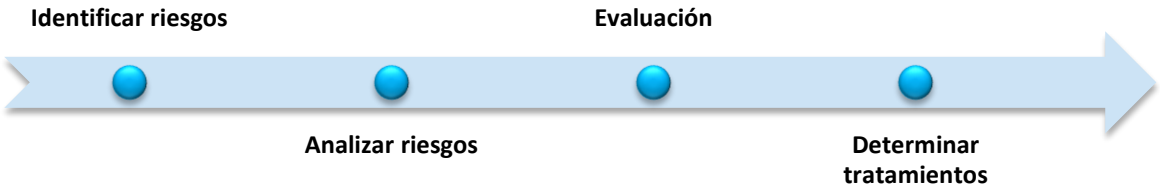


Figura No. 6. Gestión de riesgos.

Estrategias de continuidad

La fase de Estrategias de continuidad del negocio, tiene como objetivo principal analizar los diferentes esquemas o estrategias de continuidad operacional según los escenarios de riesgo definidos, de tal forma, que estas estrategias cumplan con los requerimientos reflejados por el Análisis de Impacto de Negocio y la Evaluación de Riesgos de Continuidad. Los recursos según la norma ISO 22301: 2012 que deben de ser considerados son: personas, información, edificios, equipamiento, tecnologías, transporte, finanzas, y proveedores, entre otros.

Estructura de respuesta a incidentes

La estructura de respuesta a incidentes tiene como función principal la toma de decisiones en caso de que ocurra un desastre que cause la interrupción de la entrega de los productos y la prestación de servicios críticos de la organización.

Entre las funciones principales de la estructura de respuesta a incidentes se pueden resaltar las siguientes:

- Analizar la situación para responder oportunamente
- Tomar la decisión de activar o no los planes de continuidad
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables
- Definir un presupuesto estimado para gastos que genere la crisis
- Seguir el proceso de recuperación con relación a los tiempos estimados
- Tomar decisiones ante situaciones o imprevistos durante la recuperación de operaciones
- Comunicar a los diferentes comités o equipos de la organización las decisiones que se tomen

Revisión, mantenimiento y mejoras

Llegados a este punto, se debería haber concluido lo que son las etapas de diseño e implementación. La organización debe implementar un procedimiento para revisar la efectividad de la GCN. Se deben revisar los procedimientos y planes que se tengan hasta la fecha por medio de ejercicios y pruebas. Con base en los resultados que se obtengan de estos ejercicios o pruebas, se deben realizar las correcciones pertinentes a los procedimientos, planes o estrategias. La organización debe realizar auditorías internas a intervalos regulares para revisar la conformidad del sistema. (ISO 22301, 9.2). La revisión debe ir de la mano de una supervisión continua del GCN, con el fin de obtener resultados sobre su efectividad y de esta manera proponer un plan de acción para mejorar las debilidades encontradas. Por último, pero no menos importante, se deben identificar las no conformidades, tomar acciones para corregirlas teniendo en cuenta sus causas. La organización continuamente mejorar la adecuación y la efectividad del BCMS (ISO 22301, 10.2).

Observaciones finales sobre la GCN

De acuerdo con lo anteriormente expuesto, se ha pretendido, en este artículo, por un lado, mostrar la importancia de contar con una GCN, y por el otro, entender como el estándar ISO 22301 nos da el apoyo necesario para convocar a las organizaciones a entrar en un proceso de continuidad del negocio, considerando que de esta manera se garantiza un futuro confiable a la organización y además se logra hacer una sociedad más segura y estable. La continuidad del negocio se ha comenzado a ver en muchas partes del mundo como un emprendimiento que nace de las directivas de la organización y que cuenta con un alto contenido de tipo estratégico.

Figura No. 7. Beneficios de contar con un GCN.

Por último, los beneficios, de contar con una adecuada GCN son múltiples. Las organizaciones en Colombia, debido a las constantes amenazas a las que el país está expuesto, probablemente tendrán una regulación cada vez más estricta, lo que conducirá finalmente a la adopción de la GCN por la mayoría de las organizaciones con el fin de ser cada vez más confiables, generar mejores productos y servicios y, por último, ser organizaciones globalizadas y responsables. Así, una mayor confiabilidad, mayor ventaja competitiva, disminución de costos en pólizas, adecuado cumplimiento de las leyes y las regulaciones tanto internas como externas, mejor gobierno del riesgo, junto con un mejor ambiente de trabajo y una operación mas confiable, son los beneficios esperados en mi opinión, que a manera de conclusión, se ofrecen de lo expuesto en este artículo donde se han presentado las actividades principales que deben conducir a una correcta Gestión de la Continuidad del Negocio.

Definiciones de la GCN

SANS[2]: La continuidad del negocio se refiere a las actividades requeridas para mantener su organización operando durante un periodo de desplazamiento o interrupción de la operación normal.[3]

BCI[4]: La continuidad del negocio es una colección de procedimientos e información que es desarrollada, compilada y mantenida en preparación para el uso en el evento de una emergencia o desastre.

DRI international[5]: La planeación de la continuidad del negocio es el proceso de desarrollar arreglos previos y procedimientos que capaciten a la organización para responder a un evento de tal manera que las funciones críticas del negocio continúen con los niveles planeados de interrupción o cambios esenciales.

NIST[6]: El BCM se enfoca en sostener las funciones de negocio de una organización, durante y después de una interrupción mientras se recupera paralelamente. El BCM se orienta hacia los productos y servicios críticos. Por su parte, el DRP provee procedimientos detallados para facilitar la recuperación de las capacidades en sitio alterno. Normalmente está enfocado en Tecnologías de la Información (en adelante TI) y limitado a interrupciones mayores con efectos a largo plazo. Los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y recuperar servicios críticos de TI

[2] SysAdmin, Audit, Network, Security, para mayor información consultar: http://www.sans.org

[3] Traducción del autor del documento.

[4] Business Continuity Institute, http://www.thebci.org/

[5] Disaster Recovery Institute Internacional: https://www.drii.org

[6] National Institute of Standards and Technology, Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34.

después de una emergencia. Debido a que los planes de contingencia deben ser desarrollados para cada aplicación importante o sistema de soporte, se pueden contar con múltiples planes de contingencia dentro de un BCP.

BRITISH STANDARS (BSI) & BS 25999: La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión que identifica amenazas potenciales a la organización y provee una estructura para construir confiabilidad y capacidades para una efectiva respuesta que proteja los intereses de los accionistas, la reputación, la marca y las actividades de creación de valor, también involucra la gestión de la recuperación y continuidad después de un incidente y la gestión de todo el programa por medio de entrenamientos, pruebas, y revisiones para mantener el BCM al día.

Bibliografía

Business Continuity Institute (2013) *Good Practice Guidelines: A guide to global good practice in business continuity*, Business Continuity Institute, Caversham.

Disaster Recovery Institute International (DRII) (2012) *Professional Practices for Business Continuity Practitioners*, DRII, New York.

ISO 22301 (2012) – Societal security – Business continuity management systems – Requirements

ISO 22301 (2012) – Societal security – Business continuity management systems – Guidance

ISO 22301 (2012) – Societal security – Terminology