MODELO PARA LA DEFINICIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO ENFOCADO A TI INTEGRANDO ELEMENTOS DEL MARCO PARA GOBIERNO DE TI (COBIT) Y LA GESTIÓN DE SERVICIOS DE TI (ITIL)

RICARDO ENRIQUE HERRERA HERNÁNDEZ

UNIVERSIDAD DE LOS ANDES
FACULTAD DE INGENIERÍA
DEPARTAMENTO DE SISTEMAS Y COMPUTACIÓN
BOGOTÁ D.C.
2010

MODELO PARA LA DEFINICIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO ENFOCADO A TI INTEGRANDO ELEMENTOS DEL MARCO PARA GOBIERNO DE TI (COBIT) Y LA GESTIÓN DE SERVICIOS DE TI (ITIL)

RICARDO ENRIQUE HERRERA HERNANDEZ

Trabajo de Grado presentado como requisito para optar al título de Magíster en Ingeniería de Sistemas y Computación

Director:
PhD. YEZYD DONOSO
Departamento Ingeniería de Sistemas

FACULTAD DE INGENIERÍA - DEPARTAMENTO DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

UNIVERSIDAD DE LOS ANDES

ENERO 2010

MODELO PARA LA DEFINICIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO ENFOCADO A TI INTEGRANDO ELEMENTOS DEL MARCO PARA GOBIERNO DE TI (COBIT) Y LA GESTIÓN DE SERVICIOS DE TI (ITIL)

Aprobado por:

_____
Yezyd Donoso, Asesor

_____
Olga Lucía Giraldo, Jurado

_____
Rodrigo Ferrer, Jurado

Fecha de aprobación _____

TABLA DE CONTENIDO

LISTA DE FIGURAS

INTRODUCCIÓN

Las empresas de hoy buscan obtener el mayor beneficio ante cualquier inversión que se realice, un retorno de inversión rápido y fortaleza en cada una de sus operaciones. El éxito frente a estos puntos facilitara el logro de sus objetivos y metas de negocio y de su crecimiento constante en el mercado.

Los retos que enfrentan en los mercados son diversos y de diferente magnitud. Las actividades y estrategias que se implementan para sobrellevar estos retos también tienen conllevan a un factor de riesgo incluido. Para ello las empresas buscan alinearse y aplicar los mejores estándares a nivel internacional, los cuales pueden proporcionar una guía a la mejora y al alcance de las metas organizacionales propuestas y buscar salir adelante ante estas dificultades.

Adicional a estos riesgos del mercado, existen diferentes factores internos como el logro de objetivos (alineación), obtención de beneficios, inversiones óptimas, calidad en la entrega de los productos y servicios, y factores externos como exigencias o demandas, regulaciones nacionales o internacionales, competencia en el mercado, existencias de terceras partes (clientes), los cuales dan razones para la búsqueda de soluciones que apoyen la mitigación de riesgos en el mercado y el cumplimiento de estos factores.

La adopción de este tipo de estándares proporciona un impacto positivo a nivel organizacional, a nivel económico y uno de los puntos clave es la fortaleza que la organización desarrolla en su mercado objetivo. Dentro de estas mejores prácticas definidas a nivel mundial encontramos la Gestión de Continuidad del Negocio la cual proporciona a una organización la capacidad y resiliencia para sobrellevar un incidente que afecte sus operaciones y funciones de negocio.

De acuerdo con su estructura, tamaño, objeto social y actividades de apoyo, las empresas deben definir, implementar, probar y mantener un proceso para administrar la continuidad del negocio que incluya elementos como: prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

Los planes de continuidad del negocio deben cumplir, como mínimo, con los siguientes requisitos:

a) Haber superado las pruebas necesarias para confirmar su eficacia y eficiencia.
b) Ser conocidos por todos los interesados.
c) Cubrir por lo menos los siguientes aspectos: Identificación de los riesgos que pueden afectar la operación, actividades a realizar cuando se presentan fallas, alternativas de operación y regreso a la actividad normal.

El diseño, definición e implementación del Sistema de Gestión de Continuidad del Negocio, busca asegurar la protección de personas, activos e instalaciones y su permanencia en la prestación de servicios. Volviéndolo parte de la cultura, prácticas y procesos, siendo así un sistema mucho más eficiente y con una mayor probabilidad de alcanzar los objetivos y hacerlo a menor costo.

El entendimiento de la Gestión de Continuidad del Negocio en el nivel más alto en la organización asegurará que los objetivos y las metas del planteamiento estratégico no se vean perjudicados por interrupciones inesperadas.

La Gestión de Continuidad del Negocio (GCN) es un elemento complementario con respecto al marco de gestión de riesgos que pretende entender los riesgos a que están expuestos el negocio, los productos, servicios y su operación, así como las consecuencias de dichos riesgos. A través de la GCN, la organización puede reconocer lo que debe hacerse antes de que se produzca un incidente para proteger a su personal, locales, tecnología, información, cadena de suministros, grupos de interés y prestigio. Si se cuenta con medidas de GCN apropiadas la organización puede beneficiarse de oportunidades que entrañen un riesgo elevado

JUSTIFICACIÓN

Los requerimientos de los negocios presentan cambios constantes, estos cambios se dan sobre todos los niveles organizacionales (personas, tecnología, procesos, mercados, etc.). Estos cambios en el entorno traen consigo diversos retos que exigen a las organizaciones tener un orden a su interior enfocándose siempre en el cumplimiento de estándares y regulaciones tanto a nivel internacional como nacional. Las organizaciones de todo tipo se encuentran en un proceso de mejora continua dentro del cual buscan adoptar las mejores prácticas y de esta forma encontrar una alineación entre todos los engranajes que la componen a su interior.

Uno de estos enfoques de mejora continua, pensando en mantener las actividades de la organización en producción ante cualquier falla, problema o evento se inicio con los planes de contingencia, los cuales permitían de una forma muy sencilla y simple mantener en operación a una función puntual dentro de la organización. Poco a poco y por diversos factores (nuevas tecnologías, crecimiento en la organización, nuevos requerimientos), las estrategias utilizadas hace algunos años se encuentran desalineadas con los nuevos retos y requerimientos ofrecidos por las nuevas tecnologías. Dada estas necesidades a nivel internacional y en busca de mejorar la calidad en las organizaciones, entidades como ISO, el British Standard Institute (BSI), DRI, el Business Continuity Institute (BCI), entre otros, han buscado dar pautas para formar y organizar las empresas para su mejor porvenir.

El presente trabajo busca definir un modelo para la Gestión de Continuidad del Negocio enfocada a TI, enmarcado bajo el estándar BS25999, marco de gobierno de TI proporcionado por COBIT y la gestión del servicio proporcionada por ITIL. A partir de esta integración se busca definir un modelo GRC[1] que permita la gestión a nivel de continuidad del negocio; este módelo proporcionara la interrelación de estándares conocidos a nivel mundial, tendencias a nivel de gestión y gobierno de TI.

Se espera que a partir de la definición del presente modelo, se ahonde más en el concepto de Gestión de Continuidad del Negocio y la gestión de la misma teniendo como base principal las Tecnologías de Información.

[1] Gobierno, Riesgo, Cumplimiento

1 OBJETIVOS

1.1 Objetivo general

Desarrollar un modelo de Gestión de Continuidad del Negocio relacionando las mejores prácticas para gobernabilidad de TI y gestión de servicios de TI con enfoque a continuidad.

1.2 Objetivos específicos

Desarrollar una guía detallada para la construcción y definición de un Sistema de Gestión de Continuidad del Negocio.

Identificar las relaciones del marco de trabajo para gobierno de TI (COBIT), dentro del marco de Gestión de Continuidad del Negocio definido en BS25999.

Identificar las relaciones del marco de gestión de servicios TI (ITIL) dentro del marco de Gestión de Continuidad del Negocio definido en BS25999.

Definir las responsabilidades y roles dentro del marco de Gestión de Continuidad del Negocio.

2 MARCO TEORICO

La información raíz para el desarrollo de este trabajo tiene su origen en el Código de practica BS25999-1, la especificación BS25999-2, el marco de trabajo para gobierno de TI COBIT 4.1 e ITIL v3.

2.1 GENERALIDADES DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La Gestión de la Continuidad del Negocio (GCN) es un proceso que permite a las organizaciones mejorar su preparación ante eventos inesperados mediante el establecimiento de procedimientos para recuperar los productos y servicios clave de la organización, de tal forma que se alcancen los objetivos, protegiendo al mismo tiempo los recursos (humanos y activos), la imagen y reputación de la empresa y los intereses de los inversionistas.

El proceso de GCN establece una estrategia y un marco operacional que [1]:

Proactivamente mejora la resiliencia[2] de la organización frente a interrupciones que atentan contra el alcance de sus objetivos claves.

Provea un método de prueba para recuperar la capacidad de la organización para entregar sus productos y servicios de acuerdo a un tiempo acordado de una interrupción.

Entrega una capacidad probada para manejar la interrupción del negocio y proteger el nombre y la reputación de la organización.

2.1.2 BLOQUES ESENCIALES PARA LA CONSTRUCCIÓN DE LA GCN

La Gestión de Continuidad del Negocio provee un nivel de gestión para mitigar los riesgos en las operaciones del negocio. Este proceso sistemático facilita la madurez organizacional y la resiliencia del negocio utilizando los siguientes bloques [18]:

Establece la habilidad de una organización para proveer servicio y soporte a sus clientes y para mantener su viabilidad antes, durante, y después de un evento de continuidad del negocio (desastre/crisis, natural o

Hecha por el hombre). La continuidad del negocio es solamente un punto de partida.

Este ciclo implica una metodología de mejora continua del proceso; Es el medio de asegurar que la continuidad del negocio

[2] Resiliencia, es la habilidad de recuperarse rápidamente de contratiempos o trastornos.

[3] BC: Business Continuity (Continuidad del Negocio)

está siendo gestionada y mejorada eficazmente. El ciclo se aplica a todas las partes del ciclo de vida de la GCN.

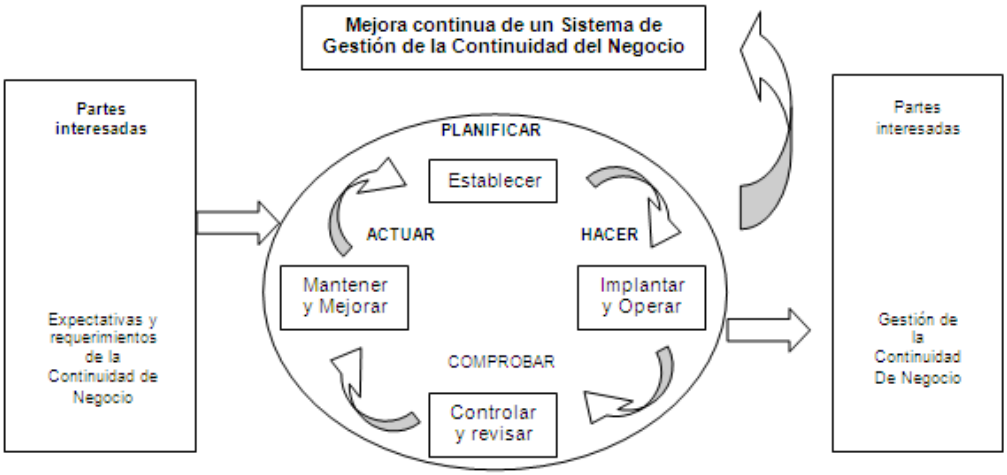

Figura No. 1 Ciclo PHVA enfocado a la Gestión de Continuidad del Negocio

Es el proceso de desarrollar y documentar acuerdos y procedimientos que permitan a una organización responder a un evento y permita retornar a sus funciones criticas del negocio de tal forma que no se cause el mayor impacto a la organización. El BCP[5] es la documentación para facilitar el proceso de mitigación de riesgo a la operación de una organización que se prepara ante la probabilidad de una crisis eventual de tal forma que no se cause un impacto significativo al negocio. Donde la Gestión de Riesgo tiende a ser preventiva, la planeación de la continuidad del negocio (BCP) fue desarrollada para manejar las consecuencias del riesgo residual. La Gestión del Riesgo cubre varias áreas que son vitales para el proceso BCP. Sin embargo, el proceso BCP va más allá de la Gestión del Riesgo y se mueve a partir de la suposición de que un desastre se hará efectivo en algún momento. Esto incluye la evaluación de cada riesgo y el establecimiento de controles de mitigación para minimizar los riesgos de mayor impacto.

La Gestión de riesgo es una aproximación estructurada para gestionar lo relacionado a amenazas, una secuencia de actividades humanas incluyendo: evaluación de riesgos, estrategias desarrolladas para manejar estos

[4] PHVA: Es una herramienta de la mejora continua, presentada por Deming a partir del año 1950, la cual se basa en un ciclo de 4 pasos: Planificar (Plan), Hacer (Do), Verificar (Check) y Actuar (Act).

[5] BCP: Business Continuity Plan (Plan de Continuidad del Negocio)

riesgos (tratamiento del riesgo), aceptación del riesgo, mitigación de riesgo usando recursos gestionados y aceptación del riesgo.

Para el desarrollo del presente trabajo se tendrá como base la propuesta del IT Governance Institute para la gestión del riesgo, tomando en cuenta el enfoque hacía la continuidad del negocio.

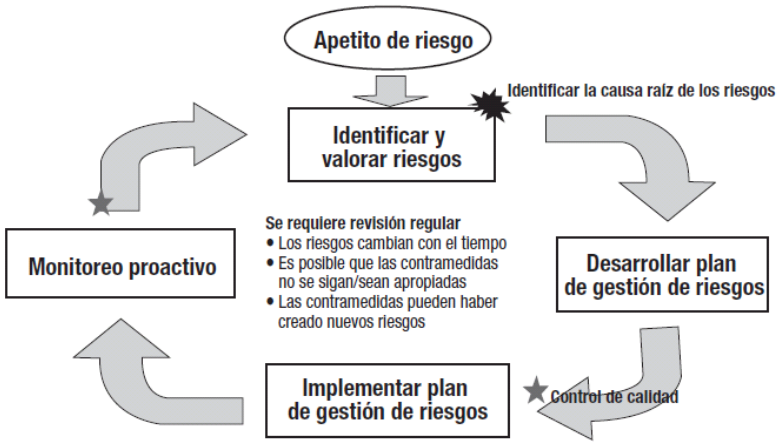

Figura 2: Procedimiento continuo de gestión del riesgo (IT Governance Institute, 2008).

Es definido como un proceso de gestión que identifica impactos potenciales que amenazan una organización y provee un marco de trabajo para construir resiliencia con la capacidad para una respuesta efectiva que salvaguarde el interés de sus principales stakeholders[6], reputación, marca, y valor creando actividades. Esta estructura de gestión incluye la facilidad de recuperación, continuidad, y/o restauración en el evento de un desastre o crisis por la gestión de un programa de contingencia y por entrenamiento, revisiones, para asegurar que los planes permanezcan activos y actualizados. Este marco de trabajo facilita el proceso entero de preparación ante una crisis que comprometa los procesos y la operación del negocio. Esto implica que la Gestión de Continuidad del Negocio puede proveer:

Un nivel de gestión al nivel organizacional apropiado que juega un papel en la continuidad de las operaciones del negocio.

Procesos de calidad que mitigan funciones de negocio críticas y sistemas soporte.

Procesos que deberían:

[6] quienes pueden afectar o son afectados por las actividades de una empresa.

Correlacionar para medir impactos financieros.

Ser clasificado acorde a su potencial de riesgo.

Incluyendo su probabilidad individual de interrupción como se refleja en la gestión de los acuerdos de nivel del servicio.

Ser cuantificables a través de medidas por métricas.

Incorporar mejora continua.

Identificar proactivamente los impactos de una interrupción en la operación.

Tener implementada una respuesta efectiva a interrupciones en la operación minimizando el impacto en la organización.

Mantener la habilidad de administrar riesgos no asegurables.

Promover el trabajo en equipo a través de la organización.

Demostrar una respuesta efectiva a través de la realización de ejercicios.

Incrementar su reputación.

Ganar una ventaja competitiva a través de la demostración de su habilidad para mantener la entrega de productos y servicios durante una situación de crisis.

2.1.3 CICLO DE VIDA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Figura No. 3 Ciclo de Vida de la GCN

Partiendo del código de práctica para la Gestión de Continuidad del Negocio definido por la norma BS25999-1 podemos definir el ciclo y el funcionamiento continuo del programa de continuidad del negocio dentro de la organización. Este funcionamiento basado en el ciclo PHVA consta de seis elementos:

Facilita tanto la capacidad de Continuidad de Negocio para establecerse como para mantenerse de una forma apropiada al tamaño y complejidad de la organización.

La gestión del programa es el corazón del proceso BCM. Una gestión efectiva del programa establece el enfoque de la organización y ayuda a alcanzar los objetivos definidos en la Política de Continuidad de GCN. Involucra tres etapas:

Asignación de responsabilidades
Implementación de la continuidad de negocios en la organización
Gestión en curso de la continuidad de negocios

Entendimiento de la Organización:

Proporciona información que permite priorizar los productos y servicios claves de la organización, recursos críticos que los soportan y la urgencia de las actividades que sean necesarias para su entrega o prestación [1]. Esto define los requisitos que determinarán la selección de estrategias de GCN apropiadas. Involucra las siguientes etapas [15]:

Análisis de Impacto al Negocio (BIA[7])
Identificación de actividades críticas
Determinación de requerimientos de continuidad
Evaluación de amenazas para las actividades críticas
Evaluación de riesgos
Determinación de medidas para tratar o mitigar los riesgos

Determinación de la Estrategia de Continuidad de Negocio:

Elegir una respuesta apropiada a cada producto o servicio, de forma que se pueda continuar entregando a un nivel operativo aceptable y en un plazo de tiempo aceptable durante o después de producirse una interrupción [14]. La elección que se haga tendrá en cuenta la capacidad de reacción y las opciones de contramedidas ya presentes en la organización [10]. Esta estrategia puede depender de:

MTPoD (Maximun tolerable period of disruption)

7

RTO (Recovery Time Objetive)
Conjunto específico de acciones a ser tomadas para soportar la estrategia
Costos de implementación de la estrategia

Las estrategias pueden involucrar:

Personas
Premisas/Restricciones
Tecnología
Información
Suministros
Stakeholders (clientes, proveedores, etc.)
Emergencia civiles

Desarrollo e Implementación de la respuesta GCN:

Creación de un marco de gestión y una estructura de gestión de incidentes, continuidad del negocio y planes de recuperación que detallen los pasos a seguir durante y después de un incidente para mantener o restaurar las operaciones [14] [11].

Incluye:

Desarrollo de una estructura de respuesta a incidentes para responder y recuperarse de una interrupción (IMT).
Desarrollo de planes ya sea que se trate de un IMP (Plan de gestión de incidentes), un BCP (Plan de continuidad de negocios) o un ARP (Plan de respuesta a actividades), estableciendo objetivos priorizados en términos de:
Actividades críticas a ser recuperadas
La oportunidad en la cual ellas necesitan ser recuperadas
Los niveles de recuperación requeridos para cada actividad crítica
La situación en la cual cada plan puede ser utilizado

Ejercicio, mantenimiento y revisión de Previsiones de GCN:

Asegurar que los preparativos de BCM son validados a través del ejercicio y revisión y que son mantenidos actualizados [12]. Consigue que la organización sea capaz de:

Demostrar la medida en que sus estrategias y planes están completos, actualizados y son correctos

Identificar las oportunidades de mejora.

Cubre las siguientes áreas de trabajo relacionadas:

Programas de ejercicios

Ejercitar los preparativos de BCM

Mantener los preparativos de BCM

Revisar los preparativos de BCM

Implantación de GCN en la cultura de la organización

Permite que la GCN se convierta en parte de los valores principales de la organización e implanta confianza entre todos los grupos de interés respecto a la habilidad de la organización para hacer frente a las interrupciones [13].

2.1.4 INTERFACES ENTRE LA CONTINUIDAD DEL NEGOCIO Y LA GESTIÓN DE RIESGO

El riesgo está presente en todas las decisiones y actividades tomadas por la organización y un número de estos riesgos pueden representar problemas en la continuidad de operaciones. La aproximación para gestionar estos riesgos de continuidad puede verse como [17]:

1. Gestionar proactivamente el riesgo en la organización sobre las bases para minimizar la probabilidad o impacto de un incidente. El proceso de Continuidad del Negocio en si puede resaltar los riesgos más significativos, que se convertirán en parte del proceso de Gestión de Riesgo.

Figura No. 4 Interfaz entre la Gestión de Riesgo y Gestión de Continuidad [17]

2. Implementar un proceso de Gestión de Continuidad del Negocio para tratar el riesgo residual. La Gestión de Continuidad del Negocio debería ser conducida como una de las salidas requeridas del programa de Gestión de Riesgo. La continuidad del negocio es una de las formas de modificar el riesgo para minimizar el impacto si el riesgo ocurre; especialmente en casos donde evitar, transferir o aceptar el riesgo no son tratamientos adecuados. Podría considerarse un método reactivo para manejar el riesgo.

ISO 27001:2005 llama a la Gestión de Continuidad del Negocio, como un método de tratamiento de riesgo, a ser considerado como medida para contrarrestar interrupciones a las actividades del negocio y para proteger procesos críticos del negocio de los efectos de fallas mayores de los sistemas de información o desastre; cabe mencionar que el Anexo A existe un dominio definido como Gestión de la Continuidad del Negocio.

En la siguiente tabla se hace una comparación entre algunos ítems importantes de la Gestión de Riesgo y la Gestión de Continuidad del Negocio:

	Gestión de Riesgo	Gestión de Continuidad del Negocio
Método clave	Análisis de riesgo	Análisis de Impacto al Negocio

Parámetros clave	Impacto y probabilidad	Disponibilidad e impacto
Tipo de incidente	Todo tipo de eventos	Eventos causando interrupción significativa del negocio
Tamaño de eventos	Todos los eventos afectando la organización	Aquellos amenazando disponibilidad de los procesos claves de la organización
Alcance	Foco principalmente sobre gestión de riesgos a objetivos core del negocio, previniendo o reduciendo incidentes	Foco principalmente sobre gestión de incidentes y recuperación de procesos críticos del negocio seguidos de un incidente.
Intensidad	Toda, de gradual a repentino	Eventos rápidos o repentinos (toda respuesta debe ser apropiada si un incidente severo se presenta)

Tabla No. 1 Relaciones clave entre Gestión de Riesgo y Gestión de Continuidad del Negocio

La Gestión de Continuidad del Negocio se relaciona con el manejo de riesgos para asegurar que a todo momento una organización pueda continuar operando al menos a un nivel de operación mínimo pre-establecido. El proceso de Gestión de Continuidad del Negocio lleva a reducir el riesgo a un nivel aceptable y da las pautas necesarias para la planeación y recuperación de los procesos de negocio.

La Planeación de Recuperación de Desastres (DRP[8]) se relaciona con la recuperación técnica de los componentes de TI y detalla los procedimientos a ser usados para restaurar estos componentes en caso de una falla. Se puede considerar al DRP como un subconjunto de actividades enmarcadas dentro del SGCN.

La Gestión de Continuidad de los Servicios de TI[9] (ITSCM[10]) asegura que las tecnologías de información e instalaciones de servicios (incluyendo computadores, redes, aplicaciones, telecomunicaciones, soporte técnico y mesa de servicios, en referencia de componentes de TI) puedan ser recuperados en las escalas de tiempo requeridas y acordadas. La mayor diferencia entre DRP e ITSCM se establece en los

[8] DRP (Desaster Recovery Plan). Plan de Recuperación de Desastres

[9] TI: Tecnologías de la Información

[10] ITSCM (IT Service Continuity Management). Gestión de la Continuidad de los Servicios de TI

requerimientos de usuarios como son tiempos de recuperación objetivos (RTO[11]), puntos de recuperación objetivos (RPO[12]) y secuencia de recuperación acordada (tomada de las dependencias, RTO y RPO para aplicaciones).Esto aumenta el servicio como su foco de recuperación hacía procesos críticos apoyando los requerimientos de continuidad del negocio. ITSCM es una de las actividades principales dentro del presente trabajo y hace parte de los lineamientos definidos en ITIL.

La siguiente figura enmarca la relación de todas las prácticas de continuidad desde el DRP, BIA, GCN y la Gestión de Riesgo en una organización;

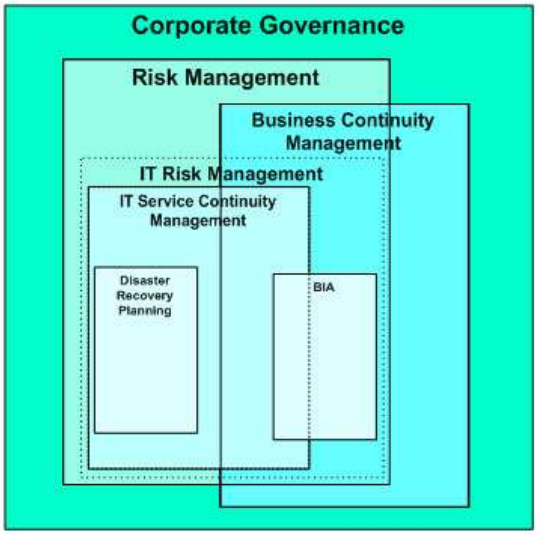

Figura No. 5 Relación de disciplinas relacionadas con continuidad [17]

2.2 GOBIERNO DE TECNOLOGÍAS DE INFORMACIÓN

Para muchas organizaciones, la información y la tecnología que las soporta represente su activo de más valor pero muchas veces el menos entendido y menos cuidado. Las organizaciones exitosas reconocen y saben sobre la contribución y los beneficios de las Tecnologías de Información (TI) y las usan para direccionar y agregar valor a su negocio y a sus principales socios (stakeholders) [3].

La necesidad para la evaluación sobre el valor de TI, la gestión de los riesgos relacionados a TI y el incremento de requerimientos para control sobre la información

[11] RTO (Recovery Time Objetive). Tiempo de Recuperación Objetivo

[12] RPO (Recovery Point Objetive). Punto de Recuperación Objetivo

son ahora entendidos como elementos claves del gobierno de la empresa. Valor, riesgo y control constituyen el core del gobierno de TI.

El gobierno de TI se considera como responsabilidad del staff más alto en la organización (ejecutivos, alta dirección, lideres) y consiste del liderazgo, las estructuras organizacionales y los procesos que aseguran que las TI de la empresa sostengan y extiendan a los objetivos y estrategias de la organización. El Gobierno de TI provee la estructura que une los procesos y recursos de TI, y la información con la estrategia y los objetivos de la empresa; además, integra una serie de mejores prácticas relacionadas con el ciclo de vida de TI para asegurar que la información que la empresa requiere para alcanzar sus objetivos es entregada por dicha área.

Por lo tanto, el gobierno de TI integra e institucionaliza buenas prácticas para asegurar que las TI de la empresa soporten los objetivos de negocio. El gobierno de TI habilita a la empresa a tomar ventaja de su información, por lo tanto maximizando beneficios, capitalizando en oportunidades y ganando ventaja competitiva; tomando en cuenta que las organizaciones deben cumplir con requerimientos de calidad, fiduciarios y de seguridad, tanto para su información, como para sus activos, la administración debe asegurar que los sistemas de control interno o el marco de referencia están funcionando y soportan los procesos del negocio y debe tener claridad sobre la forma en que cada actividad individual de control satisface los requerimientos de información e impacta los recursos de TI.

Los Objetivos de Control de Información y las Tecnologías Relacionadas (COBIT), proveen mejores prácticas a través de un marco de referencia de los procesos y presentan actividades en una estructura manejable y lógica que ayudan a optimizar el empleo de la información y proporcionan un mecanismo de medición que permite juzgar cuando las actividades van por el camino equivocado [3]. COBIT provee controles de TI y métricas de TI, sin embargo al ser un marco de trabajo de alto nivel es usado como mecanismo de entrega y describe lo que se debe hacer (what?) y no define exactamente el cómo desarrollar (How?) o poner en marcha lo definido; adicionalmente para el enfoque del presente trabajo no tiene una fortaleza en a nivel de continuidad.

En la siguiente figura se ejemplifica la forma como COBIT busca integrarse a la estrategia y objetivos de negocio en la organización:

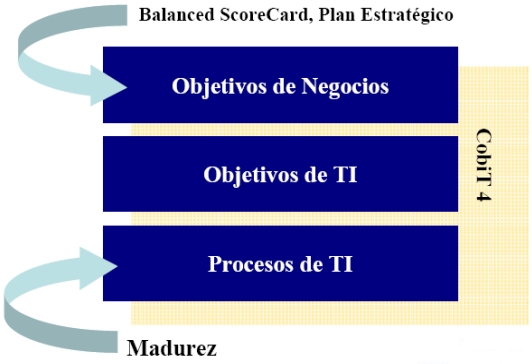

Figura No. 6 Integración de TI con el Negocio [3]

Sin embargo, debido a que es de alto nivel, amplia cobertura, y porque es basado en muchas prácticas existentes, COBIT puede actuar como un integrador entre mejores prácticas ayudando a enlazar estas prácticas hacia el logro de los objetivos estratégicos del negocio.

El marco definido por COBIT establece 34 procesos para administrar y controlar la información y la tecnología que la soporta. Los procesos se dividen en cuatro dominios:

Planear y Organizar—Este dominio abarca la estrategia y las tácticas, y se encarga de identificar la forma en la cual las TI pueden contribuir mejor a alcanzar los objetivos de negocio. Es más, la realización de la visión estratégica necesita planearse, comunicarse y administrarse para diferentes perspectivas. Por último, es preciso contar con una organización y una infraestructura tecnológica apropiadas.

Adquirir e Implementar—Para concretar la estrategia de TI, es necesario identificar, desarrollar o adquirir soluciones de TI, e implementarlas e integrarlas en el proceso de negocio. Además, este dominio cubre los cambios y el mantenimiento de los sistemas existentes para garantizar la continuidad del ciclo de vida para estos sistemas.

Prestación del servicio y Soporte—Este dominio se encarga de la prestación efectiva de los servicios requeridos, que van desde operaciones tradicionales pasando por los aspectos de seguridad y continuidad hasta la capacitación. A fin de prestar los servicios, se tienen que establecer los procesos de soporte necesarios. Este dominio incluye el procesamiento real de datos por parte de

sistemas de aplicación, que a menudo se clasifican como controles de aplicación.

Monitorizar y Evaluar—Todos los procesos de TI deben valorarse de manera periódica para determinar su calidad y cumplimiento con los requerimientos de control. Este dominio, por tanto, trata la monitorización y la evaluación del desempeño de TI y mayor control por parte de la gerencia, garantizando el cumplimiento regulatorio y brindando vigilancia del gobierno de TI.

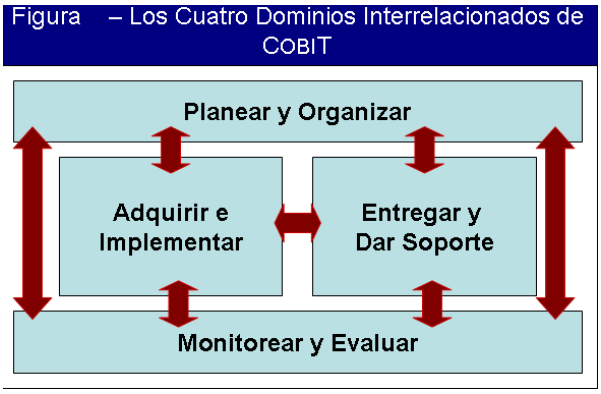

Figura No. 7 Integración de TI con el Negocio [3]

COBIT funciona provee las herramientas necesarias dentro del presenta trabajo para la definición del marco de gobierno y control de TI en la adopción e implementación de un SGCN basado en el estándar BS25999; las mejores prácticas en gestión de TI son proporcionadas por ITIL.

2.2.1 MODELOS DE MADUREZ

El modelo de madurez para la administración y el control de los procesos de TI se basa en un método de evaluación de la organización, de tal forma que se pueda evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel de optimizado (5). Este enfoque se deriva del modelo de madurez que el Software Engineering Institute definió para la madurez de la capacidad del desarrollo de software [3].

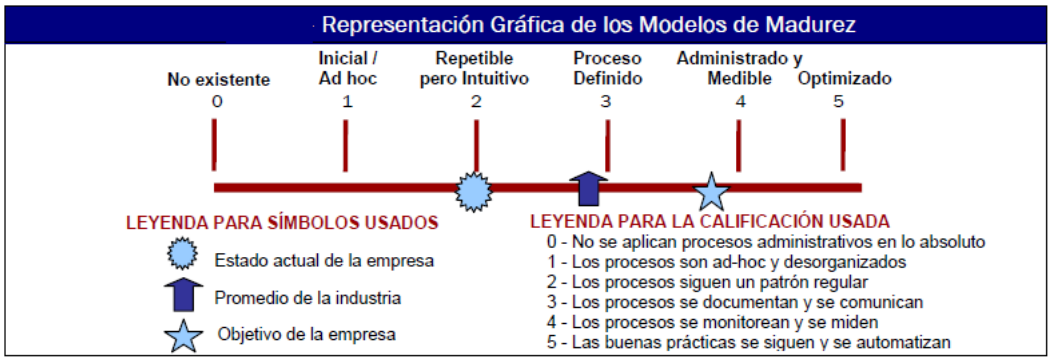

Figura No. 8 Modelo de madurez para los procesos de COBIT [3]

2.2.2 DRIVERS PARA LA IMPLEMENTACIÓN DE LA GUÍA, INCLUYENDO SITUACIONES TIPICAS

COBIT usualmente es implementado sujeto a uno o más de los siguientes requerimientos o casos en la organización:

Existe una necesidad para Gobierno de TI.

Los servicios entregados por TI no están alineados con las metas de negocio.

Es necesario un marco de trabajo para los procesos de TI.

Es necesario un marco de trabajo para gestionar la calidad para TI.

Una estructura para auditoria debe ser definida.

Parte de la función de TI esta en outsourcing.

Cumplimiento con requerimientos externos (regulaciones, organizaciones o terceras partes) son motivo de preocupación.

2.2.3 RIESGOS DE NO IMPLEMENTAR COBIT

Entre los riesgos de no implementar Gobierno de TI y COBIT se incluye:

Servicios de TI no alineados.

Soporte débil a las metas del negocio debido al no alineamiento de los servicios de TI.

Percepción de TI como una caja negra.

Costo excesivo de TI.

Decisiones erróneas de inversión en TI.

Brechas a nivel regulatorio con penalidades financieras significativas.

2.3 GESTIÓN DE SERVICIOS DE TI

La Biblioteca de Infraestructura de Tecnologías de Información, frecuentemente abreviada ITIL (del inglés Information Technology Infrastructure Library), es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI). ITIL resume un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI. Estos procedimientos son independientes del proveedor y han sido desarrollados para servir como guía que abarque toda infraestructura, desarrollo y operaciones de TI [21].

El objetivo primario de la Gestión de Servicio es asegurar que los servicios de TI están alineados a las necesidades del negocio y que las soporte activamente. Es imperativo que los servicios de TI apoyen los procesos de negocio, pero es también importante que las TI actúen como un agente para el cambio y faciliten la transformación del negocio [5].

Hoy, las organizaciones son dependientes de TI para satisfacer sus objetivos corporativos, conocer sus necesidades del negocio y entrega de valor a sus clientes. Para que esto ocurra en una forma gestionable, medible y repetible, el negocio debe asegurar la alta calidad de sus servicios de TI [22]. Estos servicios deben:

Alinearse con las necesidades del negocio y requerimientos de usuario
Cumplimiento con legislación
Efectiva y eficiente entrega
Revisión y mejora continua

La Gestión de Servicios de TI se relaciona con planear, proveer, diseñar, implementar, operar, soportar y mejorar los servicios de TI que son apropiados a las necesidades del negocio. ITIL provee un marco de trabajo comprensivo, consistente y coherente para la Gestión de Servicios de TI [22].

ITIL: Revisión y beneficios

ITIL provee una aproximación a la gestión de la provisión de servicios de TI. Dentro de los beneficios que se obtienen adoptando ITIL tenemos:

Reducción de costos.

Mejora de servicios de TI a través del uso de mejores prácticas.
Mejora en la satisfacción del cliente a través de una aproximación a la entrega de servicios.
Guía y estándar.
Mejora de la productividad.
Mejor uso de habilidades y experiencia.

2.3.1 DRIVERS PARA LA IMPLEMENTACIÓN DE LA GUÍA, INCLUYENDO SITUACIONES TIPICAS

ITIL usualmente se implementa sujeto a uno o más de los siguientes requerimientos o casos:

Establecer procesos de servicio como una función empresarial de TI o una organización de proveedores de servicios de TI.
La calidad de los servicios necesita ser definida y mejorada.
Existe la necesidad de enfocarse en el cliente y usuarios de los servicios de TI.
Existe la necesidad implementar una gestión de servicios de TI.

2.3.2 RIESGOS DE NO IMPLEMENTAR ITIL

Se pueden mencionar algunos riesgos al no tener un proceso de gestión de servicios de TI como ITIL:

Servicios ineficientes que se proveen a usuarios y clientes.
Servicios y procesos de TI no claros y definidos.
Comunicación ineficiente y poco efectiva sobre objetivos de entrega de servicios.
No existe la satisfacción por parte de usuarios y clientes con los servicios que el área de TI proporciona.

2.3.3 DESCRIPCIÓN DE LA GUIA Y SU CONTENIDO

Los cinco libros que conforman ITIL v3 son [4]:

Estrategia del Servicio (SS): Cubre la planeación estratégica de las capacidades de gestión de servicio y la alineación de servicio con la estrategia del negocio. Provee una guía sobre creación de valor, mercado, estrategia de entregas, estructura de servicios,

tipos de proveedores de servicios, desarrollo organizacional, gestión financiera. Los procesos manejados son: Gestión de la demanda, generación de estrategia, Gestión del Portafolio de Servicios y Gestión Financiera de TI.

Diseño de Servicio (SD): Cubre el diseño y desarrollo de servicios y procesos de gestión de servicio. Los procesos cubiertos por este dominio son Gestión del Catalogo de Servicios, Gestión de Niveles de Servicio, Gestión de la Capacidad, Gestión de la Disponibilidad, Gestión de la Continuidad de los Servicios de TI, Gestión de la Seguridad de la Información y Gestión de Proveedores.

Transición del servicio (ST): Ilustra como los requerimientos de etapas previas (estrategia y diseño) son realizados y como las capacidades para la entrega de un servicio pueden ser mantenidas. Los procesos cubiertos son Planeación de la Transición y Soporte, Gestión del Cambio, Gestión de la Configuración, Gestión de la Revisión e Implementación, Validación de Servicio y Prueba y Evaluación y Gestión del Conocimiento.

Operación del servicio (SO): Cubre la entrega efectiva y eficiente y soporte de servicios, y provee una aproximación para la Gestión de Eventos, Gestión de Incidentes, Cumplimiento de la Solicitud, Gestión de Problemas y Gestión de Acceso.

Mejora Continua del Servicio (CSI): Cubre la mejora del servicio y la medida del desempeño de los procesos requeridos para el servicio. Hay tres áreas claves: medición del servicio, reporte de servicio y mejora del servicio.

3 DESARROLLO METODOLOGICO PARA EL SGCN

A través de este documento se pretende definir una metodología que permita la implementación de un SGCN con la integración de un marco de gobierno de TI y uno de Gestión de TI. El punto de partida lo proporciona el estándar BS25999-1 de acuerdo al ciclo de gestión PHVA para la Continuidad del Negocio. En la figura No. 6 se definen las fases sobre las cuales se hará énfasis en el presente trabajo; etapas para la definición e implementación de un SGCN. Las actividades claves dentro de la implementación de un SGCN se ilustran en la siguiente figura:

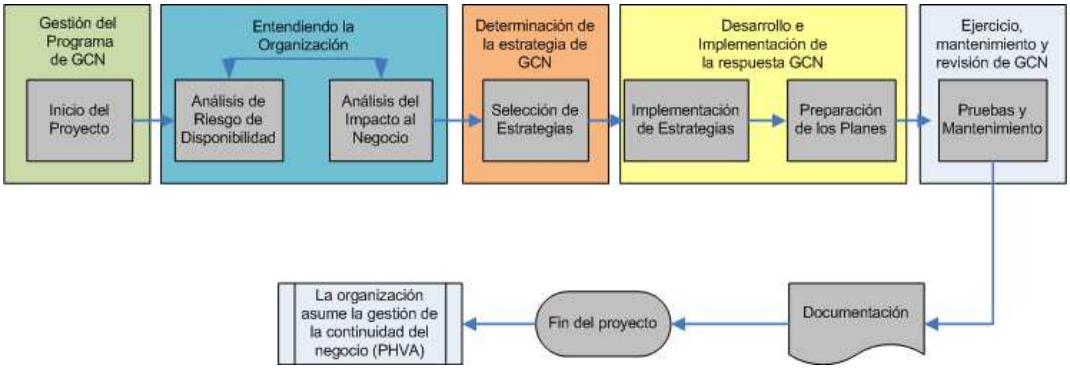

Figura No. 9 Pasos para la implementación de un SGCN

La siguiente figura amplia la visión de las actividades a desarrollar dentro de la implementación del SGCN. Cada una de las etapas de acuerdo al estándar BS25999-1 define unas actividades que serán detallas en cada sección del presente documento.

Fases y Pasos Asociados

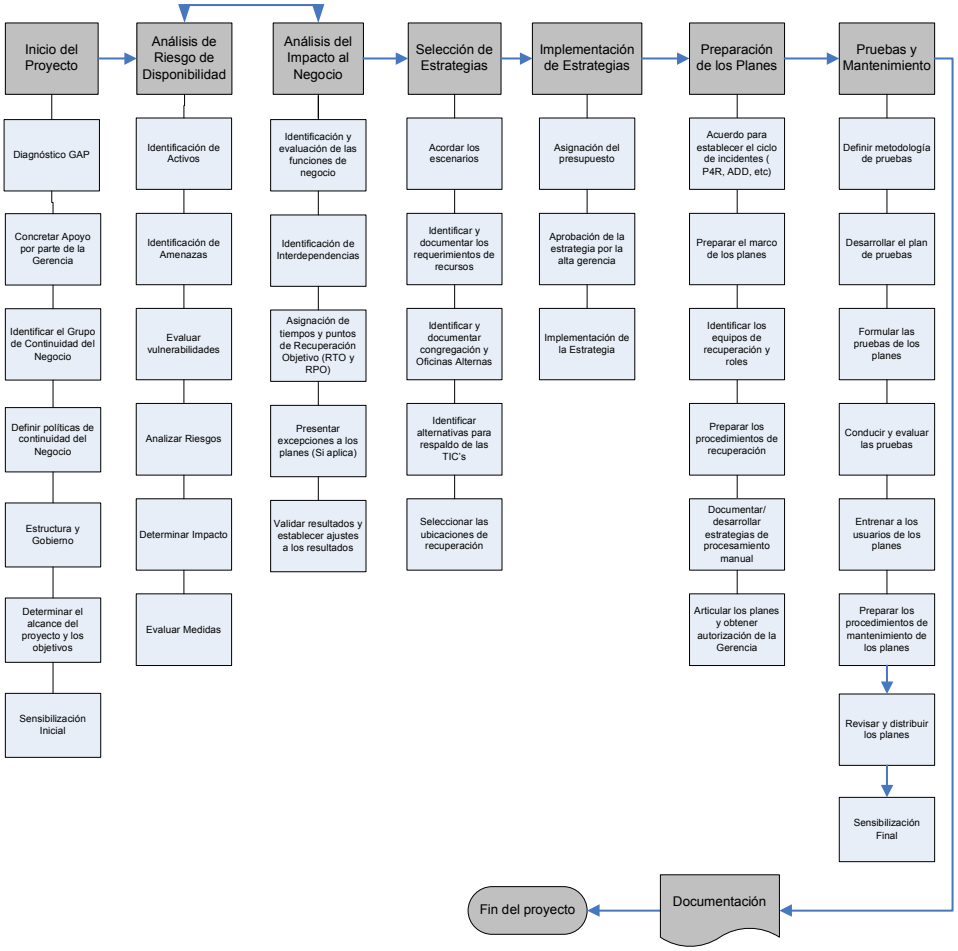

Figura No. 10 Fases detalladas para la implementación de un SGCN

3.1 ALINEACIÓN ESTRATEGICA HACIA LA GCN

Como punto inicial antes de iniciar con el establecimiento del sistema de gestión es necesario contar con un conocimiento completo de la organización, metas de negocio, objetivos de negocio, visión, su estrategia, la importancia de las TI y el impacto de las mismas en los procesos operacionales del negocio.

La GCN busca garantizar la continuidad de las operaciones de la organización protegiéndola de los riesgos asociados a eventos que atenten contra los activos de la empresa (personas, infraestructura, etc.). Es necesario tener un conocimiento sólido sobre cómo funciona la organización a su interior, definición de procesos, interdependencia de los mismos y con la tecnología.

3.2 GESTIÓN DEL PROGRAMA DE GCN

3.2.1 FASE DE INICIO DEL PROYECTO

Puede ser considerada la fase clave dentro del Sistema de Gestión de Continuidad del Negocio. En esta fase se detalla tanto el compromiso de las altas directivas de la organización, los recursos con los que se contara, la estructura organizacional y de gobierno, objetivos y alcance del sistema.

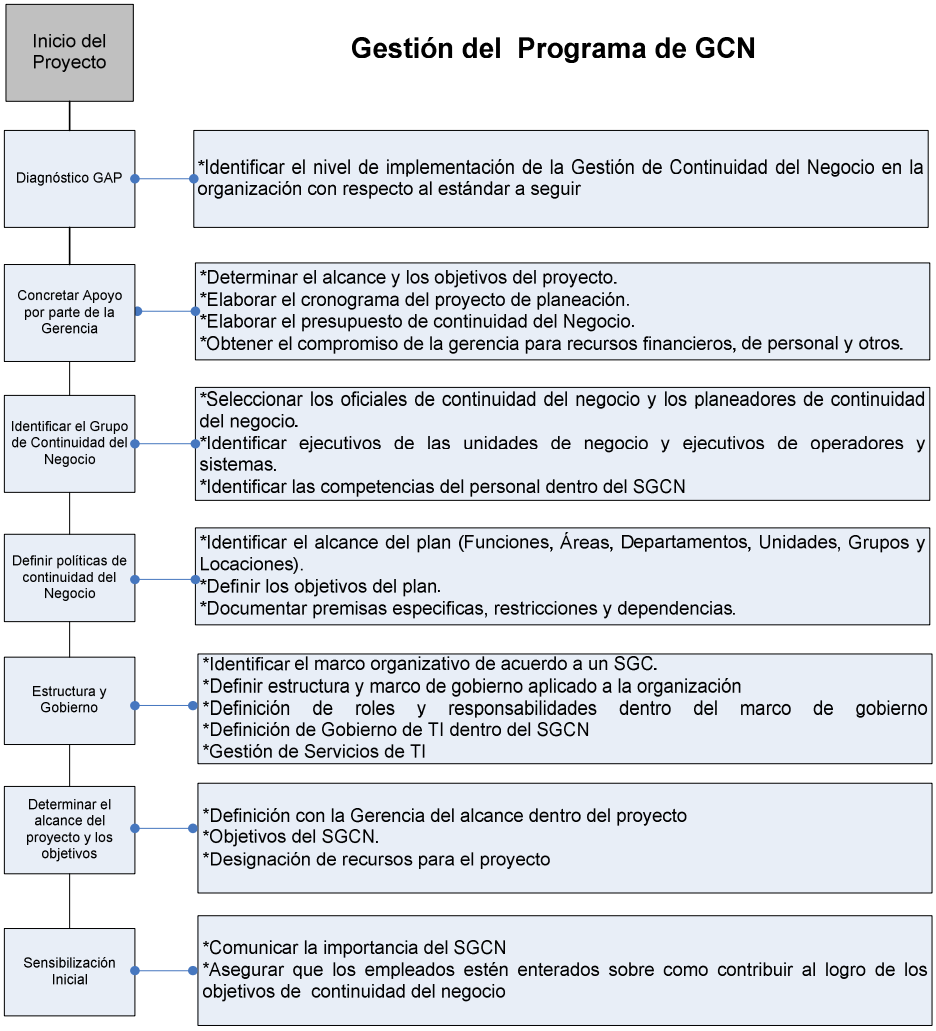

Figura No. 11 Fase Inicio del Proyecto

3.2.2 PREPARÁNDOSE PARA LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Para incluir la Continuidad del Negocio dentro de la cultura de una organización es importante establecer una estructura definida responsable por el desarrollo de actividades que permitan concientizar al personal e incrementar su compromiso con el programa. Sin embargo, muchas empresas sólo contemplan la creación de un grupo de Gestión de Continuidad del Negocio una vez que el programa comienza a operar y se hace evidente que el mantenimiento y la operación del mismo requiere un esfuerzo adicional.

Dentro del marco de la presente metodología se definirá una estructura a nivel organizacional y la definición de un marco de gobierno que será la base para iniciar con la definición y desarrollo del Sistema de Gestión de Continuidad del Negocio; esta estructura también define los componentes claves a nivel de TI para iniciar con la definición del marco de gobierno de TI así como el marco para los procesos de Gestión de TI según ITIL que estén alineados con el estándar BS25999.

A continuación se presentarán los elementos que deben ser considerados para formalizar un programa de GCN basados en el estándar BS-25999-1 y algunos ejemplos de estos.

3.2.3 ANÁLISIS GAP

Como punto de partida, es necesario identificar que tan alineada se encuentra la organización con respecto a la Gestión de la Continuidad del Negocio; este análisis se realizará con respecto a la especificación BS25999-2. También se tendrá como punto de partida lo definido en COBIT e ITIL con respecto a la forma como se está realizando la gestión de las TI en la organización.

Este análisis nos dará una visión global del estado de cumplimiento de los diferentes requerimientos, para así estar alineados con respecto a las fortalezas que tiene la organización y realizar un enfoque inicial sobre aquellas áreas donde no se evidencie un nivel de desarrollo y madurez aceptable.

A futuro el resultado del análisis GAP podrá compararse con un modelo de madurez definido permitiendo identificar los logros y avances dentro del proceso de GCN.

3.2.4 APOYO DE LA ALTA GERENCIA Y PREPARACIÓN DE RECURSOS

Ante el inicio de implementación de un SGCN o cualquier otro sistema, el éxito radica en el apoyo que las altas directivas den al proceso; aunque suene un poco

exagerando, las organizaciones se rigen por su día a día y en muchos casos las personas implicadas en el proceso siempre sacan excusas para no apoyar y participar en el mismo, por ello es necesario que la alta dirección este a la cabeza.

Por esto es importante conformar un equipo de trabajo que tenga habilidades de comunicación, que estén apoyados por la alta gerencia, que cuenten con conocimientos de continuidad del negocio (estos pueden estar al interior de la organización o pueden obtenerse a través de capacitación, tercerización y/o consultoría). Es recomendable pensar en un área u oficina enfocada únicamente a la Gestión de la Continuidad del Negocio y acoplarla al esquema organizacional que rige a la organización.

Es importante contar con referencias normativas como:

Norma Británica BS 25999:2006 BUSINESS CONTINUITY

BS25999-1:2006, Código de Practica para la Gestión de Continuidad del Negocio.

BS25999-2:2007, Especificación.

NTC 5254:2006, Gestión del Riesgo

Guía Técnica Colombiana GTC 176 Sistema Gestión Continuidad del Negocio

Cobit 4.1 Control Objectives for Information and related Technology version 4.1

ITIL v3 Information Technology Infrastructure Library version 3.

Referencias relacionadas con la continuidad del negocio de instituciones como el DRI, BCI, ENISA, entre otras.

Estas referencias y el conocimiento de las mismas facilitarán el establecimiento del modelo. En cuanto a los roles para la definición es importante contar con al menos un experto en continuidad del negocio, un experto en auditoria, el rol de la gerencia del proyecto (idealmente basado en una metodología reconocida), un apoyo fuerte de un experto en gestión del cambio, experto en otros sistemas de gestión de la organización, y participación de otras áreas como seguridad física, gestión del talento humano entre otros.

3.2.5 OBJETIVOS DEL SGCN

El alcance y objetivos definen el norte del sistema de gestión y hasta dónde quiere llegar la organización con el mismo. Es recomendable que los objetivos se encuentren alineados con la estrategia y visión de la organización y se encuentren en común acuerdo con las directivas en la empresa. Para el caso del presente modelo estos deben estar centrados a partir de las áreas de TI buscando la integración de los mismos a la estrategia de TI en la organización.

Es muy importante aclarar que aunque la visión de este proyecto es integrar dar lineamientos para que el SGSC se integre a las áreas de TI, no se debe perder la idea general del sistema aplicado a toda la organización.

A continuación se presentan algunos objetivos de ejemplo para guiar a las organizaciones a que definan los mismos de acuerdo a su realidad.

3.2.5.1 EJEMPLO DE OBJETIVOS PARA ESTABLECER EN EL MODELO

Objetivo General

El objetivo general del Sistema de Gestión de Continuidad del Negocio en la organización es asegurar la continuidad de las operaciones claves ante la materialización de algún evento o incidente que atente contra el criterio de disponibilidad.

Objetivos específicos

Definir las políticas y procedimientos requeridos para implementar, mantener y mejorar un Sistema de Gestión de Continuidad del Negocio.

Definir los recursos necesarios para la definición e implementación del Sistema de Gestión de Continuidad del Negocio en la organización. Implica personas, procesos, infraestructura, información y tecnología.

Identificar y gestionar los riesgos que puedan afectar el cumplimiento de los niveles de servicio acordados y requeridos por la organización.

Definir políticas sobre la ilustración de planes de continuidad, programas y metodología que permita a la organización gestionar los riesgos para mantener y mejorar la confiabilidad, disponibilidad y recuperación requerida para dar soporte a los procesos críticos del negocio.

3.2.6 ALCANCE DEL SGCN

Si el alcance del SGCN no es definido desde el inicio, es posible tomar rumbos que atenten contra el éxito del mismo. Su alcance debe estar limitado por las altas directivas de la organización y debe tener como puntos importantes la información y procesos críticos; pensando en el enfoque del presente trabajo es necesario pensar en la plataforma tecnológica que soporta los procesos críticos del negocio en la organización.

3.2.7 DEFINICIÓN DE LA POLÍTICA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Específicamente la política debe definir los siguientes procesos:

Establecer las actividades que incorporan la especificación (estándares), el diseño completo, la construcción, implementación y ejercicio inicial de la capacidad de darle continuidad al negocio.

Las actividades de mantenimiento y gestión que incluyen la adhesión de la continuidad del negocio dentro de la organización, la prueba regular de los planes, su actualización y comunicación, particularmente cuando hay cambios significativos en premisas, personal, procesos, mercado, tecnología o estructura organizacional.

La organización debe asegurar que su política de GCN[13] sea apropiada y ajustada a la naturaleza, escala, complejidad, geografía y criticidad de sus actividades de negocio y que refleja su cultura, dependencias y ambiente de operación.

Esta política define los requerimientos para asegurar que la preparación para la continuidad del negocio en caso de una interrupción sea la adecuada. También debe asegurar que la GCN sea promovida al interior de la cultura de la organización y debe ser integrada en el proceso de control de cambios de la misma permitiendo así que sea incorporada en el crecimiento y desarrollo de sus productos y servicios.

La política de GCN debe declarar los objetivos de CN[14] dentro de la organización. Inicialmente puede ser una declaración de alto nivel que puede irse refinando y mejorando en la medida que se va desarrollando la capacidad de CN.

[13] GCN: Gestión de Continuidad del Negocio

La política de GCN debería entregar a la organización principios documentados con los cuales se aspira cumplir y contra los que se debe medir su capacidad de CN. El propietario y promotor de esta política debería ser la Junta Directiva o su representante designado.

Consideraciones para establecer la política de CN:

1. Definir el alcance de GCN dentro de la organización.
2. Establecer recursos para la GCN.
3. Definir los principios de GCN, guías y estándares mínimos.
4. Reconocer los estándares, regulación, normatividad y políticas que deben incluirse o pueden ser usadas como una referencia de mercado.

La organización debe mantener y regularmente revisar su política de GCN, estrategias, planes y soluciones de acuerdo a sus necesidades.

El alcance de la política debe definir claramente cualquier limitación o exclusión que aplique, por ejemplo: geográfica o exclusión de productos.

La política incluye pero no está limitada a:

Cada unidad organizacional debe designar un Coordinador de Continuidad de Negocio responsable por la coordinación de la planeación de continuidad de negocio dentro del área.

Todos los planes deben ser revisados y aprobados por el Coordinador de Gestión de Continuidad del Negocio, la gerencia del área y el Equipo de Gestión de Continuidad del Negocio quienes son responsables de validar las funciones de negocio críticas documentadas, los tiempos de recuperación objetivo relacionados y demás elementos necesarios para el restablecimiento oportuno de la operación.

En una situación de desastre podría ser necesario dejar de seguir algunas políticas de la organización para permitir la recuperación exitosa de las operaciones críticas del negocio. De esta forma es necesario establecer, para cada unidad organizacional, las pautas para la delegación de autoridad en emergencia.

[14] CN: Continuidad del Negocio

Las unidades de negocio deben desarrollar un Análisis de Impacto al Negocio (BIA[15]) que les permita evaluar los impactos financieros y no financieros de cada función de negocio en el peor escenario.

Las unidades de negocio deben considerar las interdependencias en la cadena de valor del proceso, considerando las interacciones que el área tenga con otras áreas de la organización y entidades externas.

! "#$ %

"#$ &! " % "'() Las unidades de negocio deben asignar a cada función de negocio un tiempo de recuperación objetivo y un punto de recuperación objetivo basado en los resultados del BIA.

En algunas situaciones y basado en los resultados del Análisis de Impacto al Negocio, el Coordinador de Gestión de Continuidad del Negocio puede solicitar en nombre de determinada unidad de negocios una excepción al plan.

* Los registros vitales deben ser identificados, protegidos contra destrucción y sus copias resguardadas en almacenamientos externos según sea apropiado, siguiendo los procedimientos que aseguren su actualización. Este estándar no reemplaza o altera otras políticas corporativas de manejo de registros vitales.

+ El plan de continuidad del negocio debe identificar todos los recursos de computación, áreas de trabajo y registros vitales, entre otros, requeridos para la recuperación de las funciones críticas del negocio. El plan debe especificar los recursos mínimos dentro de los tiempos de recuperación objetivo.

, Cada unidad organizacional debe estar preparada para reubicar sus funciones críticas de negocio en una locación alterna para el restablecimiento de la operación. Es recomendable identificar y seleccionar soluciones internas. En el caso que sea necesario considerar opciones externas de recuperación, las unidades de negocio deben realizar y presentar un análisis costo beneficio a la gerencia del área y al EGCN[17] en

[15] BIA: Business Impact Analysis

[16] RTO: Recovery Time Objetive, Tiempo de Recuperación Objetivo y RPO: Recovery Point Objetive, Punto de Recuperación Objetivo

[17] EGCN: Equipo de Gestión de Continuidad del Negocio

cabeza de su Coordinador. De igual forma, los acuerdos de sitios alternos, ya sean internos o externos, deben ser incluidos en el documento del plan.

+ - % Los planes de continuidad del negocio deben ser documentados siguiendo los parámetros definidos por el EGCN.

" Los organigramas y descripciones de las actividades realizadas normalmente por cada unidad organizacional deben ser incluidos en el documento del plan.

Las unidades organizacionales deben verificar que los proveedores críticos cumplan con requerimientos específicos de la planeación de continuidad del negocio. Estas consideraciones deben ser incluidas en las negociaciones de los contratos de servicios. De igual forma, siempre que sea posible, se deben identificar proveedores alternos.

+ Deben identificarse los equipos de recuperación y sus miembros principales y alternos.

Los procedimientos de declaración de desastre, evacuación, evaluación de daños y respuesta a emergencia deben ser documentados dentro del plan. Los procedimientos deben tener el suficiente nivel de detalle para el seguimiento de los mismos. Las unidades de negocio deben identificar actividades prioritarias específicas para la recuperación de todas las funciones críticas del negocio.

. % ! Los planes deben incluir estrategias de procesamiento manual y temporal en aquellos casos en que estos existan o cuando se ha comprobado que puedan ser prácticos o necesarios para asegurar la continuidad de las funciones críticas de negocio.

" El plan debe incluir los procedimientos para restaurar las funciones de negocio en las instalaciones principales de la organización.

: Deben establecerse procedimientos para informar y mantener al personal actualizado en la planeación de continuidad del negocio y las responsabilidades individuales. El contenido del plan y su implementación debe ser comprendido por todo el personal.

Debe desarrollarse ejercicios de prueba de los planes para demostrar la habilidad de recuperación de las funciones críticas de cada unidad de negocio y de soporte, así como los elementos claves de tecnología y de manejo de crisis.

% - # Los resultados de las pruebas realizadas deben ser evaluados y documentados una vez se hayan completado. La evaluación debe ser realizada contra los objetivos establecidos antes de la prueba y comunicar los resultados del mismo a la gerencia del área y al EGCN. En caso que la prueba no sea exitosa, debe realizarse una nueva prueba una vez se hayan hecho los ajustes correspondientes a los problemas encontrados.

. Los planes deben ser revisados semestralmente para asegurar que todas las actualizaciones requeridas sean realizadas. Deben implementarse procedimientos de control de versiones para proteger la integridad del plan.

3.2.8 ESTRUCTURA ORGANIZACIONAL Y GOBIERNO PARA EL SISTEMA DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Toda organización debe tener como elemento clave en su Sistema de Gestión de Continuidad del Negocio (SGCN) la definición de un marco de referencia de gobierno para su administración, siendo la base fundamental para encaminar y orientar el desarrollo permanente de la disciplina de continuidad dentro de la organización. La Alta Dirección es consciente de que su participación es vital y debe ser activa, para asegurar que el proceso de GCN sea correctamente presentado, adecuadamente soportado y establecido como parte de la cultura de la organización.

El modelo de Gobierno establece el proceso para la toma de decisiones dentro de la organización y las personas o grupos autorizados para hacerlo. Este elemento es especialmente importante para la GCN ya que permite optimizar las inversiones requeridas para mitigación en todas las unidades de negocios, tecnología y funciones administrativas.

Los objetivos principales de una estructura de Gobierno de la GCN son:

Soportar la implementación de la estrategia de los Planes de Continuidad del Negocio.

Soportar el cumplimiento de las políticas de GCN en todos los niveles de la organización.

Asegurar un liderazgo sólido y responsable con roles y responsabilidades claramente definidas.

Garantizar que la función de GCN cuente con el personal apropiado para administrar el programa.

Cumplir las expectativas corporativas, expectativas regulatorias y obligaciones legales.

Facilitar el mejoramiento continuo del programa basado en los requerimientos específicos de cambio del negocio, cambios regulatorios, experiencia operacional, entre otros.

Activar los niveles apropiados de respuesta durante eventos de crisis o interrupciones del negocio.

La alta dirección de la organización debe designar la persona con autoridad y nivel jerárquico responsable de la política y su implementación. También debe asignar uno o más individuos para implementar y mantener el programa de GCN [2].

Si la estructura lo permite o lo exige la alta dirección puede nombrar representantes a lo largo de la organización por función o locación para asistir la implementación del programa de GCN.

Dentro del presente esquema organizacional y de gobierno para la GCN se define la creación del Comité Ejecutivo de Continuidad del Negocio, encargado de la aprobación de decisiones relacionadas con las estrategias para el desarrollo, implementación, mantenimiento y mejora continua de todos los elementos de la Gestión de Continuidad del Negocio.

Cada uno de los líderes de procesos identificados dentro de la organización (Coordinadores de Unidad de Negocio) como críticos, son líderes de continuidad del negocio, responsables del mantenimiento, actualización y mejora continua de acuerdo con los ajustes por procedimientos, nuevos productos o ajustes de tecnología.

La GCN tomará del Sistema de Gestión de Calidad de la organización los elementos comunes y efectivos para el conocimiento y documentación del mismo.

Cabe resaltar que la propuesta de la organización es genérica y su objetivo principal es lograr adaptarla en el entorno de cada organización sin causar el mayor impacto posible tanto a nivel de recurso humano como económico.

3.2.8.1 MODELO DE MADUREZ PARA EL SGCN

A continuación se realiza una primera propuesta para el modelo de madurez del SGCN; cabe anotar que es un modelo general pensando en todo el sistema de gestión. El modelo de Madurez se considera el gobierno de la GCN. Es un criterio para identificar el nivel de logro y madurez de un programa de GCN. La siguiente figura muestra los diferentes niveles de madurez planteados para el programa de GCN; este modelo de madurez parte de la definición dada en [3] para los modelos de madurez de procesos de TI.

	Nivel de Madurez	Programa Básico			Programa Desarrollado		
		Comité de Gestión	Soporte Profesional	Gobierno	Todas las Unidades	Planeación Integrada	Función Cruzada
Nivel 1	AutoGobierno	NO	NO	NO	NO	NO	NO
Nivel 2	AutoGobierno Soportado	MARGINAL	PARCIAL	NO	NO	NO	NO
Nivel 3	Gobierno Centralizado	PARCIAL	SI	PARCIAL	NO	NO	NO
Nivel 4	Inicio Empresarial	SI	SI	SI	SI	NO	NO
Nivel 5	Crecimiento Planeado	SI	SI	SI	SI	SI	NO
Nivel 6	Sinergico	SI	SI	SI	SI	SI	SI

Figura No. 12: Niveles de Madurez de la GCN [8] [3]

El nivel 1 considera que no existen dentro de la organización una política robusta de GCN ni una oficina o equipo encargado de estandarizar y orientar a las áreas en la planeación de continuidad de negocio, por lo que cada unidad de negocios desarrolla sus planes de acuerdo con lo que considere más conveniente. En esta etapa, la Gerencia de la organización no está involucrada en la GCN ni la considera como un elemento importante de la organización.

En el nivel 2, algunas áreas se han comenzado a percatar de la importancia de la GCN y comparten su iniciativa con otras áreas a nivel de la organización aumentando su concientización. Se involucran en el proceso a algunos profesionales en Continuidad de Negocio, ya sean internos o externos.

El nivel 3 es alcanzado cuando la organización comienza a estandarizar los diferentes elementos de la GCN tales como planes, prácticas y procesos. Se abre la puerta a la creación del Comité y el EGCN responsable por apoyar el proceso.

En el nivel 4, la gerencia es consciente de la importancia de la GCN y promueve la definición e implementación de una política robusta de continuidad de negocio. De

igual forma, se fortalece la estructura de GCN y todas las unidades de negocio han documentado sus PCN[18] y están comenzando a probarlos.

El nivel 5 involucra la culminación de las pruebas y mantenimiento de todos los planes de la organización. El equipo de Crisis ha participado en ejercicios. Existe un programa de crecimiento de la GCN integrando el programa a la cultura de la organización.

Finalmente, el nivel 6 representa a aquel en el cual la organización se encuentra totalmente comprometida con el programa de GCN. Existe una fuerte coordinación de los equipos que participan en la respuesta a los eventos críticos.

3.2.8.2 ESTRUCTURA ORGANIZACIONAL

La organización para la Gestión de Continuidad del Negocio se plantea de la siguiente forma teniendo como punto de partida un marco de gobierno y los responsables asociados con los diferentes roles. La estructura se muestra en la siguiente figura:

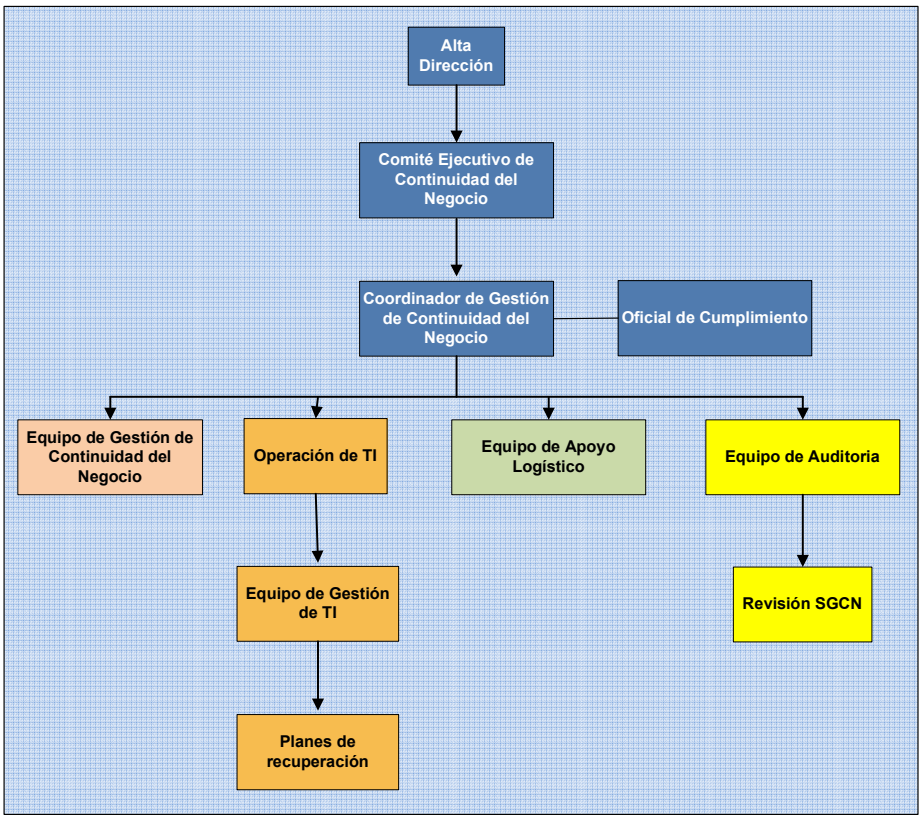

Figura No. 13 Estructura Organizacional SGCN

[18] PCN: Planes de Continuidad de Negocio

La estructura organizacional definida para el SGCN tiene como cabeza principal a la alta dirección, que es el estamento principal para cualquier decisión que se requiera con respecto a continuidad. Los grupos que se conforman de acuerdo a esta estructura se definen a continuación:

3.2.8.2.1 ALTA DIRECCIÓN

Conformado por los altos estamentos de la organización, Gerente General y socios representativos. Responsables de revisar la orientación estratégica que se ha formulado para el Sistema de Gestión de Continuidad del Negocio y si su enfoque para la organización es el correcto.

3.2.8.2.2 COMITÉ EJECUTIVO DE CONTINUIDAD DE NEGOCIO

Rol

El Comité Ejecutivo de Continuidad de Negocio es el grupo de personas que se encarga de la toma de decisiones claves en la organización en relación a la continuidad del negocio, opciones de recuperación estratégica y planeación de continuidad para la organización.

3.2.8.2.2.1 ESTRUCTURA Y RESPONSABILIDADES DEL COMITÉ EJECUTIVO DE CONTINUIDAD DE NEGOCIO

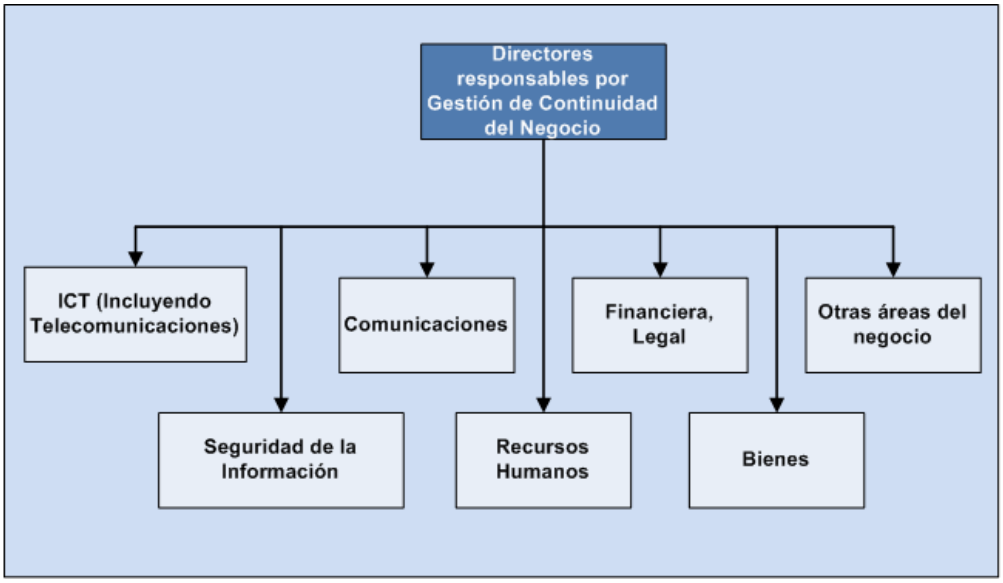

Figura No. 14 Estructura Comité Ejecutivo de Continuidad del Negocio

El Comité Ejecutivo de Continuidad de Negocio es el grupo propuesto responsable para la financiación y gobierno de los programas de Gerencia de Continuidad del Negocio. Se conforma de directores y/o recursos representando todas las áreas funcionales críticas del negocio, líderes de procesos, expertos en tecnología, profesionales en continuidad.

Es imperativo para el gobierno del programa de Continuidad del Negocio que el Comité Ejecutivo de Continuidad del Negocio sea conformado. La implementación de este comité asegura que los planes de continuidad de la organización son regularmente considerados, revisados, probados y actualizados cuando ocurran cambios organizacionales.

Responsabilidades Preventivas:

Revisar el SGCN periódicamente y cuando se produzcan cambios significativos con el fin de asegurar su conveniencia, adecuación y eficacia.

Participar en la aprobación de las políticas definidas y acciones que busquen la implementación y mantenimiento del SGCN en la organización.

Identificar, asesorar y priorizar proactivamente los riesgos relacionados con la continuidad del negocio, tecnología, respuesta a emergencias y gestión de crisis.

Tomar decisiones sobre el alcance y la eficacia del SGCN.

Aprobar y soportar la formulación, desarrollo e implementación de estrategias efectivas de GCN y/o estrategias de transferencia de riesgo.

Reunirse a intervalos regulares de tiempo durante y después del programa de implementación. Es recomendable que estas reuniones se realicen mensualmente durante la fase de implementación del programa y trimestralmente una vez el programa GCN es parte del día a día de la gestión de la organización.

Alinear las actividades con los objetivos estratégicos de la organización y los programas de continuidad del negocio.

Integrar en la cultura de la organización los siguientes elementos clave de la GCN:

Gobierno, responsabilidades y custodia del riesgo

Reporte y comunicaciones

Responsabilidades Respuesta:

Evaluar los eventos de crisis (con base en información recibida).

Tomar decisiones sobre si se debe o no declarar un desastre.

Proveer directrices estratégicas.

Desplegar los recursos de recuperación.

Actuar como el Comité de Manejo de Crisis en caso de requerirse.

Ser un punto común de coordinación y comunicación para todas las respuestas y subsecuentes actividades de continuidad y recuperación del negocio. Este Equipo está organizado dentro de los niveles estratégico y táctico.

Responsabilidades Recuperación:

Evaluar la situación con base en los reportes recibidos.

Tomar decisión de volver a operación normal.

Evaluar consecuencias del evento.

Aprobar medidas para mejoramiento y acciones correctivas.

3.2.8.2.3 COORDINADOR DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Rol

El Coordinador de Gestión de Continuidad del Negocio es la persona líder dentro del SGCN. Debe administrar el Plan General de Continuidad del Negocio y coordinar la respuesta y recuperación de una crisis junto a su Equipo de Gestión de Continuidad del Negocio y apoyado en el Comité Ejecutivo de Continuidad del Negocio. A través de la recolección de información relevante y las opciones de los diferentes equipos, facilitar una toma de decisiones precisa y delegar y hacer seguimiento a las tareas para asegurar que se lleven a cabo.

El Coordinador de Gestión de Continuidad del Negocio es el punto principal dentro de la gestión y dirección de todas las actividades que hacen parte del SGCN dentro de la organización.

Habilidades y competencias requeridas

El Coordinador de Gestión de Continuidad del Negocio es un gerente de proyecto y un individuo que toma decisiones, que trabaja con el Comité Ejecutivo para supervisar y dirigir los esfuerzos y las tareas de recuperación, con un enfoque de coordinación y gerencia. Debe contar con conocimientos específicos y experiencia relacionada a la GCN.

El Coordinador de Gestión de Continuidad del Negocio es responsable de comunicar las actualizaciones al SGCN de manera regular, con el fin de evitar un enfoque aislado de la recuperación.

El rol requiere comunicación intensa e información precisa sobre todos los aspectos de los esfuerzos de recuperación.

Responsabilidades Preventivas:

Tiene la responsabilidad general de aprobar las revisiones de los planes de continuidad de las unidades de negocio y del plan general de continuidad del negocio, así como efectuar acompañamientos de apoyo y motivación a cada uno de los Líderes de los Procesos Críticos para que el plan se mantenga vivo, analizando y verificando que las tareas que se deban desarrollar se lleven a cabo y sean las más efectivas y así determinar que los Líderes de los Procesos Críticos, transmitan estos mensajes de motivación y compromiso a cada uno de los integrantes de sus áreas.

El Coordinador de Gestión de Continuidad del Negocio debe mantener una lista de todos los colaboradores que tienen copias del plan y garantizar que todos los destinatarios tengan una versión actualizada.

Es responsable de recuperar las copias del plan de aquellos colaboradores que salgan de la empresa. Cuando se emitan nuevas versiones, se deben destruir las versiones anteriores, el Coordinador de Gestión de Continuidad de Negocio debe guardar el histórico del plan.

Debe tener una copia completa del plan (copia dura o electrónica) la cual debe ubicarse en las ubicaciones alternas definidas en la estrategia de Recuperación con el fin de garantizar su disponibilidad para ser usada durante una emergencia.

Ser cabeza dentro de la administración del Proceso de Gestión de Continuidad de Negocio.

Establecer en conjunto con el área de Recursos Humanos, las necesidades de capacitación y modificaciones al diccionario de competencias que se requieran para la Gestión de Continuidad del Negocio.

Monitorear la gestión documental de los Planes de Continuidad, buscando garantizar que se encuentran actualizados y que las modificaciones en los procesos y nuevos proyectos sean incluidos en el análisis.

Coordinar la programación y ejecución de pruebas a los diferentes componentes de los Planes de Continuidad de Negocio.

Establecer una estrategia de divulgación de los Planes de Continuidad (o Plan de Continuidad) y monitorear su ejecución.

Promover que los miembros de los equipos se encuentra consientes, familiarizados y capacitados en su rol y responsabilidades con relación a los planes de continuidad de cada una de las unidades de negocio (en caso de existir) o el plan de continuidad del negocio (empresa pequeña).

Respuesta (Manejo de Incidentes y Movilización):

Autorizar la activación de las tareas de respuesta a incidentes en coordinación con el EGCN y el Comité Ejecutivo.

Dirigir la recolección de información en general sobre el evento para validarla, filtrarla y escalarla al Comité Ejecutivo.

Dar un reporte preliminar consolidado de la evaluación del incidente al Comité Ejecutivo.

Participar en la evaluación de la situación general del incidente.

Administrar las operaciones del incidente garantizando que las tareas que sean delegadas al equipo se finalicen.

Autorizar activación de las tareas de recuperación, cuando el problema se considere no crítico.

Si el problema se considera crítico, deberá hacer un escalamiento al Comité Ejecutivo para solicitar autorización de activación del plan.

Una vez se activa el plan, instruir a los equipos de recuperación del negocio (en las unidades de negocio) para ejecutar sus planes y estrategias de recuperación en cada uno de sus procesos y funciones de negocio.

Coordinar con el Comité Ejecutivo y el área de recursos humanos los asuntos de personal en caso de un incidente en la organización.

Asesorar a los líderes de los equipos de recuperación del negocio.

Recuperación (Operación en Contingencia y Retorno a la Normalidad):

Monitorear las tareas de recuperación de incidentes en coordinación con el EGCN y el Comité Ejecutivo.

Gestionar los requerimientos de las áreas ante el Comité Ejecutivo.

Desarrollar recomendaciones para la recuperación de las operaciones.

Mantener informado al Comité Ejecutivo del avance de recuperación, con base en la información suministrada por los equipos de recuperación del negocio.

Solicitar autorización para ejecutar el proceso de retorno a la normalidad.

Debe estar atento y ser el director de los programas de sensibilización sobre continuidad de negocio (CN) para la organización.

Debe estar atento al mantenimiento y actualización de los planes de continuidad de negocio (BCP) desarrollados ya sea a nivel general (organización pequeña) o sobre cada unidad de negocio identificada (organización grande).

Reportar directamente a la alta dirección y al Comité Ejecutivo. Esta persona idealmente debe tener:

Un buen entendimiento de los aspectos críticos del negocio y su personal clave y dependencias.

Entendimiento de la metodología GCN.

Debe asegurar que todos los directivos, cabezas de servicio y líderes comprendan la importancia de la GCN, la aproximación de la organización a su SGCN.

3.2.8.2.4 OFICIAL DE CUMPLIMIENTO

Rol

El Oficial de Cumplimiento apoya al Coordinador de Gestión de Continuidad del Negocio, Comité Ejecutivo y al EGCN en lo relacionado a normatividad y requerimientos legales.

Responsabilidades

Monitorear y evaluar nueva legislación y nuevas regulaciones para definir lineamientos a considerar en cuanto a la Gestión de Continuidad del Negocio.

Hacer conocer a la alta dirección sus responsabilidades legales según las leyes y regulaciones vigentes.

Hacer recomendaciones legales para prevenir que la organización tome riesgos indebidos como resultado del uso de nuevas tecnologías, tales como los servicios por Internet.

Informar al Comité de Ejecutivo de Continuidad acerca de los requerimientos legales en contratos de provisión de servicio y outsourcing.

Definir y revisar periódicamente toda la documentación relacionada con contratos, acuerdos con proveedores y terceros.

Representar a la organización ante las autoridades judiciales en situaciones en las

cuales se vea involucrada en procesos relacionados con incumplimientos en contratos de provisión de servicios o con terceros en aspectos relacionados a continuidad del negocio.

3.2.8.2.5 EQUIPO DE GESTIÓN DE TECNOLOGÍA

Rol

Este equipo debería ser parte de la estructura definida por la organización para afrontar cualquier situación o evento catastrófico. El rol principal es apoyar al Comité Ejecutivo de Continuidad del Negocio con las actividades iníciales de evaluación, activación y supervisión de las tareas de recuperación relacionadas con los servicios de TI y trabajar en conjunto con el Equipo de Gestión de Continuidad del Negocio en la implementación y pruebas de los planes de GCN.

Habilidades y competencias requeridas

Conocimiento total de la Infraestructura de TI de la organización en todos los niveles (servidores, software, aplicaciones, sistemas de bases de datos) y las relaciones existentes entre la plataforma de TI y los procesos críticos de negocio. También debe estar al tanto de las estrategias y planes de recuperación de TI y en general del Plan de Recuperación de Desastres (DRP) desarrollado en la organización.

Responsabilidades

Este equipo es responsable de suministrar la recuperación técnica del hardware (servidores), software (sistemas operativos, bases de datos y sistemas de información), sistemas eléctricos, plantas telefónicas y servicios de conectividad en general.

El equipo es responsable de verificar que los aplicativos estén funcionando adecuadamente, asegurar la conectividad del usuario y suministrar servicios de recuperación según se definan en el ámbito de aplicación y en los objetivos establecidos en más detalle dentro del Plan de Recuperación de Desastres (DRP).

Iniciar el plan de recuperación de desastres, el cual detallará el cambio de actividades al sitio de operación alterna, si es adecuado y si se considera necesario por parte del Comité Ejecutivo de Continuidad del Negocio.

Supervisará la evaluación de daños técnicos.

Coordinará las actividades de retorno al sitio principal de operación siguiendo las actividades y tareas de respuesta y recuperación definidos en el Plan.

Acatará las prioridades de recuperación de los sistemas de información con base en los requerimientos de la empresa (RTO) y la evaluación de los daños.

Desarrollar y mantener los planes de Recuperación de Tecnología para las aplicaciones críticas del negocio.

Entregar al Coordinador de Gestión de Continuidad del Negocio la versión actualizada de los planes de Recuperación de Tecnología.

Cumplir con las políticas/lineamientos de CN establecidos por la organización.

Identificar y designar un Líder de Recuperación de Tecnología, responsable por la coordinación de las actividades de respuesta, recuperación y retorno a la normalidad.

Coordinar junto con el EGCN el cronograma y la ejecución de las pruebas de los Planes de Recuperación de Tecnología.

Participar activamente en las sesiones de concientización, entrenamiento y otras actividades programadas por el EGCN.

Asegurar que la información del equipo del área se encuentre actualizada y que todos los miembros conocen sus roles y responsabilidades.

En una emergencia, informar al Coordinador de Gestión de Continuidad del Negocio y al Equipo de Gestión de Continuidad del Negocio la situación siguiendo los procedimientos y los lineamientos de comunicación.

Cumplir las metas de GCN establecidas por la organización.

Reportar periódicamente al EGCN los avances, estatus y el cronograma de implementación de la estrategia de recuperación de tecnología.

Trabajar en conjunto con las unidades de negocio para mantener actualizadas las necesidades de tecnología y su criticidad.

Llevar a cabo un mantenimiento adecuado de la infraestructura tecnológica.

Garantizar las actividades de backup, almacenamiento de copias por fuera de las instalaciones y rotación de las mismas.

En conjunto con el EGCN, evaluar los proveedores de tecnología, actuales y nuevos, para identificar riesgos, prevenir incidentes y asegurar una respuesta efectiva (estableciendo acuerdos de niveles de servicio, identificando proveedores alternos, etc.).

Restaurar los sistemas operativos, aplicaciones y conexiones a la red.

Dar asistencia a las unidades de negocio para responder a incidentes.

Enmarcar sus actividades dentro del marco de gobierno de TI definido para la organización.

Cumplir con los indicadores de desempeño y métricas relacionadas a los procesos de GCN.

3.2.8.2.6 EQUIPO DE AUDITORIA

Rol

El equipo de auditoría es responsable por apoyar al negocio y a las unidades en el diseño, implementación y continuo monitoreo del SGCN. Las responsabilidades del equipo de auditoría incluyen:

Responsabilidades

Revisar que las unidades de negocio cumplan con los requerimientos establecidos en los estándares de continuidad del negocio de la organización.

Efectuar chequeos de cumplimiento donde se determine, no solo el cumplimiento por parte de los empleados de las diferentes Políticas de GCN.

Ayudar a asegurar la existencia e implementación de un programa efectivo de Continuidad de Negocio.

En coordinación con el EGCN, evaluar y, de ser apropiado, aprobar las solicitudes de excepciones de los planes enviadas por las unidades de negocio asegurando que se implementen los controles compensatorios.

Revisar los planes existentes para asegurar que estos estén de conformidad con los requerimientos corporativos de continuidad del negocio.

Monitorear las pruebas de recuperación para asegurar su efectividad y la solución oportuna de los problemas identificados en el desarrollo de las mismas.

Acordar con el EGCN la interpretación de los estándares de Continuidad de Negocio y otros temas relacionados.

Evaluar en forma periódica la responsabilidad de las directivas de la organización respecto a una variedad de amenazas tales como negligencia, no cumplimiento de responsabilidades con el sistema y generar las recomendaciones necesarias.

3.2.8.2.7 EQUIPO DE APOYO LOGISTICO

Rol

Responsables de evaluar las condiciones de las instalaciones e infraestructura

afectadas por el evento, dar apoyo logístico ante un incidente y ser punto de apoyo para el EGCN. Debe estar formado por personal responsable de los servicios básicos, tecnología, recursos humanos, seguridad física e infraestructura. Las actividades que debe realizar este equipo en un evento de desastre son:

Responsabilidades

Determinar la probabilidad de nuevos daños.

Identificar las funciones de negocio y las áreas afectadas.

Identificar el estado de los servicios básicos (electricidad, agua, aire acondicionado, red, entre otros.)

Identificar los recursos que deben ser remplazados de inmediato.

Dar inicio a los procesos disciplinarios que se deriven del no cumplimiento con las políticas internas, estándares u otros requerimientos de seguridad de la información.

Estimar el tiempo en que se pueden recuperar las instalaciones y servicios básicos.

Si el tiempo estimado para recuperar las instalaciones es mayor al tolerable, se debe declarar el desastre y activar el procedimiento de recuperación para este escenario.

3.2.8.2.8 EQUIPO DE GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La definición del Equipo de Gestión de Continuidad del Negocio es uno de los pilares dentro del SGCN. Este equipo tiene la responsabilidad de ser el ente orquestador de las actividades que se desarrollan en el ciclo del sistema. Dada su importancia, en la presente propuesta se considera que el EGCN constituya una estructura con las siguientes definiciones:

Misión y Visión: La Misión y Visión definen la razón de existencia del EGCN. Se definen sus metas a largo plazo, aspiraciones y objetivos.

Alcance y Objetivos: Define el rol y alcance del EGCN. Adicionalmente, debido que la GCN es una actividad que se desarrolla a través de toda la organización, especifica los roles y responsabilidades del negocio, las unidades operativas y las funciones administrativas dentro de la organización.

Organización: Para garantizar una respuesta efectiva a una emergencia es necesario que la organización brinde los recursos requeridos para realizar las actividades necesarias y recuperar las funciones principales, siendo importante involucrar al personal solicitado para establecer, operar y mantener la GCN, creando los equipos necesarios para hacer frente a eventos. Este elemento también expone las competencias y el perfil profesional de las personas requeridas para la realización de las tareas relacionadas con la GCN, definiendo roles y responsabilidades y conduciendo entrenamientos al personal identificado.

Modelo de Gobierno. Junto con el Coordinador de Gestión de Continuidad del Negocio, el Comité Ejecutivo de Continuidad del Negocio y la Alta Dirección se establece el proceso para la toma de decisiones dentro de la organización y las personas o grupos autorizados para hacerlo. Este elemento es especialmente importante para la GCN ya que permite optimizar las inversiones requeridas para mitigación en todas las unidades de negocios, tecnología y funciones administrativas.

3.2.8.2.8.1 ESTRUCTURA Y RESPONSABILIDADES DEL EGCN

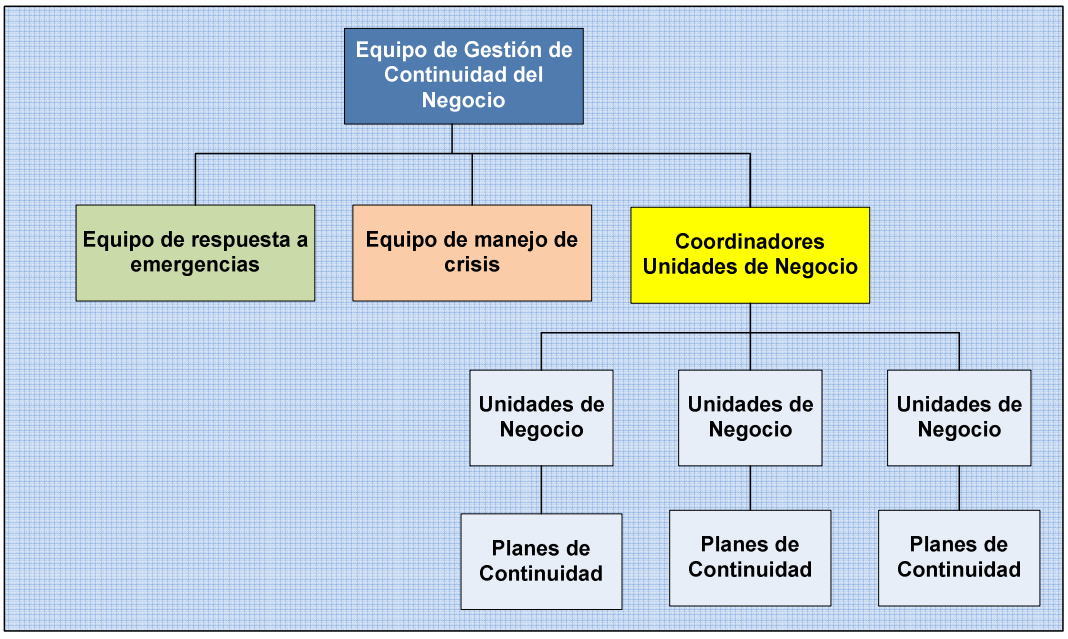

Figura No. 15 Estructura del Equipo de Gestión de Continuidad del Negocio

Rol

El Equipo de Gestión de Continuidad del Negocio es responsable por la entrega y estrategias de continuidad del negocio dentro de la organización, planes de recuperación, respuesta a emergencias, manejo de crisis, recuperación de tecnología y mantenimiento del SGCN.

Este grupo debe promover el desarrollo y establecimiento de políticas y estándares soportando a las unidades de negocio en el desarrollo de planes y pruebas. Este equipo también debe participar en la planeación y ejecución de las pruebas necesarias y asegurar la consistencia e integración de todos los planes. La estrategia de recuperación de tecnología se convierte en una responsabilidad compartida con la Dirección de Tecnología.

El equipo está integrado por miembros de cada uno de los procesos y subprocesos identificados como críticos, quienes serán responsables de la recuperación de los mismos y de la activación de las actividades de comunicación de sus equipos cuando ocurra un incidente que requiera la evacuación de la instalación afectada y su subsiguiente reubicación en instalaciones de recuperación, de ser necesario. Cada equipo tiene un líder principal y uno suplente (en caso de que el principal no esté disponible), con el fin de liderar los esfuerzos de recuperación para ese equipo específico.

Habilidades y Competencias Requeridas

Conocimiento de la funcionalidad de los procesos y los servicios y productos de la organización. Estar familiarizado con los procesos del negocio y los fundamentos del plan de recuperación.

Responsabilidades Preventivas:

Conocer y participar en el desarrollo de las tareas preventivas identificadas en los planes de cada proceso crítico.

Participar en las pruebas y simulacros programados.

Identificar las mejoras y ajustes a los procedimientos e instructivos que apoyen procesos críticos.

Estar a cargo del desarrollo de políticas, planeación estratégica, direccionamiento y soporte a las unidades de negocio o administrativas para la planeación de la continuidad del negocio, plan de recuperación de tecnología y gestión de crisis, evaluación de riesgos y análisis del impacto al negocio.

Estar a cargo de la definición de estándares y la administración de los recursos necesarios para responder a un evento.

Estar a cargo del diseño de la clasificación de los tipos de niveles de emergencia, reglas y criterios.

Velar por el desarrolló, entrega y mantenimiento de las políticas y estándares de continuidad, liderazgo de los procesos de comunicación y divulgación de los mismos, etc.

Identificar claramente las unidades de negocio en la empresa.

Definir las responsabilidades de cada unidad de negocio identificada.

Ser soporte a las unidades de negocio quienes son responsables por el diseño, implementación y mantenimiento de sus Planes de Continuidad del Negocio.

Participar en la formulación, con la Gerencia de la organización y junto al Comité Ejecutivo de Continuidad de Negocio una política corporativa de GCN.

Colaborar con las funciones corporativas tales como auditorias, comunicaciones corporativas para que puedan soportar el programa de GCN.

Liderar y guiar la capacitación de las personas involucradas con la GCN.

Conducir investigaciones y desarrollos encaminados al mejoramiento de la arquitectura y tecnología de la compañía con el enfoque de CN.

Direccionar los esfuerzos de análisis de impacto al negocio y análisis y evaluación de riesgos.

Ser un recurso de información relativa a las prácticas de recuperación, contratos, proveedores y socios.

Generar periódicamente informes a la Gerencia y al Comité Ejecutivo de Continuidad del Negocio.

Responsabilidades de Respuesta (Manejo de Incidentes y Movilización):

Seguir las instrucciones del Coordinador de Gestión de Continuidad del Negocio.

Ejecutar las actividades definidas en los planes de recuperación.

Comunicar la situación al Comité de Manejo de Crisis.

Definir en común acuerdo con el Comité Ejecutivo de Continuidad de Negocio cuando se activa el Plan de Continuidad de Negocios.

Ayudar a los Coordinadores de Unidad a cumplir con los objetivos de respuesta.

Movilizarse, si es necesario.

Ser el único punto de contacto para la mesa de servicio en caso de un incidente que atente contra la disponibilidad de la plataforma de TI. La mesa de servicio

monitoreará la respuesta a la emergencia y los esfuerzos de recuperación, ofreciendo asistencia y generando informes del estado de la situación a la Gerencia.

Ayudar a las unidades del negocio con el análisis de incidentes.

Dar seguimiento a la situación durante y después del evento.

Garantizar que las áreas afectadas utilicen los procedimientos de continuidad.

Responsabilidades de Recuperación (Operación en contingencia y Retorno a la Normalidad):

Seguir las instrucciones del Coordinador de Gestión de Continuidad del Negocio.

Ayudar a otros miembros del equipo a cumplir con los objetivos de recuperación.

Asegurar la disponibilidad de la información de las operaciones realizadas de manera manual o semiautomática durante la contingencia (dependiendo de la naturaleza del evento).

Movilizarse, si es necesario.

3.2.8.2.8.2 EQUIPO DE MANEJO DE CRISIS

Rol

El Comité de Manejo de Crisis debe estar formado por representantes de diferentes áreas de la empresa (este comité puede estar conformado por integrantes del Comité Ejecutivo de Continuidad del Negocio), con la experiencia y autoridad para manejar los efectos de un incidente que interrumpa el normal funcionamiento de los procesos críticos en la organización. Normalmente lo conforman la Alta Dirección de la empresa, entre ellos el Gerente General o Presidente, los Vicepresidentes de la empresa y el Coordinador o Gerente de Continuidad de Negocios, o quien haga sus veces.

Responsabilidades

Brindar la dirección a seguir y las prioridades durante un incidente no contemplado en el plan de continuidad.

Comunicar a los accionistas, clientes, proveedores y entidades interesadas, sobre la situación de la empresa.

Toma de decisiones estratégicas durante la crisis o incidentes.

Comunicación efectiva con los medios de comunicación.

Supervisión de la efectividad de las actividades de recuperación

3.2.8.2.8.3 COORDINADORES DE UNIDADES DE NEGOCIO

Rol

El Coordinador de Unidad es el líder frente a su respectiva Unidad de Negocio en lo relacionado a la continuidad del negocio. Debe participar en el desarrollo, implementación y administración del plan de continuidad desarrollado para la respectiva unidad.

Habilidades y competencias requeridas

El Coordinador de Unidad de Negocio es una persona con conocimientos sólidos sobre su proceso, el cual trabaja junto con el EGCN para el desarrollo de los planes de continuidad y recuperación.

Debe conocer la interrelación entre su proceso de negocio y los demás procesos de la organización así como la relación de la plataforma de TI que es soporte para el desarrollo de las funciones del proceso.

Responsabilidades Preventivas:

Responsables de coordinar la ejecución de los procedimientos de respuesta y recuperación de sus respectivas áreas, verificando el estado de los procesos afectados durante y después del evento.

Debe identificar las funciones claves en su unidad de negocio.

Debe identificar los recursos de TI que soportan las funciones claves en su unidad de negocio; de forma similar tiene que identificar el recurso humano que participa en la unidad de negocio.

Tiene la responsabilidad de ayudar en el desarrollo de los planes de continuidad de las unidades de negocio y efectuar el acompañamiento respectivo en opciones de mejora, cambios que sean realizados a estos planes.

El Coordinador de Unidad de Negocio debe mantener una lista de todos los colaboradores que hacen parte del proceso al cual representa y garantiza que todos tienen conocimiento de los roles y responsabilidades identificados para dicha unidad.

Debe estar atento a los cambios realizados en los planes de la unidad y de dar a conocer a los integrantes de la unidad de negocio cualquier cambio en cuanto a cambios, roles y responsabilidad.es

Monitorear la gestión documental del plan de continuidad dentro de su unidad de negocio, buscando garantizar que se encuentra actualizado.

Coordinar junto al EGCN la programación y ejecución de pruebas a los diferentes componentes del Plan de Continuidad de Negocio.

Respuesta (Manejo de Incidentes y Movilización):

Coordinar las tareas de respuesta a incidentes dentro de su unidad de negocio en coordinación con el EGCN.

Participar en la evaluación de la situación general del incidente si se presentará en su unidad de negocio.

Recuperación (Operación en Contingencia y Retorno a la Normalidad):

Desarrollar recomendaciones para la recuperación de las operaciones de su unidad de negocio.

Mantener informado al Coordinador de Gestión de Continuidad del Negocio y al EGCN del avance de recuperación de su unidad.

Coordinar el seguimiento paso a paso los procesos de retorno a la normalidad definidos para la unidad de negocio.

Ser punto de comunicación directo con el EGCN durante esta etapa.

3.2.8.2.8.4 UNIDADES DE NEGOCIO

Rol

La Unidad de Negocio está conformada por el conjunto de empleados pertenecientes a un proceso crítico dentro de la organización. Como Unidad de Negocio debe tener conocimiento del impacto que traería una interrupción a sus funciones (Impacto de Análisis al Negocio) y debe velar por el desarrollo de estrategias de recuperación y continuidad.

Las Unidades de Negocio deben ejecutar las actividades que permitan verificar la consistencia e integridad de los datos y la funcionalidad de las aplicaciones críticas respaldadas en el Centro de Cómputo.

Habilidades y competencias requeridas

Conocimiento de las dependencias con tecnología y otras unidades de negocio, conocimiento y funcionalidad de los aplicativos críticos y los productos de la organización. Estar familiarizado con los procesos del negocio y los fundamentos del plan de recuperación.

Responsabilidades

Desarrollar y mantener los Planes de Continuidad de Negocio para las funciones críticas del área.

Entregar al Coordinador de la Unidad de Negocio y al EGCN la versión actualizada de los Planes de Continuidad desarrollados para la unidad.

Cumplir con las políticas/lineamientos de CN establecidos por la organización.

Identificar y designar un Líder de Continuidad en el área, responsable por la coordinación de las actividades de respuesta y recuperación de las funciones críticas del área. Este líder puede tomar el rol de Coordinador de la Unidad de Negocio.

Coordinar junto con el EGCN el cronograma y la ejecución de las pruebas de los Planes de Continuidad del Negocio.

Participar activamente en las sesiones de concientización, entrenamiento y otras actividades programadas por el Coordinador de Gestión de Continuidad de Negocio y el EGCN.

Comunicar a los Coordinadores de la Unidades y al EGCN las necesidades relativas a la respuesta y recuperación del área, tales como recursos necesarios, entre otros.

Asegurar que la información del equipo del área se encuentre actualizada y que todos los miembros conocen sus roles y responsabilidades.

Asistir en la definición de los controles derivados de las Políticas de Continuidad del Negocio.

Evaluar iniciativas tecnológicas propuestas para la ejecución de correctivos.

Asesorar a la gerencia de la empresa en la adquisición de tecnología de continuidad del negocio.

3.2.8.3 DOCUMENTACIÓN DE LA FASE DE PLANEACIÓN

En esta fase inicial se deben generar o actualizar los siguientes documentos:

Alcance y objetivos del SGCN

Política de GCN

Definición de roles, responsabilidades y competencias en GCN para la organización.

Sensibilización en GCN

Control de registros del SGCN

Control de la documentación del SGCN

3.3 ENTENDIENDO LA ORGANIZACIÓN

Durante esta fase se busca identificar la información que permite priorizar los productos y servicios de la organización y permite conocer el nivel de urgencia de las actividades que son necesarias para su entrega o prestación. Esto define los requisitos que determinarán la selección de estrategias de GCN apropiadas.

BS25999-2 define al BIA y al análisis de riesgos como las herramientas claves para identificar las variables necesarias para la siguiente etapa dentro del ciclo de vida del SGCN; desarrollo de estrategias.

3.3.1 ANÁLISIS DE IMPACTO AL NEGOCIO

El Análisis de Impacto al Negocio (BIA), permite a la organización identificar las actividades críticas como los recursos necesarios para que soporten a los productos y servicios fundamentales, entender las amenazas a que se enfrentan y elegir los tratamientos de riesgo apropiados [9].

Las actividades críticas deben ser identificadas en todos los departamentos, áreas en la organización. Esto incluye toda la información, procesos, actividades e infraestructura necesaria para continuar las operaciones en caso de algún incidente. Para determinar las necesidades críticas de la organización, cada departamento debe documentar todas las funciones importantes. Es necesario tener presente preguntas como [18] [17]:

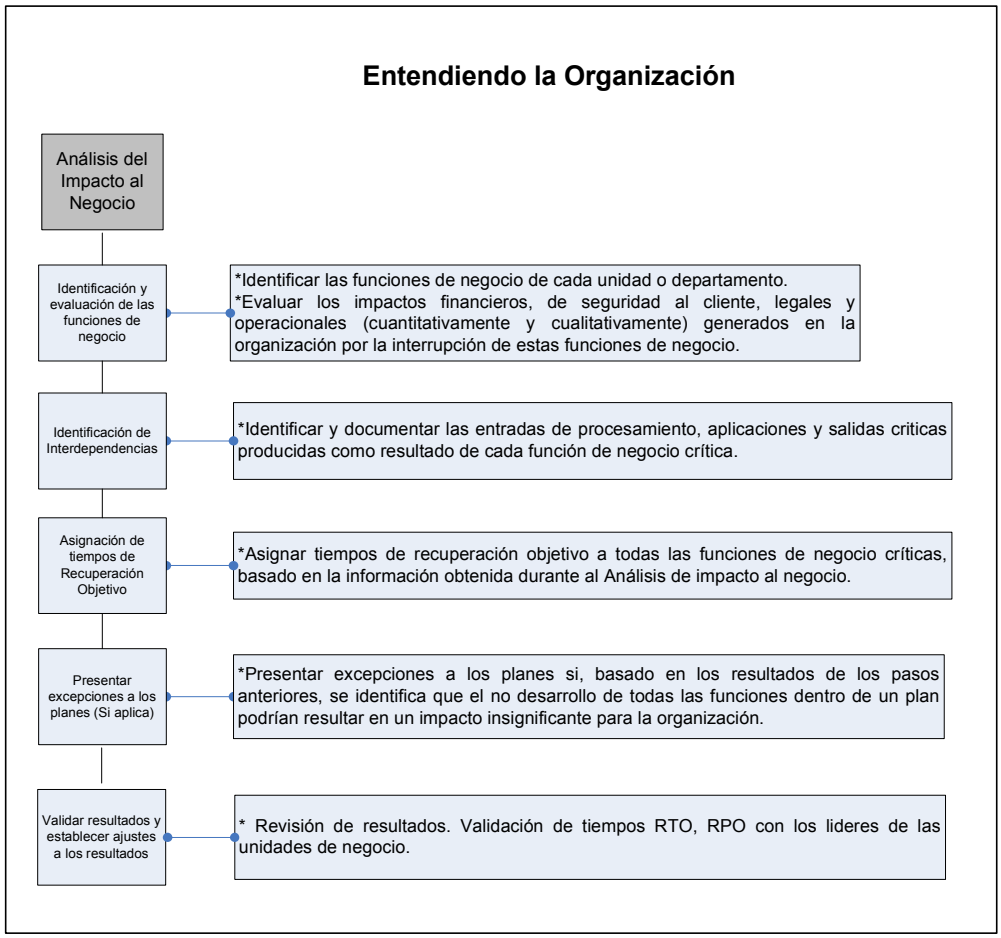

Figura No. 16 Actividades enmarcadas dentro del Análisis de Impacto al Negocio

¿Qué equipamiento especializado es usado en cada área y como es utilizado para el desarrollo de las funciones de negocio?

¿Cuáles son los tiempos mínimos que se deberían tomar para reemplazar el equipamiento crítico?

Si los sistemas no se encuentran disponibles, ¿cómo podrían continuar sus operaciones los departamentos?

¿Cuál es el recurso humano especializado mínimo y el espacio necesario para continuar las operaciones en otra instalación?

¿Qué elementos de comunicación (teléfonos, fax, equipamiento de transmisión de datos) podrían ser necesarios para continuar operaciones?

Es importante determinar el impacto de una interrupción sobre los sistemas críticos y funciones de negocio. El impacto depende del tipo de incidente que ocurra, y el tiempo hasta que las operaciones normales vuelvan a reiniciarse.

Para el presente trabajo se definió un formato que se debe seguir para el desarrollo del Análisis de Impacto al Negocio en una organización. Este formato se encuentra dentro de los documentos anexos con el nombre "Formato_Análisis_Impacto_al_Negocio.docx", el cual se diligencia para cada uno de los procesos identificados.

Con el Análisis de Impacto desarrollado se documentan las funciones críticas, impactos financieros y operacionales, exigencias de recuperación de procesos de negocio, procedimientos de backup, registros vitales, amenazas potenciales que afrontan los procesos y/o funciones de negocio, entre otros puntos.

La forma de trabajar o desarrollar las actividades para el desarrollo del BIA, se plantea a través de reuniones guiadas con los responsables de los procesos, los cuales son los entes claves para el estableciendo del Tiempo de Recuperación Objetivo (RTO), y el Punto de Recuperación Objetivo (RPO) para cada proceso y sus correspondientes sistemas de TI. Los impactos y riesgos para el negocio de una interrupción potencial se analizan con el fin de establecer prioridades de recuperación. También se identifican las interdependencias críticas, tanto internas como externas en la organización por cada proceso.

La tabla siguiente describe algunas de las actividades específicas al realizar el Análisis de Impacto por proceso [5] [18] [17]:

Descripción	Explicación
Actividades Clave	Conducir BIA y reunir la información requerida del negocio y del personal de tecnología que soporta las actividades mediante un proceso de entrevistas individuales. Identificar el tamaño de la función de negocio (ingresos totales, número de empleados, etc.). Identificar el propósito principal de la función de negocio (generación de ingresos, administración, servicio al cliente, soporte de función, etc.). Identificar las dependencias entre funciones de negocio, entre áreas o departamentos y entre sistemas. Identificar, categorizar y priorizar los procesos. Identificar los recursos mínimos de personal para una recuperación óptima.

Descripción	Explicación
	Identificar los registros vitales y los procedimientos de backup, los Planes Alternos de Operación (si existen), así como confirmar que las informaciones que deben replicarse en tiempo real (espejo) estén siendo contempladas dentro de la actual estrategia de DRP. Identificar las circunstancias y estrategias especiales para las funciones del negocio. Identificar los sistemas implicados en la ejecución de funciones críticos de negocio Confirmar la misión crítica del soporte de TI (la red, el hardware, el software) y los requerimientos para los procesos críticos del negocio. Recolectar información adicional para el desarrollo de las estrategias. Identificar dependencias internas y externas de los procesos del negocio o de tecnología. Identificar el "Tiempo de Recuperación Objetivo" (RTO) y el "Punto de Recuperación Objetivo" (RPO). Desarrollar un reporte BIA que detalle el estado actual de todas las áreas de negocio. Identificar los impactos financieros y operacionales de interrupciones imprevistas. Identificar impactos como en el servicio al cliente, por no cumplimiento con regulaciones del gobierno, no cumplimiento con contratos existentes, pérdida de ingresos, perdida de negocios, pérdida de imagen, otros impactos.
Premisas Clave	Es importante que en cada entrevista y/o cuestionario participe el siguiente personal clave: Líder del proceso Responsables operativos del proceso Analista de procesos designado Representante de Tecnología que apoya el proceso. Para que los cuestionarios se diligencien de una manera consciente y responsable, con el fin de que reflejen la real esencia y realidad del proceso en lo referente a la continuidad del negocio.

Descripción	Explicación
	La participación del área de Tecnología es vital.

3.3.2 ANÁLISIS DE RIESGOS

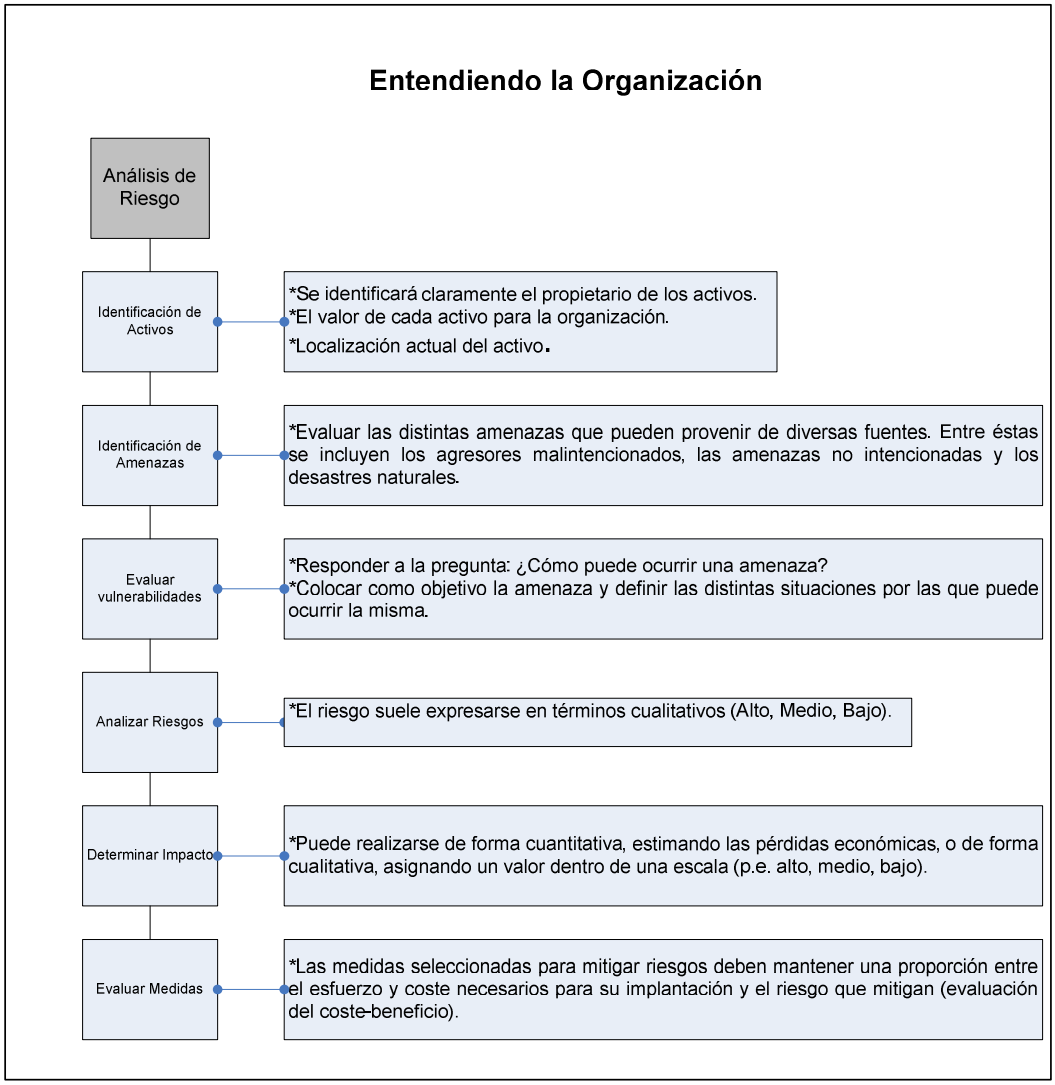

Figura No. 17 Actividades enmarcadas dentro del Análisis de Riesgo

La Gestión del Riesgo es un proceso que se articula con la Gestión de Continuidad de Negocio, pensando en que si la entidad es consciente de los riesgos que pueden poner en peligro la continuidad de sus operaciones, deberá realizar todos los esfuerzos razonables para evitar que los mismos se materialicen, disminuyendo así la

probabilidad de poner en práctica los planes de continuidad. Dentro de la gestión del riesgo se identifica, analiza, evalúa y se da tratamiento a los riesgos a que está expuesta la organización y sus partes interesadas.

El análisis de riesgos, parte de la premisa que a pesar de los esfuerzos de las organizaciones para evitar los siniestros, siempre habrá una posibilidad de que se presente un evento indeseado. Y de que los recursos disponibles en la organización no son suficientes en todos los casos frente a un evento de grandes proporciones que amenace la continuidad. De ahí la importancia de gestionarlos para minimizar su ocurrencia.

Las consecuencias de un riesgo no rutinario pueden generar una crisis y afectar la operatividad de la organización, las personas, las instalaciones, la economía del negocio, la imagen y el buen nombre de la organización, la operación, la información y el medio ambiente. Con la gestión óptima de este tipo de riesgo se espera que la organización minimice sus riesgos, cerrando así las brechas u oportunidades que puedan ocasionar una eventual suspensión de las operaciones y por ende del negocio.

La organización deberá actualizar anualmente el Análisis de Riesgo para Continuidad del Negocio con la participación de los miembros del Comité Directivo. Los resultados del análisis definirán ajustes al plan de acción de la Gestión de Continuidad del Negocio con el fin de cerrar las brechas identificadas.

3.3.2.1 MITIGACIÓN DE RIESGO

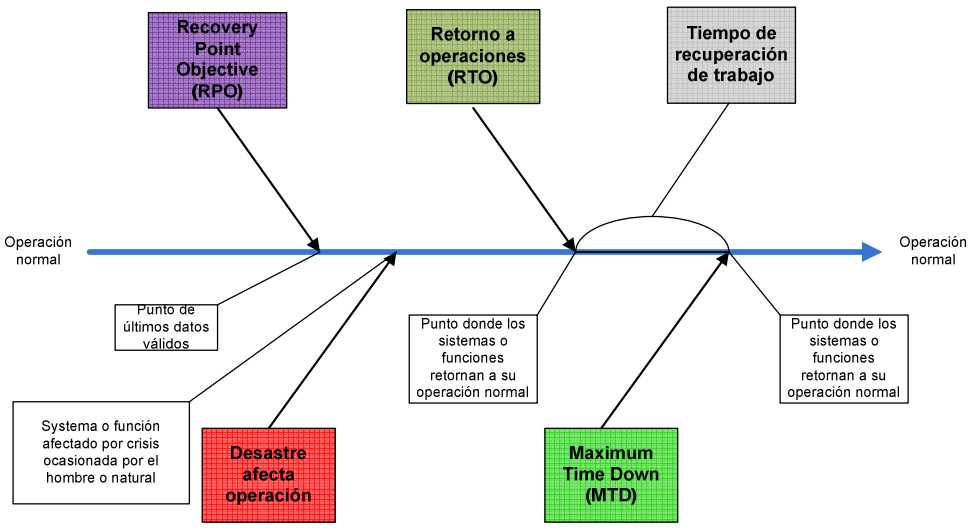

Figura No. 18 Línea de tiempo de recuperación de desastre

La línea de tiempo de recuperación de desastre mostrada en la siguiente figura ilustra los puntos elementales de riesgo que deben ser identificados, evaluados y priorizados por impacto y que incorporan la tolerancia establecida por el negocio.

3.3.3 DOCUMENTACIÓN FASE ENTENDIENDO LA ORGANIZACIÓN

En esta fase se deben generar o actualizar los siguientes documentos:

- Metodología de Análisis de Impacto al Negocio
- Documento de Análisis de Impacto al Negocio
- Metodología de evaluación de riesgos
- Resultados análisis de riesgos
  - Formatos
  - Gestión de activos
- Estrategias de continuidad
- Estructura de respuesta a incidentes
- Plan de Gestión de Incidentes
  - Planes, procesos y procedimientos para la activación, operación, coordinación y comunicación de la respuesta a incidentes
- Planes de Continuidad del Negocio

3.4 DETERMINACIÓN DE LA ESTRATEGIA DE GCN

La determinación de la estrategia para la Continuidad del Negocio depende en gran medida del resultado del Análisis de Impacto al Negocio y Análisis de Riesgo. En estas actividades se identifica la plataforma crítica y se definen los tiempos claves para la reanudación de la operación en caso de falla.

La primera etapa durante esta fase es la identificación de opciones de recuperación que permitirían a la organización alcanzar sus objetivos de Continuidad del Negocio, política de Gestión de Continuidad, así como con el cumplimiento de los acuerdos de nivel de servicio que se han establecido tanto a nivel de operaciones, procesos como de infraestructura y servicios de TI. El documento "Formato_Desarrollo_Estrategias_Continuidad.docx" facilita el inicio de la identificación de las estrategias de continuidad para la organización

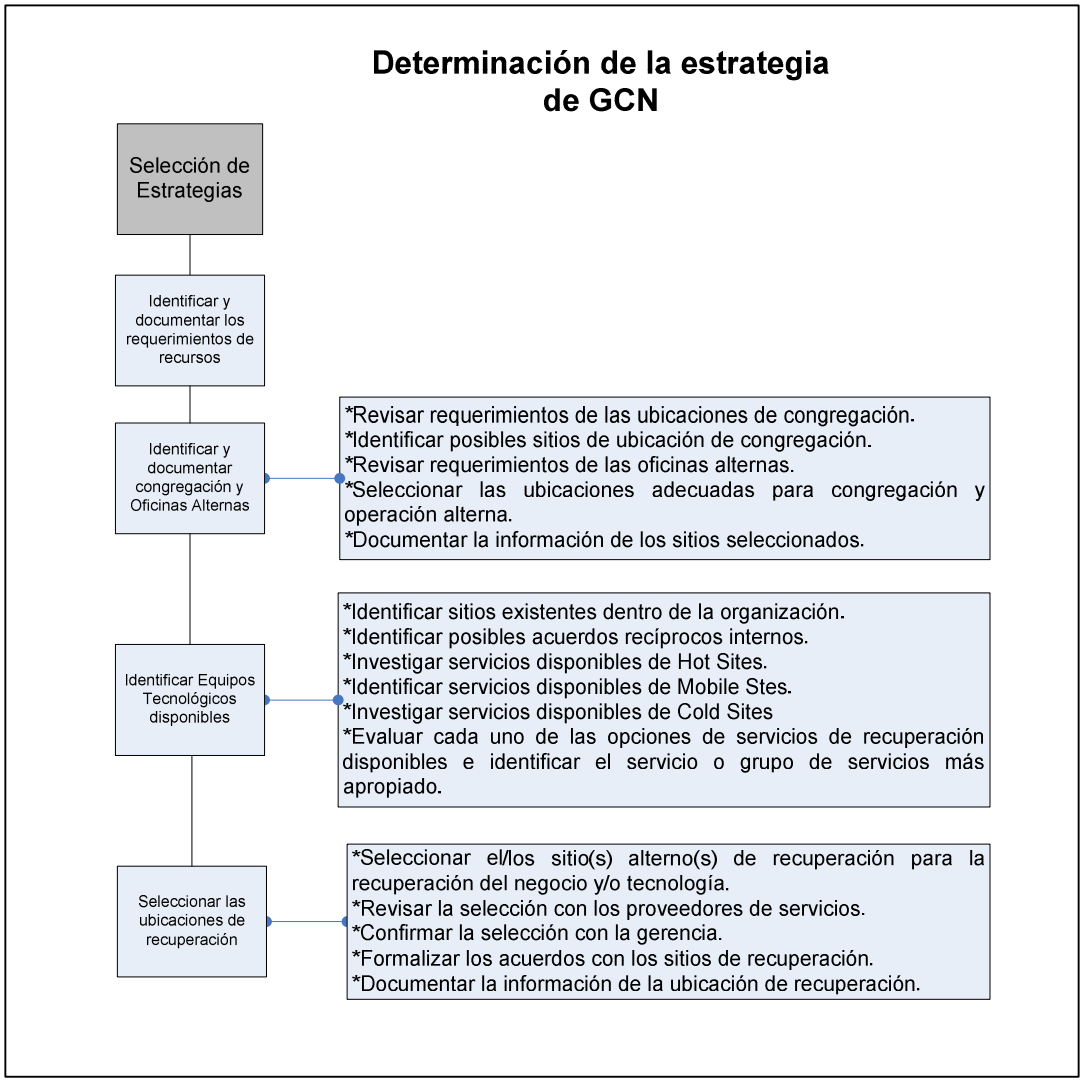

Figura No. 19 Determinación de la estrategia de GCN

La estrategia es desarrollada con las opciones de recuperación más apropiadas lo cual permitirá ser insumo principal para la definición de los Planes de Continuidad del Negocio en la organización.

La tabla siguiente describe las actividades específicas y las tareas:

Descripción	Explicación
Actividades clave	Revisión del “plan de recuperación de desastres” y “plan de contingencias” Facilitar la recolección de recursos y requerimientos para la selección de estrategias de recuperación de los procesos y/o actividades/tareas claves y determinar el peso apropiado de cada alternativa.

Descripción	Explicación
	Analizar las estrategias considerando los resultados del Análisis de Impacto en el negocio (BIA) con el fin de identificar las soluciones más realistas, viables y efectivas para la recuperación. Identificar estrategias y soluciones para responder a interrupciones imprevistas de las operaciones del negocio, con el fin de recuperar procesos de negocio identificados como críticos de acuerdo con lo establecido en los RTO/RPO definidos, identificando actividades de restauración para el regreso a niveles de operaciones establecidas por el BIA. Confirmar las estrategias de recuperación para los procesos críticos y los recursos y servicios necesarios de estos procesos de acuerdo con los resultados de BIA. Resaltar las implicaciones de cada opción de estrategia.
Premisas Clave	Es importante que en cada entrevista y/o cuestionario participe el siguiente personal clave: Líder del proceso. Responsables operativos del proceso. Analista de procesos designado. Representante de Tecnología que apoya el proceso.

La estrategia de continuidad integra los diferentes componentes críticos (equipos de recuperación, miembros de equipos, líderes, contactos de recursos críticos, configuración de infraestructura, etc.) de cada uno de los involucrados en las tareas de recuperación: Proveedores, Organización, Infraestructura Tecnológica y Entidades Externas. Estos se encuentran relacionados a continuación.

Los involucrados en la Estrategia son:

Proveedores (Servicios y Productos).

Entidades Externas.

Equipos de recuperación.

Infraestructura (Plataformas).

Planes de Recuperación.

En el marco general de la estrategia de continuidad se definen tres fases: una preventiva, una de respuesta al incidente y la correspondiente a la recuperación de la operación normal.

Tareas Preventivas

Operación Normal para Continuidad: Procedimientos para garantizar la disponibilidad de la infraestructura para los servicios que entrarán en un incidente. (Ej. Ampliación niveles de atribuciones, transferencia del conocimiento, elevar montos caja menor, mantenimiento preventivo y correctivo de equipos).

Tareas de Respuesta (Manejo de Incidentes y Movilización)

Manejo de Incidentes: Procedimientos que documentan y facilitan la toma de decisiones por parte de los equipo de Gestión de Incidentes ante cualquier evento que pueda ocurrir con los niveles de servicio que sean establecidos.

Movilización: Procedimientos que documentan las tareas específicas para trasladar la operación al Centro de Operaciones de Contingencia.

Tareas de Recuperación (Operación durante el Incidente y Retorno a la Normalidad)

Movilización: Procedimientos que documentan las tareas específicas para trasladar la operación al Centro de Operaciones de Contingencia.

Operación durante el incidente: Procedimientos para operar las funciones de negocio trasladadas en el Centro de Operaciones de Contingencia.

Ampliación de niveles de servicio respecto de los establecidos en las tareas de respuesta.

Retorno a la Normalidad: Procedimientos que documentan las tareas específicas para trasladar la operación total o parcial al sitio de Operación Normal y asegurar el almacenamiento de transacciones efectuadas durante el incidente y de esta forma, regresar a la normalidad.

Para cada plan de cada proceso identificado como crítico se presentan las tareas a ejecutar en cada una de estas fases, debidamente documentadas

3.4.1 DETERMINANDO OPCIONES DE RECUPERACIÓN

Las opciones deberían ser determinadas teniendo en cuenta los siguientes puntos [17]:

- Staff (incluyendo habilidades y conocimiento)
- Premisas en operación (Locaciones de trabajo)
- Tecnología (Telefonía, datos, aplicaciones, sistemas)
- Provisiones (materiales y equipamiento)
- Stakeholders

Las estrategias adoptadas para continuidad del negocio son algo complejas y son típicamente alguna combinación de las siguientes alternativas de site [1].

- Provisión hecha con la organización (desplazamiento, trabajo remoto, acuerdos)
- Servicios entregados a la organización (unidades prefabricadas o ubicaciones móviles)
- Servicios provistos externamente por terceras partes
- Sitios alternos que son idénticos a los centros principales en todos los aspectos técnicos

La selección de opciones de recuperación de TI dependen de:

- Tiempos de recuperación objetivo para procesos que soporten las actividades críticas identificadas en el BIA
- Localización y distancia entre unidades de negocio a nivel organizacional y las opciones o sitios alternos
- Acceso remoto
- Opciones de telecomunicaciones configuradas (redundancia)

Estrategia de backup y acuerdos con proveedores.

3.5 DESARROLLO E IMPLEMENTACIÓN DE LA ESTRATEGIA DE GCN

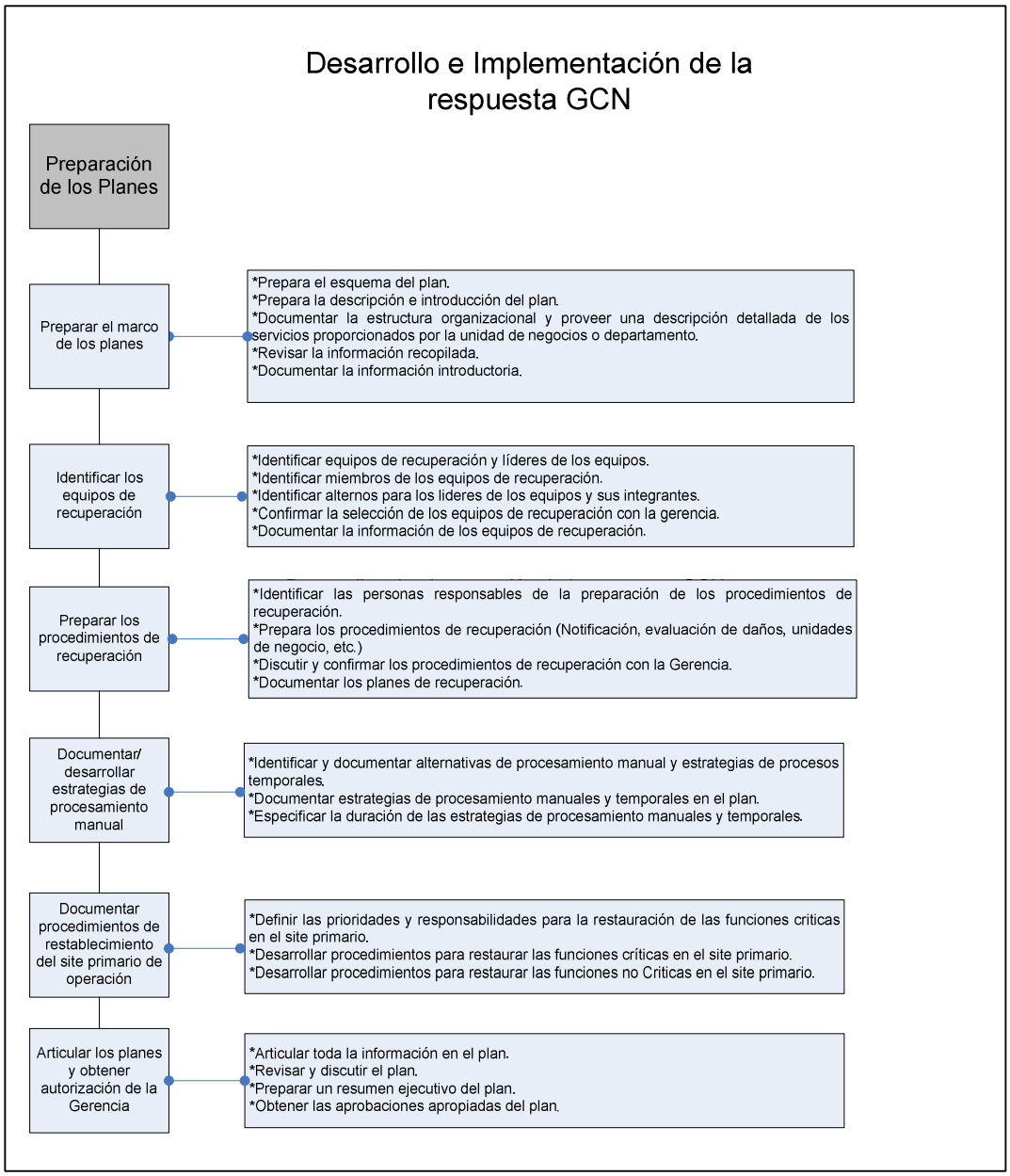

Figura No. 20 Determinación e implementación de la respuesta BCM

3.5.1 COMPONENTES DEL PROCESO DE GCN

La GCN utiliza diferentes tipos de componentes para proveer la cobertura apropiada y la gestión de los procesos definidos; estos componentes orientan a la GCN en el

desarrollo de su gestión y a la hora de presentarse un incidente que pueda afectar la operación de la organización. Estos componentes incluyen:

Gestión a nivel organizacional que incluye el programa de GCN, metas, objetivos y controles. Se definen:

Plan maestro

Plan de comunicaciones

Planes de procesos para facilitar la interacción con otros planes

Gestión a nivel operacional que incluye los planes de continuidad del negocio los cuales detallan paso a paso las acciones a tomar. Estos planes incluyen:

Plan de sitio (localización)

Sub - Planes con tareas especificas

3.5.1.1 PLAN MAESTRO (BCM)

El Plan Maestro es utilizado por las altas directivas para facilitar el desarrollo y activación de los planes de continuidad del negocio. Este plan se puede considerar como un documento integrador, el cual describe los planes de continuidad de forma puntual dentro de toda la organización, además de contener políticas, procesos, procedimientos y acciones necesarias ante algún incidente.

3.5.1.2 PLAN DE COMUNICACIONES (BCM)

Este plan debe ser creado para ser la primera sección dentro del Plan Maestro para asegurar la identificación de todos los recursos de GCN para los sitios y funciones los cuales serán cubiertos por los planes de continuidad (BCP) definidos.

Este plan debe incluir información de contacto como:

Identificación del EGCN, el Coordinador de Gestión de Continuidad, el Equipo de Gestión de Emergencias.

Identificación de las unidades de negocio

Identificación de los Coordinadores de Unidades de Negocio, por localización y función.

Identificación de contingencias externas, ubicaciones de emergencia, principales proveedores, vendedores, clientes clave e información de contacto en general.

3.5.1.3 PLAN DE PROCESO (BCM)

Este plan debería ser creado y ser una sección complementaria a el Plan Maestro BCP y al plan de comunicaciones para asegurar un estatus de reporte y ejecución a las actividades entre el EGCN y el Coordinador de Gestión de Continuidad del negocio.

Este plan notificara el estatus sobre las actividades adelantadas y asegurara que el EGCN se encuentra informado sobre el estado actual de la crisis o emergencia. Este plan debería incluir la siguiente información:

Requerimientos para todos los equipos
Reporte de estado
Pasos tomados por el Equito de Gestión de Emergencia, Coordinadores, EGCN.
Otras actividades requeridas durante la ejecución del BCP.

3.5.1.4 PLANES DE CONTINUIDAD DEL NEGOCIO (BCP)

Una vez se han definido las estrategias y han sido aprobadas por la Alta Dirección, Comité Ejecutivo de Gestión de Continuidad del Negocio entre otros, se debe iniciar el desarrollo del plan (o los planes de continuidad) respectivo. El BCP debe ser un conjunto de actividades, que correlacionen y respondan a las tres fases dentro de un incidente [17] (Figura No. 17):

Responder a un incidente, emergencia o desastre.
Recuperar actividades de negocio críticas.
Reanudar trabajo normal de todas las operaciones de negocio de acuerdo a las medidas adoptadas durante la recuperación.

El BCP incluye puntos como:

Identificación de las funciones de negocio y sus riesgos asociados, con los recursos necesarios para facilitar la ejecución de los planes definidos y la restauración de las funciones de negocio.
Los procesos, procedimientos, acciones, tareas y pasos necesarios para mitigar los riesgos identificados en los distintos escenarios.

Identificación de todas las locaciones, con los planes necesarios para proveer la cobertura adecuada ante cualquier incidente o interrupción que se presente.

Un proceso de comunicaciones para identificar, evaluar, declarar y recuperar de las causas de pérdida de servicio más típicas que incluye los recursos, roles, locaciones, con información y guías necesarias.

Los procesos para los planes de continuidad actualizan sensibilización, entrenamiento y pruebas.

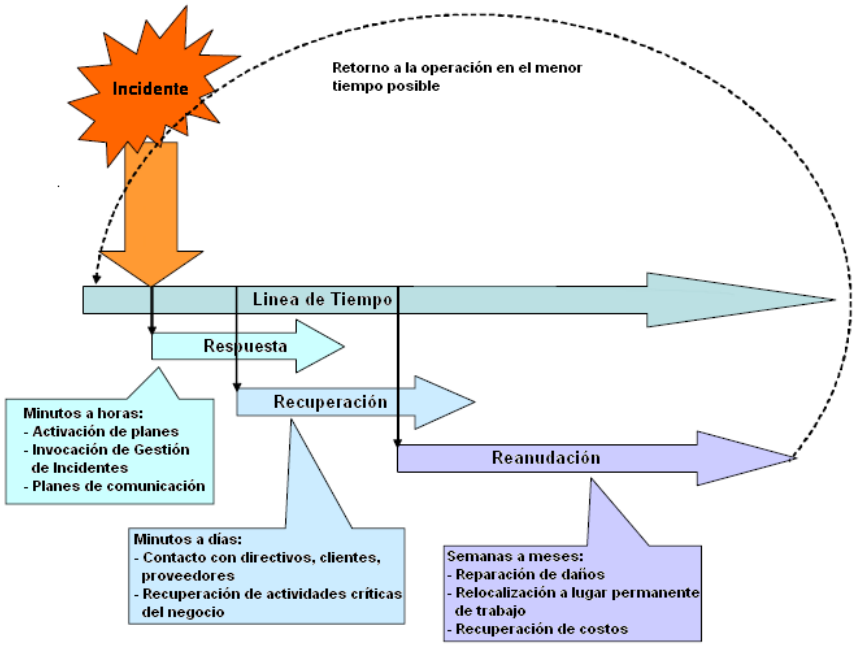

Figura No. 21 Determinación e implementación de la respuesta BCM

3.5.1.4.1 DOCUMENTOS DENTRO DE UN BCP

La estructura de un BCP puede variar dependiendo de la organización, su tamaño, objeto de negocio, ubicación geográfica entre otros. Sin embargo existen ciertos puntos comunes a considerar dentro de un Plan de Continuidad del Negocio.

3.5.1.4.2 PLAN DE RESPUESTA A INCIDENTES

Este plan entra en ejecución una vez se ha presentado un incidente y su enfoque clave está dirigido a la seguridad y salud de las personas que hacen parte de la organización. Este plan relaciona detalles como:

La estructura del Equipo de Respuesta a Incidentes.
Miembros del Equipo de Respuesta a Emergencias.
Roles y responsabilidades.
Proceso para toma de decisiones y escalamiento.

3.5.1.4.3 PLAN DE GESTIÓN DE INCIDENTES

Este plan detalla como el incidente puede ser gestionado desde su punto de ocurrencia a la operación normal y provee información acerca de la estructura del equipo de gestión de incidentes (proceso de Gestión de Incidentes según ITIL), el criterio para invocar Continuidad del Negocio, la gestión del incidente, requerimientos de recursos.

3.5.1.4.4 PLANES DE RECUPERACIÓN DE NEGOCIO

Son los planes usados por los equipos de recuperación que incluyen información para la recuperación a bajo nivel de servicios de TI y propios para cada área o departamento dentro de la organización. También definen roles para área como:

Recursos humanos
Salud
Seguridad
Legal
Evaluación de daños

3.5.1.4.5 PLANES DE REANUDACIÓN DE NEGOCIO

Mientras la continuidad del negocio se enfoca en adoptar medidas temporales (como relocalización, reducción de horas de trabajo, reducción de personal, utilización de sistemas backup), la reanudación de negocio se relaciona con restaurar las operaciones a niveles de operación normales.

La reanudación puede ser del sitio original a una nueva localización (dependiendo del daño) y necesitara ser tratada como un programa donde se deben manejar diferentes prioridades para no ver afectadas las funciones del negocio. El plan detalla la secuencia, partes y otras consideraciones como (seguridad, tiempos, medidas intermedias, comunicación, etc.)

3.6 MONITOREANDO Y REVISANDO EL SGCN

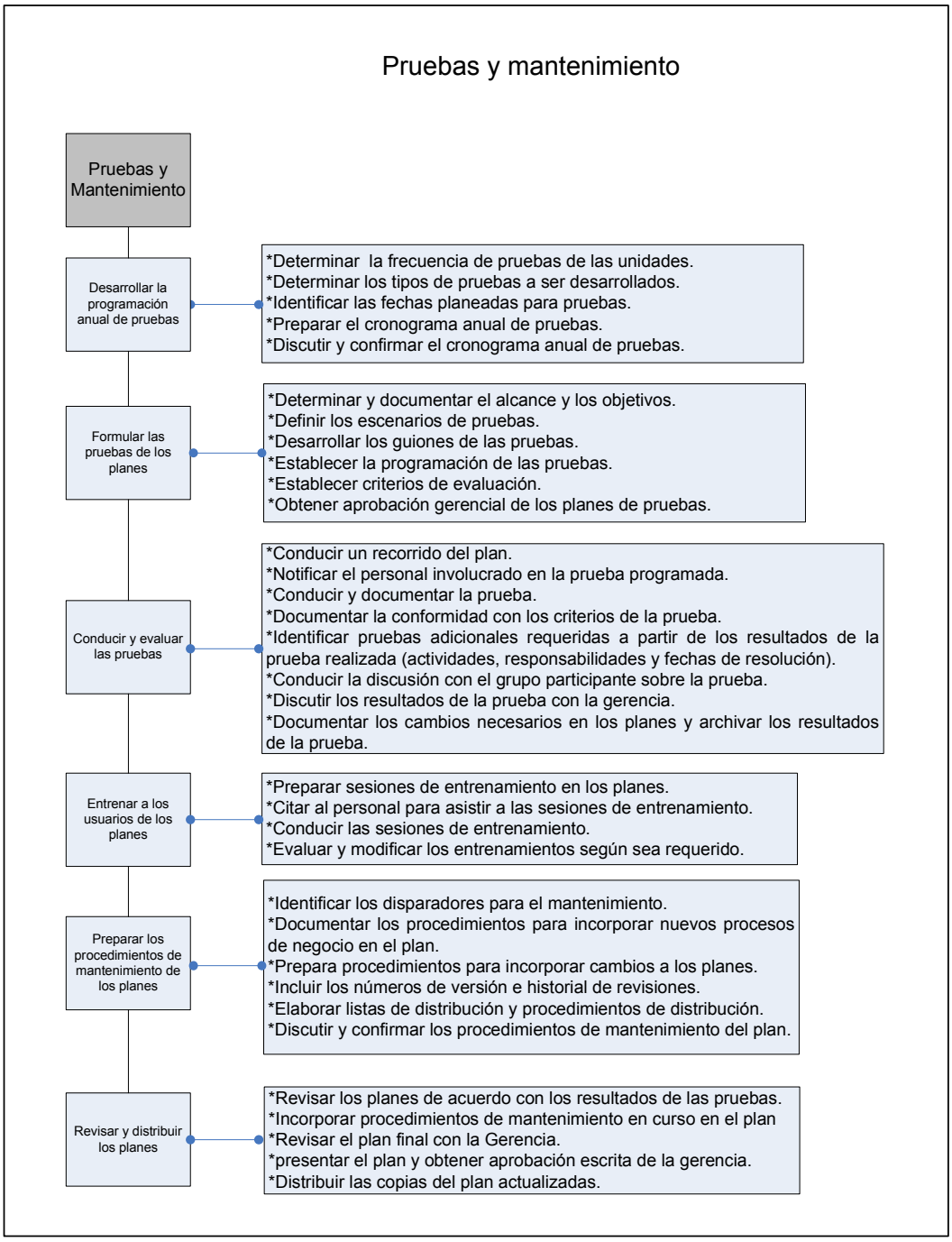

Figura No. 22 Pruebas y mantenimiento

Con el fin de verificar la eficacia continua de las previsiones de la GCN y proporcionar mayor certidumbre tras producirse un incidente de que las actividades críticas serán recuperadas según sea preciso, es necesario contar con:

Una programación (intervalos) de ejecución de pruebas del plan de continuidad del negocio y cuando se produzcan cambios significativos al plan.
Definir los objetivos y metas de cada prueba.
Plan de revisión luego de las pruebas para validar consecución de objetivos y metas del ejercicio.
Elaborar informe.

El Plan de Pruebas debe ejercitar:

Los sistemas técnicos, logísticos, administrativos, procedimentales y otros operativos de la GCN.
Infraestructura de GCN (incluyendo funciones, responsabilidades, y todos los lugares de gestión de incidentes y zonas de trabajo).
Validar la recuperación tecnológica y de telecomunicaciones, incluyendo la disponibilidad y traslado de personal.

Como premisas del Plan de Pruebas:

Deben ser realistas, estar planificadas cuidadosamente y pactarse con grupos de interés, de forma que exista el mínimo riesgo de interrupción a los procesos de negocio.
Deben tener objetivos y metas claramente definidos.
La envergadura y complejidad debe ser apropiada a los objetivos de recuperación.
Los planes de continuidad y de incidentes deben ejercitarse para asegurar que pueden ejecutarse correctamente y que contengan datos e instrucciones apropiadas.

3.6.1 OBJETIVO DE LAS PRUEBAS

La organización a través de las pruebas programadas, busca:

Determinar el estado de preparación de la organización de recuperación para responder y recuperarse de una interrupción del negocio y las operaciones de los sistemas.

Determinar si están disponibles los recursos requeridos (identificados en el análisis de impacto sobre el negocio) para la recuperación en los sitios de recuperación.

Determinar si el plan (planes) de continuidad del negocio ha sido adecuadamente mantenido para reflejar los cambios en el negocio y en tecnología (actividades de mantenimiento).

Inculcar sentido de calma y confianza dentro de la empresa mostrando que hay buen estado de preparación demostrable para una interrupción potencial de los servicios.

Demostrar que se cumple con los requerimientos regulatorios aplicables.

3.6.2 TIPOS DE PRUEBAS

Los ejercicios se clasifican con base en el grado de recursos reales que se están empleando y la manera en las cuales se van probando. Para el presente proyecto se da un ejemplo de prueba de escritorio la cual se encuentra en el documento "Formato_Prueba_Escritorio.xlsx". Se pueden considerar los siguientes tipos de prueba [17]:

TIPO DE PRUEBA	FUNCIÓN DE PRUEBA	PARTICIPANTES	FRECUENCIA	COMPLEJIDAD
Chequeo de escritorio	Desafío y evaluación de calidad del contenido del BCP	Autor del plan, coordinadores	Una vez al año	Baja
Tutorial de escritorio	Revisión del contenido del BCP	Autor del plan y principales participantes en el plan	Una vez al año	Baja
Escenario de escritorio	Utilización de un escenario para recorrer el plan y validar que contiene la información necesaria para permitir	Participantes en el plan, observadores, facilitadores	Una vez al año	

	una recuperación exitosa			
Prueba de comunicaciones	Evaluar los números de contacto establecidos en los árboles de llamadas y en los planes	Árbol de llamadas	Dos veces al año	Baja
Ejercicio de escenario	Utilización de un escenario con el fin de probar la validez de los planes de gestión de incidentes y de continuidad del negocio.	Participantes en los planes, observadores y facilitadores	Anualmente o dos veces en el año	Media
Evaluación técnica	Evaluar la efectividad de los planes de recuperación sobre los sistemas tecnológicos.	Equipo de gestión de TI e infraestructura, observadores	Anualmente	Media
Evaluación completa	Prueba simulando un incidente que afecta totalmente las operaciones del negocio y sus instalaciones principales	Todo el personal, todos los equipos definidos, observadores	Anualmente	Alta

3.6.3 DOCUMENTACIÓN FASE EJERCICIO, MANTENIMIENTO Y REVISIÓN

En esta fase se deben generar o actualizar los siguientes documentos:

Programa de ejercicio aprobado por la dirección

Plan de pruebas técnicas

Objetivo de cada una de las pruebas

Resultados de las pruebas ejecutadas (Reporte)

Programa de revisión de los requerimientos de GCN

Reportes e informes de revisión al SGCN

Plan de auditorias

Resultado de auditorías internas al SGCN

Resultado de auditorías externas al SGCN

Procedimiento para realizar la revisión del SGCN por la Gerencia.

Procedimiento para realizar la revisión del SGCN por el Coordinador de Gestión de Continuidad.

Procedimiento para realizar auditorías internas..

Procedimiento para realizar auditorías externas

3.7 MANTENIMIENTO Y MEJORA DEL SGCN

Como fase final durante el diseño e implementación del SGCN se encuentra la mejora continua. Durante esta fase se busca generar acciones tanto correctivas como preventivas.

3.7.1 ACCIÓN CORRECTIVA

El objetivo de estas acciones es eliminar la causa de no conformidades y problemas asociados con los requisitos del SGCN (Estas no conformidades son el resultado de las auditorías realizadas dentro del seguimiento y revisión del SGCN), con el fin de prevenir que ocurran nuevamente.

Determinar y evaluar las causas de las no conformidades del SGCN

Diseñar e implementar la acción correctiva necesaria.

Revisar la acción correctiva tomada.

Registrar los resultados de las acciones tomadas.

3.7.2 ACCIÓN PREVENTIVA

El objetivo de las acciones preventivas es eliminar la posibilidad de ocurrencia de no conformidades potenciales con los requisitos del SGCN. Los procedimientos necesarios para esta acción son:

Determinar y evaluar las causas de las no conformidades potenciales.

Diseñar e implementar la acción preventiva necesaria.

Revisar la acción preventiva tomada.