PROCESO DE DIAGNÓSTICO PARA LA IMPLEMENTACIÓN DE ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO EN LA DIRECCIÓN DE OPERACIONES DE UNE EPM TELECOMUNICACIONES

HÉCTOR DANIEL ZAPATA ATEHORTÚA - 71.260.445
CRISTYAN CAMILO ECHEVERRY BARRERA - 98.704.274

UNIVERSIDAD DE MEDELLÍN
ESPECIALIZACIÓN EN ALTA GERENCIA
COHORTE 45
MEDELLÍN
2011

PROCESO DE DIAGNÓSTICO PARA LA IMPLEMENTACIÓN DE ESTRATEGIAS DE CONTINUIDAD DE NEGOCIO EN LA DIRECCIÓN DE OPERACIONES DE UNE EPM TELECOMUNICACIONES

HÉCTOR DANIEL ZAPATA ATEHORTÚA - 71.260.445
CRISTYAN CAMILO ECHEVERRY BARRERA - 98.704.274

Trabajo de grado presentado como requisito para optar al título de Especialista en Alta Gerencia

Asesor metodológico:
MARIA CECILIA ARCILA GIRALDO

Asesor temático:
JUAN CARLOS RAMIREZ G.

FACULTAD DE CIENCIAS ADMINISTRATIVAS
UNIVERSIDAD DE MEDELLÍN
MEDELLÍN
2011

PAGINA DE ACEPTACION

_____

JUAN CARLOS RAMIREZ GONGORA

Asesor Temático

_____

MARIA CECILIA ARCILA GIRALDO

Asesor Metodológico

Medellín, septiembre de 2011

AGRADECIMIENTOS

Agradecemos a todas las personas que de alguna forma nos apoyaron y ayudaron en la realización de esta monografía, especialmente a nuestros compañeros de UNE que aportaron todo su conocimiento y experiencia en el tema.

CONTENIDO

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE GRAFICOS

Pág.

LISTA DE TABLAS

Pág.

RESUMEN

La propuesta que se plantea en esta monografía se desarrolla para afrontar la exigencia actual del mercado de las TIC por garantizar un excelente nivel en la prestación de los servicios. La gran cantidad de oferta hace que el mercado se vuelva cada día más competitivo y es en este punto donde la preparación de las compañías para afrontar eventos que comprometan los niveles de calidad se vuelve definitiva y un gran factor diferenciador. Pasa en algunos casos, que solo hasta que se enfrentan a una crisis, es que se dan cuenta que un proceso de continuidad de negocio era el factor clave podría haber evitado la situación de quedar fuera del mercado.

Es por este motivo que a través de los tres capítulos se presenta toda una metodología que permite evaluar el diagnóstico actual de los procesos de operaciones de la compañía y proponer unas estrategias correctivas, todo esto basándose completamente en los conceptos de la administración de la continuidad de negocio.

Primero se establece un background general sobre todo el concepto de continuidad de negocio y luego se realiza un diagnóstico de los procesos basados en la metodología. Finalmente se presentan los resultados y se sugieren unas estrategias buscando siempre minimizar el riesgo y generar una cultura de continuidad de negocio a través de los procesos críticos de la operación.

ABSTRACT

The proposal developed in this monograph rises to meet the current demands of TIC’s market to ensure excellent standards in services delivery. The great services offer makes the market becomes increasingly competitive and it is at this point that companies preparation to face events that compromise the quality levels becomes essential and a great differentiator. It happens in some cases that, only until they face a crisis, they realize that a process of business continuity could have been the key factor that might have prevented the situation and keep them on stage.

It is because of this reason that through all three chapters we present a methodology to evaluate current diagnosis of the processes of the company's operations and propose corrective strategies, all based entirely on the concepts of Business Continuity Management

Firstly, we establish a general background on the whole concept of business continuity followed by a diagnosis based on the methodology process. Finally, we present the results and suggest strategies always looking to minimize risk and create a culture of business continuity through the critical processes of the operation.

GLOSARIO

AMENAZA: Persona, situación o evento natural del entorno (externo o interno) que es visto como fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos, virus, sabotaje, aplicativos mal diseñados, errores humanos, fallo de equipos, entre otros. (Gobierno en Línea, Ministerio de Comunicaciones, 2009).

BCM: Proceso de administración holístico que identifica impactos potenciales que amenazan una organización y que provee un marco de referencia flexible para una efectiva respuesta a la emergencia protegiendo los intereses de los accionistas (stakeholders), la reputación, marca y actividades que generen valor.

CONTROL: Cualquier acción que ayude a reducir la probabilidad de ocurrencia de un riesgo o permita reducir el impacto en caso de que este ocurra (Gobierno en Línea, Ministerio de Comunicaciones, 2009).

IMPACTO: Se puede definir como las consecuencias para el negocio dado el daño del activo o como la evaluación del efecto o consecuencia del riesgo. Generalmente, la implicación del riesgo se mide en aspectos económicos, financieros, integridad e imagen de las personas o empresas, disminución de capacidad de respuesta y competitividad, interrupción de operaciones, entre otros (Gobierno en Línea, Ministerio de Comunicaciones, 2009).

PROBABILIDAD: Se puede definir como la cifra que expresa el grada de que un hecho de que sea absolutamente seguro de que ocurra o no y se expresa cualitativamente como bajo, medio, alto y extremo y cuantitativamente como 0 y 1. (Gobierno en Línea, Ministerio de Comunicaciones, 2009).

PROCESOS: Un proceso es un conjunto de actividades o eventos (coordinados u organizados) que se realizan o suceden (alternativa o simultáneamente) bajo ciertas circunstancias con un fin determinado. Este término tiene significados diferentes según la rama de la ciencia o la técnica en que se utilice.

RESILIENCE: Este término sirve para indicar que algo puede sufrir un fallo y a pesar de ello seguir operando. Muchas veces se utiliza como si fuera un valor absoluto y, sin embargo, como sucede con los términos "cerca" o "lejos" el concepto de robustez es relativo y su alcance debe ser definido en cada utilización. Ejemplo: La duplicación del suministro eléctrico mejora la robustez ó resistencia de las instalaciones frente a cortes de electricidad, pero el lugar puede volverse inservible si el fallo eléctrico afecta a ambos suministros.

RIESGO: El riesgo se define como el evento que puede ocasionar un daño a un activo. Para determinar la probabilidad de ocurrencia de posibles eventos adversos, las amenazas deben ser analizadas en conjunto con las vulnerabilidades potenciales y los controles implementados. Es decir que el riego es directamente proporcional a la probabilidad y el impacto. (Gobierno en Línea, Ministerio de Comunicaciones, 2009).

TECNOLOGÍA: Es el conjunto de conocimientos técnicos, ordenados científicamente, que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de las personas.

VULNERABILIDAD: Es una debilidad que puede ser ejecutada accidentalmente o explotada intencionalmente, esta debilidad puede ser causada por la falta de uno o varios controles, que puede permitir que la amenaza ocurra y afectar el objeto de evaluación. Ejemplo: deficiente control de accesos, administración deficiente de la continuidad, poco control de versiones de software, ausencia de entrenamiento

cruzado (respaldo de personas), políticas inexactas e insuficientes, entre otros. Una vulnerabilidad por si misma no produce daño, es una condición para la amenaza afecte el activo (Gobierno en Línea, Ministerio de Comunicaciones, 2009 - Plan de continuidad de negocio, UNE - 2009).

INTRODUCCIÓN

En los últimos años se ha incrementado la preocupación del mercado y los entes regulatorios por la entrega de productos y servicios que las Compañías prometen a sus clientes en tiempo, condiciones contratadas y compromisos adquiridos; por lo que han establecido leyes, normas y estándares que velan por la promesa hecha a los clientes. Los clientes a su vez, demandan la entrega de servicio con mayor efectividad y calidad, en el tiempo en que lo necesitan y con la atención oportuna. No quieren escuchar explicaciones técnicas sobre las causas que afectaron los servicios y no quieren esperar que la Compañía esté disponible o recuperada.

A pesar de los efectos negativos de no contar con un plan de gestión de la continuidad de negocio, muchas empresas aún no toman medidas para implementar las estrategias que les permitan asegurar los procesos que generan valor y en consecuencia garantizar la sostenibilidad de la empresa a largo plazo.
UNE EPM TELECOMUNICACIONES al ser una empresa en el mercado de las TIC es en gran parte dependiente de la tecnología y compite en escenarios complejos debido a la globalización, se hace más susceptible a que una serie de amenazas puedan penetrar sus vulnerabilidades y causarle daño, al grado de dejarla fuera del mercado.

Para la empresa, mantener continuidad de los servicios administrando la continuidad del negocio más que un cumplimiento regulatorio, es un elemento estratégico y táctico que permite afrontar el reto por mantenerse en un mercado cada vez más competido, y el cual debe ser asumido por las Compañías para mantener la fidelidad de sus clientes, y por supuesto, mantener un crecimiento sostenible y rentable.

OBJETIVOS

OBJETIVO GENERAL

Crear una herramienta de diagnóstico y evaluación que permita identificar posibles amenazas, vulnerabilidades e impactos en la entrega de productos y servicios, dentro de los procesos que generan valor en la operación de UNE EPM TELECOMUNICACIONES según los estándares de continuidad de negocio.

OBJETIVOS ESPECÍFICOS

Contextualizar y familiarizar a los usuarios de este proyecto de investigación con el proceso, objetivos, elementos y conceptos básicos de continuidad de negocio según los estándares definidos por el Business Continuity Management Institute.

Definir la metodología que se debe utilizar para realizar el diagnóstico de los procesos y mostrar los resultados obtenidos permitiendo conocer el estado actual de los procesos de operaciones en los cuales implementaremos continuidad de negocio.

Definir las estrategias que se deben usar para asegurar la continuidad del negocio basándose en el diagnóstico del estado actual de los procesos analizados.

ALCANCE

Este proyecto se enfocará en proponer una metodología de diagnóstico organizacional que permita implementar las estrategias necesarias para mantener la continuidad de negocio en los procesos críticos de la Dirección de Operaciones de UNE EPM TELECOMUNICACIONES.

Se indicarán los elementos que hacen parte del proceso de evaluación y finalmente tendremos como resultado una lista de chequeo que podrá ser interpretada y aplicada por la alta gerencia de la compañía en la toma de las decisiones necesarias para implementar continuidad de negocio.

Este proyecto tendrá una duración de un año que es consecuente a la velocidad de cambio en el mercado de las TIC’s. No está dentro del alcance de este proyecto sino que es responsabilidad de la empresa, generar un plan de mantenimiento posterior donde se vayan reflejando los cambios de la compañía, el sector y el mercado.

JUSTIFICACIÓN

Este proyecto brindará herramientas a la dirección de UNE EPM TELECOMUNICACIONES para mantenerla funcionando a pesar de los factores que puedan afectarla, ofreciendo elementos que permitan identificar y focalizar la necesidad de contar con un sistema de gestión de continuidad de negocio con el fin de apoyar la gestión de la dirección de la organización y mantener las continuidad en sus operaciones y servicios.

En esta herramienta se definirán elementos que le permitirán a la organización gestionar el caos y el riesgo para mantener y mejorar la confiabilidad, disponibilidad y recuperabilidad requerida para dar soporte a los procesos críticos del negocio.

En el aspecto académico nos permitirá poner en práctica las teorías de gestión de procesos y gestión de indicadores aprendidas durante la especialización, desarrollar nuestras habilidades de investigación y generar ideas que aporten valor en los procesos de decisión de la alta gerencia de la compañía.

A nivel personal nos permitirá desarrollar nuestras habilidades gerenciales haciendo uso de las nuevas perspectivas aprendidas y la forma como afrontamos los proyectos e iniciativas organizacionales en las cuales podremos participar y aportar activamente.

1. CONTEXTUALIZACIÓN EN CONTINUIDAD DE NEGOCIO

1.1 DEFINICIÓN DE CONTINUIDAD DE NEGOCIO

1.1.1 Definición. La Administración de Continuidad de Negocio o también conocida como BCM (Business Continuity Management) es definida como “un proceso de administración holístico que identifica impactos potenciales que amenazan una organización y que provee un marco de referencia flexible para una efectiva respuesta a la emergencia protegiendo los intereses de los accionistas (stakeholders), la reputación, marca y actividades que generen valor”.

La gestión de Continuidad de Negocios contiene elementos para reducir el riesgo ante un evento, como responder ante tal evento y lo que se hace para recuperarse después del evento (funciones criticas principalmente).

La BCM debe desarrollarse desde dentro de la Organización y debe ser un proceso formal como cualquier otro de negocio. Busca proveer a la Organización de un estado real de preparación para responder a una contingencia e identifica los impactos potenciales de una amplia gama de interrupciones súbitas que afecten la capacidad de operación normal de la organización. También debería enfocarse en soportar pérdidas significativas de recursos, como personal o maquinaria.

Al identificar por adelantado los posibles impactos de una amplia gama de incidencias que trastornarían de forma súbita el éxito de la organización, establece prioridades para los esfuerzos de los especialistas en implantar robustez en sus respectivas áreas de especialización, como seguridad, instalaciones y tecnologías de la información.

Debido a que la capacidad de resistencia de la BCM de una organización depende de su equipo de gestión y su personal, además de su tecnología y la diversificación geográfica, se debe desarrollar esta capacidad de recuperación a todos los niveles de la organización, desde la alta dirección hasta el nivel operativo, y en todos los demás integrantes de la cadena de valor.

El factor determinante de esta robustez en toda la organización se sustenta en la responsabilidad de la alta dirección de proteger los intereses a largo plazo del personal, clientes y todos aquellos que dependen de algún modo de la organización. Si bien se pueden calcular las pérdidas financieras ocasionadas por una interrupción, generalmente el mayor daño suele reflejarse en una pérdida de imagen o de confianza fruto de un incidente mal gestionado. Del mismo modo, un incidente bien gestionado puede mejorar la imagen de la organización y su equipo de gestión.

En defensa de la Gestión de Continuidad de Negocio

“No nos pasará”, “Aguantaremos, como siempre lo hemos hecho”, “Somos demasiado grandes para fracasar” y “No somos un objetivo para los terroristas” son algunas de las respuestas más frecuentes que dan las empresas cuando se les cuestiona acerca de su falta de preparación. Otros creen que las empresas de seguros van a pagar por todo. La mayoría piensa que no dispone de tiempo para prepararse para algo que nunca sucederá. El gran número de negocios que se han hundido después de sufrir un incidente sugiere que estas respuestas se sustentan en premisas falsas.

Si bien las bombas, incendios e inundaciones acaparan los titulares de los medios de comunicación, el 90% de las incidencias que ponen en riesgo el negocio son "catástrofes silenciosas" que no figuran en los medios pero que pueden tener un efecto devastador para el buen funcionamiento de una organización. Muchas de

las causas son ajenas al control de la organización y suelen estar a merced de los servicios de emergencias o de proveedores que marcan los plazos de la interrupción.

A la hora de gestionar cualquier acontecimiento, el éxito se mide tanto por la respuesta técnica dada como por la competencia de su equipo gestor. Una investigación efectuada por Rory Knight y Deborah Pretty, de la firma Oxford Metrica, indica que las organizaciones que se ven afectadas por catástrofes se dividen en dos grupos muy claros: las que tienen capacidad para recuperarse y las que no. Cuando una organización ha lidiado una crisis con éxito el valor de sus acciones ha crecido en el largo plazo, mientras que aquellas que se considera que no han gestionado bien su crisis, vieron caer el precio de sus títulos y, pasado un año, seguían sin recuperarse.

Investigaciones más recientes demuestran que aquellas organizaciones que destinan un mayor presupuesto a control de riesgos, BCM y buen gobierno son las empresas más rentables en su sector, lo que indica que la BCM es una inversión, no un coste.

Un elemento clave para el éxito de los programas de BCM es que las distintas responsabilidades se asuman a los niveles apropiados de la organización. En estas empresas las implicaciones de la BCM se evalúan en todas las etapas del proceso de desarrollo de nuevos productos y forman parte del proceso de control del cambio.

¿Cómo beneficiará a mi organización?

El objetivo principal de la BCM es asegurar que la organización tiene una respuesta para los trastornos importantes que pondrían en riesgo su

supervivencia. Esto de por sí es suficientemente valioso, pero además incorporar la BCM en la gestión diaria puede aportar otras ventajas.

Ya sea por sus estatutos o por ley, algunas organizaciones tienen que incorporar BCM o, de forma más genérica, la "gestión de riesgos", como parte de sus obligaciones de buen gobierno corporativo. Un plan apropiado de BCM cumplirá con las obligaciones específicas y además constituirá una respuesta tanto a posibles incidentes específicos como a la creación de una "conciencia de riesgos" para la organización en su conjunto. No obstante la motivación principal para instaurar BCM no debe centrarse en las cuestiones de buen gobierno u obligaciones legales, sino que su puesta en marcha agrega valor a una organización y a los productos y servicios que ofrece.

“Para muchas empresas, la BCM tendrá en cuenta algunos…riesgos clave y les ayudará a cumplir con sus obligaciones". Nigel Turnbull, Presidente de Turnbull Committee acerca del buen gobierno corporativo en Reino Unido.

Las empresas que venden a otras empresas han recurrido a la BCM como una ventaja competitiva para lograr nuevos clientes y mejorar sus márgenes al incorporarla a su política de atención al cliente. Un repaso exhaustivo de las actividades a través de los ejercicios de Evaluación y Planificación de Impacto al Negocio puede poner en relieve las ineficiencias y destacar prioridades que de otra forma no hubieran nunca salido a la luz.

Las empresas que ofrecen productos o servicios saben que conservar a un cliente mediante un servicio más confiable es más barato que tratar de recuperar un cliente perdido después de una interrupción del negocio.

El espíritu de equipo que se crea durante la buena gestión de un incidente puede mejorar el resultado de un negocio mucho después de que el problema se haya solucionado.

"Muchas veces me preguntan cuál es el consejo más útil que puedo ofrecer en el mundo de los negocios. La respuesta es un sencillo y efectivo plan de continuidad de negocio que esté continuamente actualizado y probado". (Extraído de un discurso de Eliza Manningham-Buller, Directora General de MI5, en la Conferencia UK CBI, Noviembre 2004).

Relación con otras especialidades

Determinar cuáles son las responsabilidades de la Gestión de Continuidad de Negocio dentro de una organización concreta tendrá mucho que ver con la persona que se nombrará para estar a cargo así como de su experiencia previa en la materia. Esto puede significar que un responsable de Continuidad de Negocio puede considerar que la seguridad, la disponibilidad de TI o la gestión de riesgos constituyen las cuestiones clave, mientras restará importancia a otras áreas. Por esta razón es extremadamente difícil llegar a un acuerdo en cuanto a la lista general de responsabilidades específicas para la Gestión de Continuidad de Negocio. En concreto existen muchos debates acerca de su relación con la Gestión de Riesgos.

Se considera que, si bien se trata de facetas complementarias, los enfoques y métodos empleados en Continuidad de Negocio son muy diferentes de los dedicados a Gestión de Riesgos. La siguiente tabla trata de destacar las diferencias entre ambos.

Tabla 1. Diferencias entre gestión de riesgos y gestión de continuidad

	GESTIÓN DE RIESGOS	GESTIÓN DE CONTINUIDAD DE NEGOCIO
Método clave	Análisis de riesgo	Análisis de impacto sobre el negocio
Parámetros clave	Impacto y Probabilidad	Impacto y Tiempo
Tipo de incidente	Todo tipo de eventualidades generalmente segmentadas	Acontecimientos causantes de trastornos serios para el negocio
Magnitud del incidente	Toda magnitud (coste) de los acontecimientos. Generalmente segmentados	Para la planificación estratégica: sólo los incidentes que afectan a la supervivencia del negocio
Alcance	Se enfoca primordialmente en la gestión de riesgos para los objetivos del negocio principal	Se enfoca sobre todo en gestión de incidentes en su mayor parte externos a los aspectos fundamentales de negocio
Intensidad	Todas, desde graduales hasta súbitos	Acontecimientos súbitos o de rápida evolución (aunque es posible que la respuesta también resulte apropiada si un incidente persistente se transforma en severo)

La visión que se presenta en esta investigación pretende presentar la características esenciales de la Gestión de Continuidad de Negocio al mismo tiempo que entiende que los que las apliquen de forma concreta muchas veces tendrán, ya sea por sentido común o por órdenes recibidas, que ampliar su papel debido a la situación que desempeñen en la organización para la que trabajan.

1.1.2 Marco conceptual de BCM. En la Administración de la Continuidad encontramos tres áreas del conocimiento trabajando juntas:

- Administración de incidentes (Incident Management).
- Manejo de Crisis (Crisis Management).
- Recuperación del Negocio (Business Recovery).

Cada una de ellas es un área de conocimiento específico que se encarga de proveer los mecanismos de recuperación adecuados.

Administración de incidentes

Se encarga de detectar y evaluar la gravedad de un incidente que se presente para coordinar la respuesta más adecuada que lo resuelva, salvaguardando la vida e integridad de las personas y activos de una Organización en caso de desastre.

Entre sus disciplinas se encuentran la Respuesta a la Emergencia (ER), Protección civil, Seguridad física y de inmuebles. Las herramientas que se usan son el Sistema de manejo de incidentes y el Centro de Comando (CC).

Está área está encargada de definir e implementar el Plan de protección civil y seguridad física, el Sistema de administración de incidentes (ICS) y además velar por el cumplimiento de la normatividad respectiva.

El objetivo principal es la protección del recurso humano, la contención del incidente, la evaluación del evento ocurrido y la definición e implementación de las acciones apropiadas.

Entendemos como desastre cualquier evento súbito que rebasa la capacidad de respuesta del sistema. En un marco de negocios se considera como cualquier interrupción crítica de las funciones del negocio que resulte en impactos operacionales o financieros significativos y/o que requiera la reubicación a un lugar alterno.

Dentro de las acciones en la administración de incidentes encontramos las 4C.

- Confirmación (identificación).
- Contención.
- Control.
- Comunicación.

Dentro de las normas se encuentran definidas las tareas principales en el manejo de incidentes, los puntos claves a considerar y el contenido del Plan de administración de incidentes.

Manejo de crisis

Se encarga de detectar, evaluar, comunicar y resolver un evento de crisis dentro de una organización.

Entre sus disciplinas se encuentran la Evaluación y análisis de un evento de crisis, la Comunicación con los grupos de recuperación y el Manejo de medios informativos internos y externos. Se usan herramientas de notificación masiva y un Centro de Comando (CC).

Esta área está encargada de definir el Plan de administración de crisis, el Plan de comunicación interna y externa de crisis y además velar por el cumplimiento de la normatividad respectiva. Los grupos encargados de este proceso son el Comité de Crisis (CrC) y la Organización de Manejo de Crisis (CMO).

Por crisis podemos definir a cualquier evento en el que el flujo de efectivo disminuye, un evento negativo capaz de afectar las instalaciones, la seguridad de empleados o consumidores, las operaciones normales del negocio y que tiene el potencial de afectar la marca o una perdida importante en la participación del mercado.

El objetivo principal es construir una estructura de respuesta para la toma de decisiones con el fin de contener una crisis a tiempo, de manera organizada y efectiva, con base en procedimientos definidos, para contener un escalamiento público.

Dentro de las normas se pueden encontrar las definiciones de los tipos de crisis, las fases de una crisis, el sistema integral de manejo de crisis, la implementación del Centro de Operaciones de Emergencia (EOC) y el Incident Command System (ICS).

Recuperación del Negocio

Se encarga de identificar y reestablecer en el menor tiempo posible los procesos y la tecnología críticos de la Organización.

Entre sus disciplinas se encuentran el Análisis de riesgos, Continuidad de negocio (Procesos), la recuperación de desastres (Tecnología) y la Seguridad informática. Las herramientas que se usan son la Administración de riesgos operacionales e informáticos (ORM e IRM), la Administración de procesos de negocio (BPM) y las Tecnologías de información.

Esta área está encargada de realizar el Análisis de riesgos y el Análisis de impacto al negocio (BIA) e impacto en aplicaciones (AIA), definir el Plan de Continuidad de Negocio (BCP), el Plan de recuperación de desastres (DRP) y además velar por el cumplimiento de la normatividad respectiva.

El Plan de Continuidad de Negocio (BCP) es una colección bien documentada de procedimientos, que es desarrollada, compilada y mantenida, y que deben estar listos para usarse en un incidente, para permitir a una organización continuar la entrega de sus actividades críticas en un nivel predefinido aceptable.

El Plan de Recuperación de Desastres (DRP) era un conjunto de procedimientos de carácter técnico que estaban orientados a reanudar las aplicaciones que sustentan los procesos críticos del negocio. Hoy día, la norma que se encarga específicamente de la parte de tecnología es la BS25777-1 y ha sustituido el

término DRP por ICT–BC (Information & Telecommunication Technology – Business Continuity).

Dentro de las normas se encuentran las definiciones y estructura del BCP y el DRP.

1.2 PARA QUÉ SIRVE UN PLAN DE CONTINUIDAD DE NEGOCIO

La Continuidad de Negocio protege los procesos vitales de las actividades que generan ingresos a las empresas y organizaciones. Ante cualquier incidente crítico, se busca que los componentes esenciales de la organización sigan operando. Estas directrices son aplicables a todas las organizaciones sin importar el tamaño, sector y ubicación.

El diagnóstico para un plan de continuidad se establece con base a la información proporcionada, las evaluaciones y entrevistas realizadas. De aquí se desprenden actividades básicas para el diagnóstico como son la evaluación de riesgos, el análisis de impactos y la definición de estrategias.

1.2.1 Evaluación de riesgos. La actividad de evaluación de riesgos nombrada por sus siglas en ingles RA (Risk Assessment), busca determinar la probabilidad de que se presenten amenazas y/o vulnerabilidades que puedan impactar la operación normal de los procesos, las personas, la infraestructura tecnológica que soporta los procesos, y la infraestructura física donde se opera y que pueden llegar a afectar la continuidad del negocio.

Al realizar la evaluación de riesgos, el equipo profesional de continuidad tiene en cuenta la información recopilada mediante entrevistas, solicitud de información, análisis internos y externos, visitas guiadas a edificaciones, o cualquier aspecto que pueda generar interrupciones o afectar la operación normal. La evaluación de

riesgos se ha dividido en las cuatro dimensiones consideradas para mantener la continuidad, así:

- Procesos.
- Personas.
- Tecnología.
- Infraestructura física.

Los aspectos relevantes que se evalúan como posibles desestabilizadores de la continuidad en estas cuatro dimensiones, se presentan en forma general a continuación:

Dimensión de personas (Organización - Recursos Humanos)

- Administración del conocimiento (repositorios de soluciones, manuales, artículos, lecciones aprendidas).
- Entrenamiento y capacitación del personal.
- Entrenamiento cruzado.
- Segregación de funciones.
- Salud ocupacional (manejo de epidemias, virus).
- Índices de rotación de personal.
- Políticas de retención de personal.
- Política de comunicación formal.
- Trabajo en equipo, personal motivado, capacitado y comprometido.

Dimensión de procesos negocio (Operación)

- Definición de actividades y procesos interrelacionados.
- Definición de entradas y salidas de cada proceso.

- Definición, medición y gestión de indicadores de comportamiento del proceso.
- Definición de procedimientos alternos de trabajo.
- Actualización de los procedimientos y procesos base de operación.
- Claridad en roles y responsabilidades relacionadas con las operaciones críticas.
- Consideración de recursos de respaldo suficiente y necesario para cada actividad del proceso.
- Administración de proveedores de servicios profesionales y socios de negocio.
- Control y gestión de proveedores de servicio.
- Acuerdos de Nivel de Servicio medibles y confiables con proveedores, clientes internos y externos.
- Medición de tiempos y cantidad de recursos críticos.
- Gestión de calidad (disciplina de registro, documentación, comunicación, integración, evaluación).

Dimensión de tecnología

- Control, gestión y mantenimiento de servidores, bases de datos, redes, almacenamiento, aplicaciones, sistemas de información, datos, archivos y operación de usuarios.
- Procesos definidos e implementados para el soporte del servicio (administración de incidentes, administración de problemas, administración de cambios, administración de configuración, administración de versiones).
- Procesos definidos e implementados para la entrega del servicio (administración de capacidad y desempeño, administración de continuidad de la tecnología de información y comunicación, administración de acuerdos de niveles de servicios con áreas usuarias).
- Procedimientos definidos e implementados para el mantenimiento preventivo y correctivo.

- Disponibilidad de planes o procedimientos de contingencia.
- Inventario (*stock*) de componentes o partes críticas.
- Sitios alternos de procesamiento.
- Capacidad de enlaces de transmisión y redundancia.
- Pruebas de recuperación y retorno, restauración de cintas de respaldo.
- Respaldos de datos (tipo, frecuencia, software, políticas de respaldo de datos, rotulado y rotación de cintas, ubicación de almacenamiento).
- Centro de custodias (distancia, frecuencia de recolección, convenios).
- Requerimientos a proveedores (contingencias, sitios alternos).

Dimensión de infraestructura física

- Definición de planes de atención y evacuación ante conatos de incendio, amenazas de terrorismo, terremoto, o situaciones similares que ponen en riesgo las vidas humanas.
- Planes de emergencia, comunicación de crisis.
- Controles ambientales mínimos para prevenir acciones de riesgo que ponen en peligro activos y personas.
- Control de accesos en áreas críticas restringidas.
- Control de recursos dentro de las edificaciones.
- Construcción de edificaciones bajo normas de sismo resistencia y control de impactos de afectación física.
- Controles predictivos, preventivos o correctivos de fallas relacionadas con aire acondicionado, suministro de energía y potencia eléctrica requerida por equipos electrónicos o mecánicos.
- Control proactivo de suministro de elementos críticos como agua, indispensables para mantener condiciones higiénicas dentro de las edificaciones, además de equipos de control de temperatura y ambiente.

- Verificación de controles definidos para centros de documentación y almacenamiento de medios.
- Administración de controles ambientales y gestión de edificios.

Los tópicos enumerados anteriormente se evalúan basados en la presencia o carencia de características de excelencia y bajo el juicio y experiencia de los profesionales del proyecto. Esta evaluación comparada contra estándares y prácticas líderes permiten identificar las fortalezas, debilidades y oportunidades de mejoramiento.

1.2.2 Análisis de impactos. El Análisis de Impacto conocido por las siglas en ingles BIA (Business Impact Analysis), es una técnica de evaluación que se utiliza a nivel gerencial para determinar los impactos y exposiciones potenciales asociados con una interrupción significativa de las operaciones de la organización. Este análisis permite identificar funciones críticas, sus prioridades de recuperación e interdependencias, para posteriormente identificar y seleccionar estrategias de recuperación adecuadas.

Este tipo de análisis identifica los tiempos máximos de interrupción, impacto operativo y financiero y sirve como insumo para definir las estrategias y prioridades para mitigar el impacto, de forma que la Compañía continúe sus operaciones críticas en el evento de una interrupción. El Análisis de Impacto del Negocio se utiliza además, como base para la definición de acuerdos de niveles de servicio (ANS) que permitan administrar en forma eficiente y efectiva la continuidad del negocio. El resultado del Análisis de Impacto permite a la alta gerencia identificar lo siguiente:

Análisis de impactos tangibles

- Impactos financieros.

- Impactos legales.
- Impactos operacionales.

Análisis de impactos intangibles

- Impactos en la imagen de la Compañía.
- Impactos en la competitividad.
- Análisis de tiempos de interrupción
- Identificar el Tiempo Máximo de Interrupción (MTO)
- Identificar el Tiempo Objetivo de Recuperación (RTO)
- Identificar el Punto de Recuperación de Información (RPO)

Análisis de servicios de tecnología de información

- Identificar las aplicaciones de negocio soporte del proceso de negocio.
- Identificar otras aplicaciones o servicios de información soporte de los procesos de negocio.
- Hallar el grado de criticidad de las aplicaciones y/o servicios de TI.

Otros análisis generadores de impactos

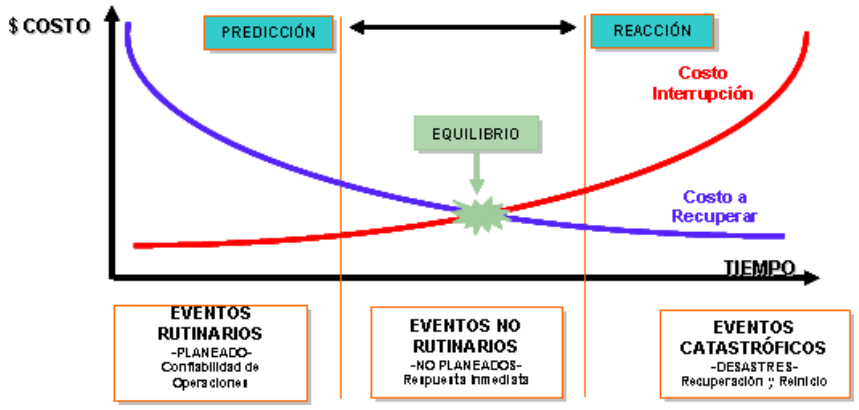
- Grado de vulnerabilidad de los procesos.
- Interrupciones presentadas en el proceso.
- Personas críticas para el proceso.

1.2.3 Definición de estrategias. La definición de estrategias resume las posibles alternativas y estrategias de continuidad que pueden ser aplicadas a la situación específica de la operación, de acuerdo con resultados del diagnóstico, y en aras

de fortalecer el estado de preparación del negocio ante situaciones de interrupciones o desastres no planeados.

Las estrategias consideradas de mayor acercamiento a las necesidades de continuidad de negocio son abordadas como las más recomendables para su implementación, sustentado en un análisis de costo/beneficio, acompañada del conocimiento, experiencia y las buenas prácticas del mercado.

Figura 1. Costo / Beneficio



La definición de estrategias de continuidad busca alcanzar el equilibrio entre el costo de las estrategias a considerar frente a la efectividad que se persigue al incorporar la estrategia como solución de continuidad de la operación en el tiempo establecido por cada una de las áreas del negocio.

1.3 DEFINICIONES Y ELEMENTOS BÁSICOS UTILIZADOS EN CONTINUIDAD DE NEGOCIO

Se manejan dos grandes enfoques en la continuidad de negocio:

- Proteger el valor económico de las empresas.
- Cuidar aspectos regulatorios que pueden poner en serios problemas a las organizaciones en caso de no cumplirlos.

1.3.1 Protección del valor económico de las empresas a través del programa BCM. Dentro de este enfoque hay varios aspectos que se deben tener en cuenta:

- El valor bursátil cae rápidamente inmediatamente después de un evento adverso.
- La recuperación del valor bursátil esta directamente relacionada con la percepción sobre la capacidad que la empresa tenga para manejar la crisis.
- Las empresas preparadas para gestionar una crisis manejaran mejor el evento.
- Las pólizas de seguros no protegerán el valor bursátil.
- Existe mucha diferencia entre el valor bursátil en empresas "recuperables" y las "no recuperables" aun cuando este se haya ajustado a las condiciones del mercado y rendimiento de su sector.
- Las empresas "recuperables" encuentran que su valor bursátil aumenta meses después de sufrir una crisis, mientras la "no recuperables" continúan con una declinación del valor y sufren un periodo de depresión sostenible.

1.3.2 Aspectos regulatorios fundamentales internacionales de BCM. A continuación se resaltan las normas más conocidas en el marco de BCM y cuales son sus propósitos.

Tabla 2. Normas más conocidas en el marco de BCM

ORIGEN DE LA NORMA	NOMBRE DE LA NORMA O ESTÁNDAR
Respuesta a la emergencia, protección de vidas e inmuebles, Administración de riesgos.	NFPA 1600, Protección Civil, HB 221, AS/NZ 4360
Sectores de negocio específicos (por ejemplo, financiero), gobierno corporativo, control interno	SOX, Basilea 1 y 2, Lavado de dinero, UK FSA, APS 232
Tecnologías de la Información	ITIL, CoBit, BS 17799, AS 4444, ISO 27000
Mejores Practicas internacionales en términos de BCM	DRII, BCI, BS 25999(BCM), BS25777(DRP)

El aporte de Basilea al BCM es a través de la emisión de “los principios de alto nivel para Continuidad de Negocios” en Junio de 2006. Estos principios fueron emitidos teniendo en cuenta que la Continuidad de Negocios es una actividad prioritaria para los participantes y autoridades de la industria financiera, los bancos son el pivote de la estabilidad económica de cualquier país: interdependencias en todos los sectores nacionales de producción o servicios y que el fallo en los procesos o sistemas bancarios esta relacionado con “consecuencias materiales adversas”

Los 7 Principios de Alto Nivel de Basilea

1. La Alta Dirección de una Organización es la responsable de la gestión de la BCM.

2. Los participantes y autoridades financieras deben incluir el riesgo de una interrupción operacional mayor en su alcance de BCM.
3. Desarrollar objetivos de recuperación en conjunto con las autoridades financieras.
4. y **5.** Incluir en el BCP procedimientos de comunicación con otras organizaciones relevantes locales e internacionales.

6. Los planes deben ser probados periódicamente.
7. Los planes deben ser revisados por las autoridades financieras de manera regular.

Ley Sarbanes-Oxley (SOX)

“The public Company Accounting Reform and Investor Protection Act of 2002” mejor conocida como Ley de Sarbanes-Oxley o SOX.

Se creo para dar respuesta a escándalos financieros. Su objetivo es devolver la confianza a los accionistas en el mercado de valores y reportes financieros (de empresas que cotizan en la Bolsa de EU) y definir responsabilidades en caso de fraude. Aplica para todas las empresas bajo políticas de la SEC (Securities and Exchange Commissions).

Algunas de ellas son:

- 3Com Corp.
- Colgate-Palmolive Co.
- Unisys Corporation.
- Citigroup, Inc.
- ING.

CoBit

Trabaja 4 dominios:

- Planear y organizar (planea la inversión).
- Adquirir y poner en práctica (Integra la Infraestructura).
- Libera y soporta (Continuidad del servicio).
- Monitorea y Evalúa (Audita y Controla).

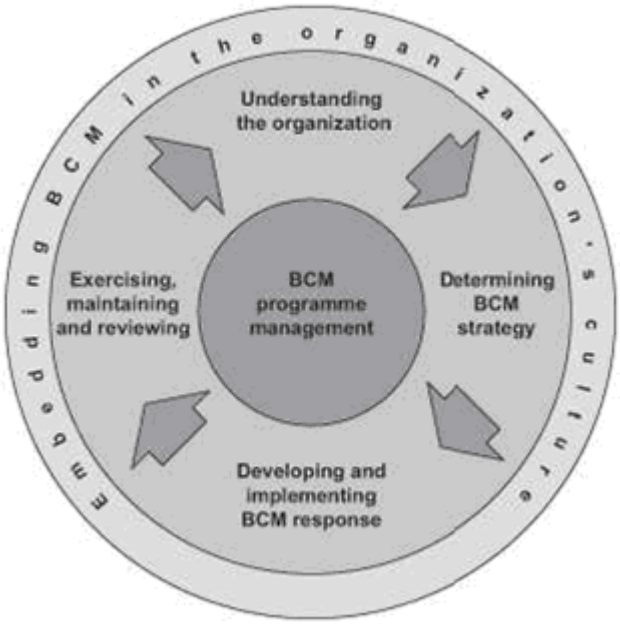
Enfatiza el cumplimiento normativo, ayuda a las organizaciones a incrementar el valor de TI, apoya el alineamiento con el negocio. Tiene 34 Objetivos de nivel Alto y 215 de control

DRII (Mejores Prácticas)

- Paso 1: Iniciación y Gestión del Proyecto.

- Paso 2: Evaluación y Control de Riesgos.
- Paso 3: Análisis del impacto en el Negocio.
- Paso 4: Desarrollar Estrategias de Gestión de Continuidad del Negocio.
- Paso 5: Respuesta y Operaciones de Emergencia.
- Paso 6: Desarrollar e Implementar planes de Continuidad del Negocio.
- Paso 7: Creación de conciencia y entrenamiento.
- Paso 8: Ejercitar y mantener los planes de Continuidad del Negocio.
- Paso 9: Comunicación de crisis.
- Paso 10: Coordinación de agencias externas.

Figura 2. BS 25999



Otros estándares que contienen elementos de BCM son:

- PAS 77 sobre Continuidad de Servicio de TI
- ISO 27002 (Antes ISO 17799) – Aunque primordialmente se trate de un estándar relativo a la seguridad de la información, contiene aspectos de Continuidad de Negocio que deben ser atendidos para implantar correctamente ISO 27001.

- ITIL este estándar se ocupa de disciplinas de Gestión de Servicio, como Riesgos y Seguridad, Cambios, Problemas, Configuración, Capacidad y Disponibilidad. No obstante existe un vínculo entre la Continuidad de Servicio de TI de ITIL (Recuperación de Desastres) y la Continuidad de Negocio.
- Legislación de Protección de Datos
- Legislación garante de la libertad de información
- Normas sanitarias
- Reglas y directrices como las previstas en la ley Sarbanes-Oxley de Estados Unidos y el acuerdo internacional bancario Basilea II, influyen sobre BCM al ser obligatorias e imponer parámetros para la continuidad de servicios.

2. METODOLOGÍA UTILIZADA PARA EL DIAGNÓSTICO Y RESULTADOS ENCONTRADOS

2.1 ENFOQUE DE LA CONTINUIDAD DE NEGOCIO

El diagnóstico de Continuidad se fundamenta en la experiencia y conocimiento de los miembros del equipo de trabajo, apoyados en la aplicabilidad de la metodología *Business Continuity Management® (BCM*) y de igual forma en modelos de referencia y estándares reconocidos como prácticas líderes (*BCI, BS25999, DRI, ITIL, COBIT, NFPA, NIST, ISO 20000*).

El diagnóstico realizado se establece con base a la información proporcionada, las evaluaciones y entrevistas realizadas, la evaluación de riesgos, el análisis de impacto, la planeación estratégica actual. El análisis de las dimensiones trabajadas está enmarcado a la luz de las prácticas líderes en planeación de continuidad, de aquí se desprenden actividades básicas para el diagnóstico como son la evaluación de riesgos, el análisis de impactos y la definición de estrategias.

2.1.1 Evaluación de riesgos. La actividad de evaluación de riesgos busca determinar la probabilidad de que se presenten amenazas y/o vulnerabilidades que puedan impactar la operación normal de los procesos, las personas, la infraestructura tecnológica que soporta los procesos, y la infraestructura física donde se opera y que pueden llegar a afectar la continuidad del negocio.

Al realizar la evaluación de riesgos, el equipo profesional de continuidad tiene en cuenta la información recopilada mediante entrevistas, solicitud de información, análisis internos y externos, visitas guiadas a edificaciones, o cualquier aspecto que pueda generar interrupciones o afectar la operación normal. La evaluación de riesgos se ha dividido en las cuatro dimensiones consideradas para mantener la continuidad, así:

- Procesos.
- Personas.
- Tecnología.
- Infraestructura física.

Los aspectos relevantes que se evalúan como posibles desestabilizadores de la continuidad en estas cuatro dimensiones, se presentan en forma general a continuación:

DIMENSIÓN DE PERSONAS (ORGANIZACIÓN - RECURSO HUMANO)

- Administración del conocimiento (documentación de soluciones, manuales, artículos, lecciones aprendidas).
- Entrenamiento y capacitación del personal.
- Entrenamiento cruzado.
- Segregación de funciones.
- Salud ocupacional (manejo de epidemias, virus).
- Índices de rotación de personal.
- Políticas de retención de personal.
- Política de comunicación formal.
- Trabajo en equipo, personal motivado, capacitado y comprometido.

DIMENSIÓN DE PROCESOS NEGOCIO (OPERACIÓN)

- Definición de actividades y procesos interrelacionados.
- Definición de entradas y salidas de cada proceso.
- Definición, medición y gestión de indicadores de comportamiento del proceso.
- Definición de procedimientos alternos de trabajo.
- Actualización de los procedimientos y procesos base de operación.

- Claridad en roles y responsabilidades relacionadas con las operaciones críticas.
- Consideración de recursos de respaldo suficientes y necesarios para cada actividad del proceso.
- Administración de proveedores de servicios profesionales y socios de negocio.
- Control y gestión de proveedores de servicio.
- ANS medibles y confiables con proveedores, clientes internos y externos.
- Medición de tiempos y cantidad de recursos críticos.
- Gestión de calidad (disciplina de registro, documentación, comunicación, integración, evaluación).

DIMENSIÓN DE TECNOLOGÍA

- Control, gestión y mantenimiento de servidores, bases de datos, redes, almacenamiento, aplicaciones y sistemas de información, información, archivos y operación de usuarios.
- Procesos definidos e implementados para el soporte del servicio.
- Procesos definidos e implementados para la entrega del servicio.
- Procedimientos definidos e implementados para el mantenimiento preventivo y correctivo.
- Disponibilidad de planes o procedimientos de contingencia.
- Inventario (*stock*) de componentes o partes críticas.
- Sitios alternos de procesamiento.
- Capacidad de enlaces de transmisión y redundancia.
- Pruebas de recuperación y retorno.
- Respaldos de datos (tipo, frecuencia, software, políticas de respaldo de datos, rotulado y rotación de cintas, ubicación).
- Centro de custodias (distancia, frecuencia de recolección, convenios).
- Requerimientos a proveedores (contingencias, sitios alternos).

DIMENSIÓN DE INFRAESTRUCTURA FÍSICA

- Definición de planes de atención y evacuación ante conatos de incendio, amenazas de terrorismo, terremoto, o situaciones similares que ponen en riesgo las vidas humanas.
- Planes de emergencia, comunicación de crisis.
- Controles ambientales mínimos para prevenir acciones de riesgo que ponen en peligro activos y personas.
- Control de accesos en áreas críticas restringidas.
- Control de recursos dentro de las edificaciones.
- Construcción de edificaciones bajo normas de sismo resistencia y control de impactos de afectación física.
- Controles predictivos, preventivos o correctivos de fallas relacionadas con aire acondicionado, suministro de energía y potencia eléctrica requerida por equipos electrónicos o mecánicos.
- Control proactivo de suministro de elementos críticos como agua, indispensables para mantener condiciones higiénicas dentro de las edificaciones, además de equipos de control de temperatura y ambiente.
- Verificación de controles definidos para centros de documentación y almacenamiento de medios.
- Administración de controles ambientales y gestión de edificios.

Los tópicos enumerados anteriormente se evalúan basados en la presencia o carencia de características de excelencia, y bajo el juicio y experiencia de los profesionales del proyecto. Esta evaluación comparada contra estándares y prácticas líderes nos permite identificar las fortalezas, debilidades y oportunidades de mejoramiento.

2.1.2 análisis de impactos. El Análisis de Impacto es una técnica de evaluación que se utiliza a nivel gerencial para determinar los impactos y exposiciones

potenciales asociados con una interrupción significativa de las operaciones de la organización. Este análisis permite identificar funciones críticas, sus prioridades de recuperación e interdependencias, para posteriormente identificar y seleccionar estrategias de recuperación adecuadas.

Este tipo de análisis identifica los tiempos máximos de interrupción, impacto operativo y financiero y sirve como insumo para definir las estrategias y prioridades para mitigar el impacto, de forma que la Compañía continúe sus operaciones críticas en el evento de una interrupción. El Análisis de Impacto del Negocio se utiliza además, como base para la definición de acuerdos de niveles de servicio (ANS) que permitan administrar en forma eficiente y efectiva la continuidad del negocio. El resultado del Análisis de Impacto permite a la alta gerencia identificar lo siguiente:

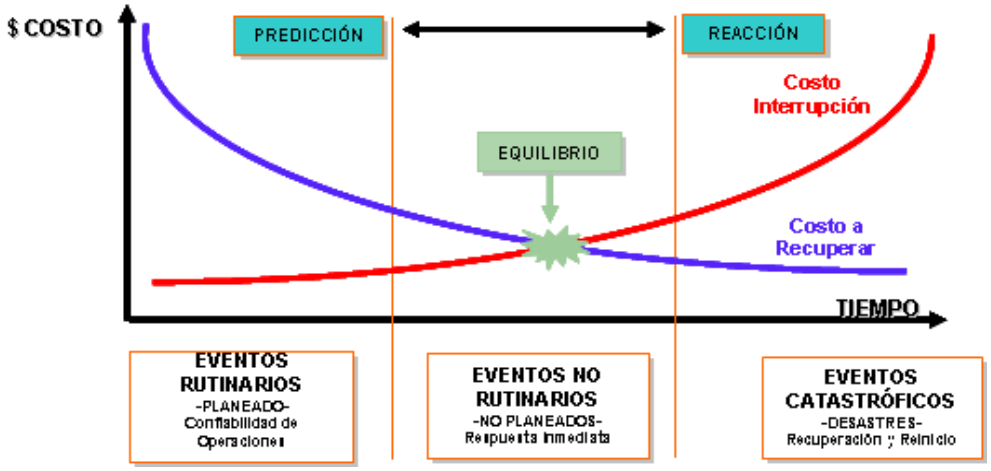
- Análisis de impactos tangibles: impactos financieros, legales y operacionales.
- Análisis de impactos intangibles: impactos en la imagen de la Compañía y en la competitividad.
- Análisis de tiempos de interrupción: identificar el Tiempo Máximo de Interrupción (MTO), el Tiempo Objetivo de Recuperación (RTO) y el Punto de Recuperación de Información (RPO).
- Análisis de servicios de tecnología de información: identificar las aplicaciones de negocio soporte del proceso de negocio, identificar otras aplicaciones o servicios de información soporte de los procesos de negocio y hallar el grado de criticidad de las aplicaciones y/o servicios de TI.
- Otros análisis generadores de impactos: grado de vulnerabilidad de los procesos, interrupciones presentadas en el proceso, personas críticas para el proceso.

2.1.3 Definición de estrategias. La definición de estrategias resume las posibles alternativas y estrategias de continuidad que pueden ser aplicadas a la situación

específica de la operación, de acuerdo con resultados del diagnóstico y en aras de fortalecer el estado de preparación del negocio ante situaciones de interrupciones o desastres no planeados.

Las estrategias consideradas de mayor acercamiento a las necesidades de continuidad de negocio son abordadas como las más recomendables para su implementación, sustentado en un análisis de costo/beneficio, acompañada del conocimiento, experiencia y las buenas prácticas del mercado.

Figura 3. Costo / Beneficio



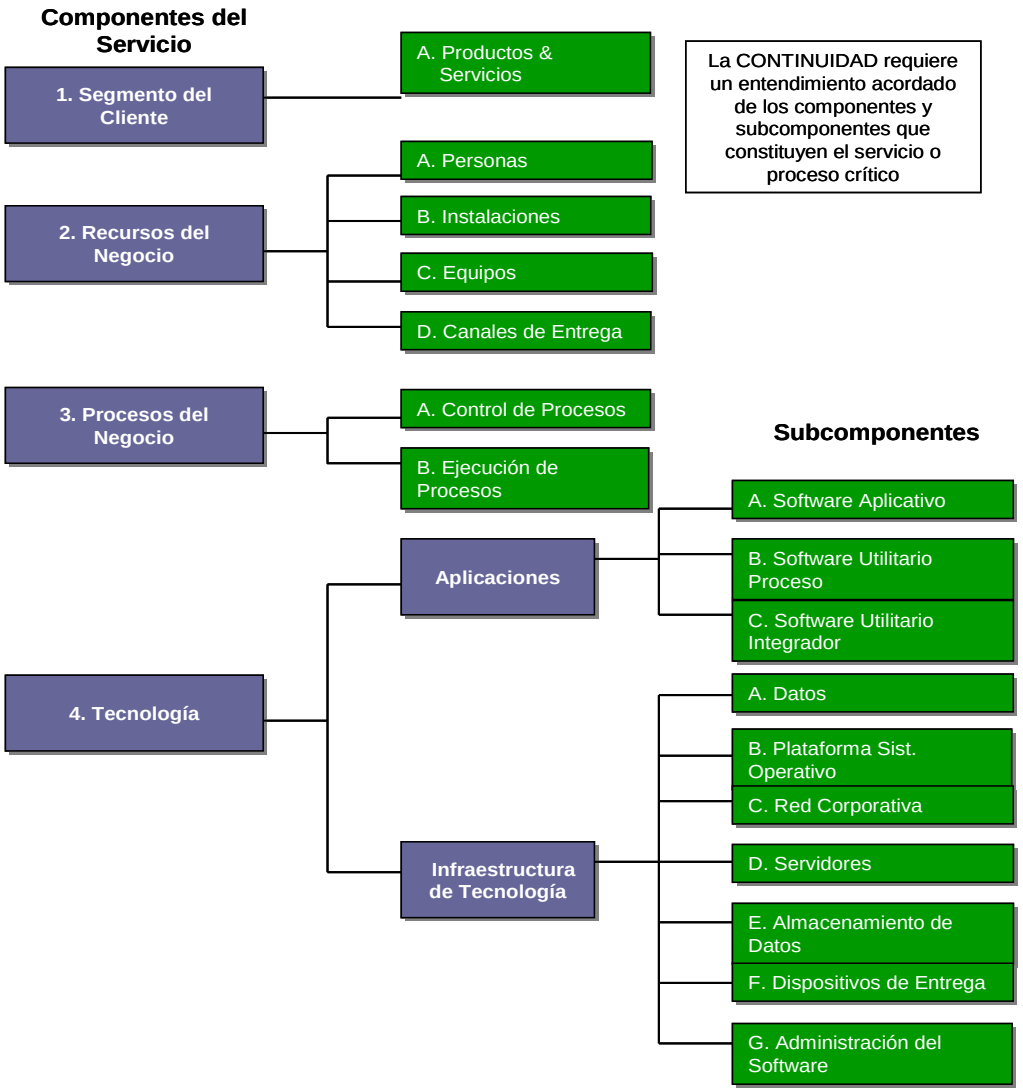
La definición de estrategias de continuidad busca alcanzar el equilibrio entre el costo de las estrategias a considerar, frente a la efectividad que se persigue al incorporar la estrategia como solución de continuidad de la operación en el tiempo establecido por cada una de las áreas del negocio.

2.2 METODOLOGÍA

Para la elaboración del diagnóstico del estado actual frente a la continuidad de negocio, se realizan diferentes fases y actividades dispuestas metodológicamente para lograr el objetivo requerido por el proyecto. El siguiente es un recuento metodológico de como se elabora y presenta el diagnóstico.

2.2.1 mapeo de interdependencias. El objetivo es entender como las personas, procesos y tecnología están distribuidos a través de la línea de continuidad, y trazar la misma. En esta actividad se busca identificar los enlaces entre la arquitectura de los servicios de negocio, los servicios informáticos y la arquitectura tecnológica que los soporta. En la evaluación de interdependencias es necesario que los encargados de la actividad evalúen riesgos de continuidad de negocio, analizando el impacto de la no-disponibilidad o no-confiabilidad de alguno de los componentes de la cadena.

Figura 4. Componentes del servicio



BASES CONCEPTUALES

Alineación estratégica y diseño organizacional: entendimiento claro y preciso del negocio y su entorno, se requiere comprender la estructura organizacional y entender como es su ambiente de competencia, estrategias internas, esfuerzos de mejoramiento continuo, proveedores, servicios, crecimiento e iniciativas de cambio, políticas y estrategias de continuidad de negocio establecidas, entre otros aspectos.

Perfil de servicios del negocio: entender como están diseñados los procesos del negocio y los servicios que presta a sus clientes, es fundamental el entendimiento de la cadena de continuidad que debe tejerse para la prestación del servicio ofrecido a los clientes.

Perfil de la infraestructura tecnológica: obtener un conocimiento formal de la infraestructura tecnológica (aplicativos, servidores, bases de datos, redes, PCs, entre otros) que soportan los servicios de negocio y los servicios informáticos soporte de los procesos.

ACTIVIDADES DEL MAPEO DE INTERDEPENDENCIAS

Realizar mapa de interdependencias de procesos: construir un mapa que describa el flujo de información entre las diferentes etapas o actividades de un proceso e identificando los aplicativos que la soportan. Se debe tener en cuenta el inventario de aplicaciones, la información existente entregada, entrevistas con líderes de procesos.

Realizar mapa lógico de tecnología: realizar un flujo de interfaces entre los diferentes sistemas informáticos, y la tecnología que soporta los servicios de negocio, haciendo énfasis en aquellos que se encuentran dentro del alcance del proyecto. Se debe tener en cuenta el inventario de hardware y software, la

información de arquitectura actual y entrevistas con personal clave del área tecnológica.

2.2.2 Evaluación de riesgos. La elaboración de la evaluación de riesgos requiere de una comprensión de la terminología de riesgos y los procedimientos para evaluar el riesgo. Para esto, metodológicamente se debe tener en cuenta los siguientes aspectos:

BASES CONCEPTUALES

Amenaza: persona, situación o evento natural del entorno (externo o interno) que es visto como fuente de peligro, catástrofe o interrupción. Ejemplos: inundación, incendio, robo de datos, sabotaje, ausencia del plan de contingencias, insuficiente gestión de monitoreo, aplicativos mal diseñados, entre otros.

Vulnerabilidad: es una debilidad que puede ser ejecutada accidentalmente o explotada intencionalmente, esta debilidad puede ser causada por la falta de uno o varios controles, que puede permitir que la amenaza ocurra y afectar el objeto de evaluación. Ejemplo: deficiente control de accesos, administración deficiente de la continuidad, poco control de versiones de software, ausencia de entrenamiento cruzado (respaldo de personas), políticas inexactas e insuficientes, entre otros.

Riesgo: definimos el riesgo como la probabilidad de la materialización de una amenaza por la existencia de una o varias vulnerabilidades y las impactos adversos resultantes. Para determinar la probabilidad de ocurrencia de posibles eventos adversos, las amenazas deben ser analizadas en conjunto con las vulnerabilidades potenciales y los controles implementados.

Impacto: es la evaluación del efecto o consecuencia del riesgo. Generalmente, la implicación del riesgo se mide en aspectos económicos, imagen de las personas o

empresas, disminución de capacidad de respuesta y competitividad, interrupción de operaciones, entre otros.

Control: cualquier acción que ayude a reducir la probabilidad de ocurrencia de un riesgo o permita reducir el impacto en caso de que este ocurra.

Riesgo puro: es la evaluación de la probabilidad e impacto de un riesgo sin considerar los controles implementados para gestionarlo.

Riesgo residual: el riesgo residual es el resultante tras la evaluación de los controles implementados para su gestión y que es considerado el riesgo asumido por la organización.

CLASIFICACIÓN DEL RIESGOS

Para la clasificación de riesgos se utilizan tres tablas que califican la probabilidad de ocurrencia, el impacto y los controles.

Tabla 3. Clasificación de probabilidad

CALIFICACIÓN	DESCRIPTOR	PROBABILIDAD DE OCURRENCIA
5	**Casi Seguro**	• Es casi seguro que ocurrirá en la mayoría de las circunstancias. El evento es rutinario y puede presentarse frecuentemente en la operación del día a día (más de una vez en un año). • Se presenta en el día a día, su origen es atribuible a situaciones normales del proceso como interrupciones menores de los servicios de la tecnología, los recursos de papelería, y otros similares.
4	**Frecuente**	• Se presenta con cierta regularidad y su causa es atribuible a los recursos mínimos del proceso los cuales son necesarios para su operación (una vez cada dos años). • El evento es rutinario e inherente a causas específicas, puede presentarse en cualquier momento. Este evento podría suceder en períodos cortos de tiempo (minutos, horas, días)
3	**Ocasional**	• Suceso que se presenta de forma esporádica (una vez

CALIFICACIÓN	DESCRIPTOR	PROBABILIDAD DE OCURRENCIA
		cada cinco años). • El evento no se clasifica como rutinario, y su ocurrencia es condicionada bajo circunstancias que requieren supervisión controlada.
2	**Improbable**	• Suceso inhabitual (al menos una vez cada 10 años) • El evento se clasifica como no-rutinario y no es inherente a la tecnología, su frecuencia se asocia con variables externas a la tecnología, los procesos o componentes.
1	**Raro**	• Suceso que ocurre de forma excepcional (al menos una vez cada 15 años o más) • El evento es no-rutinario. Se presenta sólo bajo situaciones excepcionales o fuera de la operación normal.

Tabla 4. Clasificación de impactos

CALIFICACIÓN	DESCRIPTOR	IMPACTO
20	**Catastrófico**	• Indisponibilidad del 50% de funcionarios de una misma área clave, por un mismo evento. • Pérdida de activos o ingresos superior a USD 85 millones. • Difusión externa a nivel internacional. • Daño ambiental grave no recuperable. • Pérdida de participación de mercado mayor al 20%.
10	**Mayor**	• Indisponibilidad del 25% al 50% de funcionarios de una misma área clave, por un mismo evento. • Pérdida de activos o ingresos entre USD 25 y 85 millones. • Difusión externa a nivel nacional (país). • Daño ambiental grave recuperable a largo plazo (más de 100 años) • Pérdida de participación de mercado entre el 15 y el 20%.
5	**Moderado**	• Indisponibilidad del 10% al 25% de funcionarios de una misma área clave, por un mismo evento. • Pérdida de activos o ingresos entre USD 5 y 25 millones • Difusión externa a nivel departamental. • Daño ambiental grave recuperable a mediano plazo (entre 20 y 100 años). • Pérdida de participación de mercado entre el 7 y el 15%.
2	**Menor**	• Indisponibilidad superior a 6 meses de menos del 5% de funcionarios de una misma área clave, por un mismo evento. • Pérdida de activos o ingresos entre USD 1 y 5 millones • Difusión externa a nivel local y/o de organización a nivel nacional.

CALIFICACIÓN	DESCRIPTOR	IMPACTO
		• Daño ambiental leve no recuperable. • Pérdida de participación de mercado entre el 2 y el 7%.
1	**Insignificante**	• Indisponibilidad temporal de algunos funcionarios no claves de una misma área clave por un mismo evento. • Pérdida de activos o ingresos menores a USD 1 millón. • Difusión a nivel interno (proceso, equipo de trabajo) • Daño ambiental leve recuperable. • Pérdida de participación de mercado menor al 2%.

Tabla 5. Clasificación del control actual

CALIFICACIÓN	DESCRIPTOR	DEFINICIÓN
1	Fuerte	El control y/o procedimiento de control observado es preventivo, está documentado e implementado, es efectivo para mitigar los riesgos y siempre es aplicado con la intensidad y rigurosidad esperada.
2	Normal	El control y/o procedimiento de control observado es preventivo está documentado e implementado, es apropiado para mitigar los riesgos, pero el personal no siempre lo cumple o aplica.
3	Moderado	El control y/o procedimiento de control observado es correctivo, está documentado pero sólo algunas veces es aplicado por múltiples motivos, cuando es implementado ayuda a reducir la exposición al riesgo, puede requerir rediseño.
4	Débil	El control existente es informal, casi siempre es correctivo, ayuda a mitigar los riesgos, pero no siempre es aplicado. Se debe realizar una documentación e implementación.
5	Inexistente	No se observó o evidenció procedimientos de control o controles que ayuden a reducir o mitigar el riesgo. Se debe definir, documentar, e implementar controles.

CATEGORIZACIÓN DEL RIESGO

Los riesgos de continuidad encontrados en la fase de evaluación de riesgos serán agrupados según la siguiente categorización:

Riesgos en Personas

- Falta de administración del conocimiento.

- Carencia de capacitación y entrenamiento.
- Insuficiente número de personas
- Inadecuada preparación ante desastres.
- Falta de seguridad laboral y salud ocupacional.
- Falta de pertenencia y cultura en continuidad.

Riesgos en Procesos

- Falta de administración
- Carencia de dueños de procesos.
- Falta de controles
- Falta de procedimientos alternos
- Dependencias entre procesos
- Limitaciones de capacidad
- Falta de definición de acuerdos de nivel de servicio.
- Falta de documentación
- Dependencia y falta de control de proveedores.

Riesgos en Infraestructura Tecnológica

- Carencia de procesos de administración de servicios de tecnología de información.
- Falta de estrategias de disponibilidad.
- Inadecuadas estrategias de recuperación.
- Falta de acuerdos de servicio con proveedores.
- Puntos únicos de falla en la infraestructura de TI.
- Alta dependencia de proveedores.

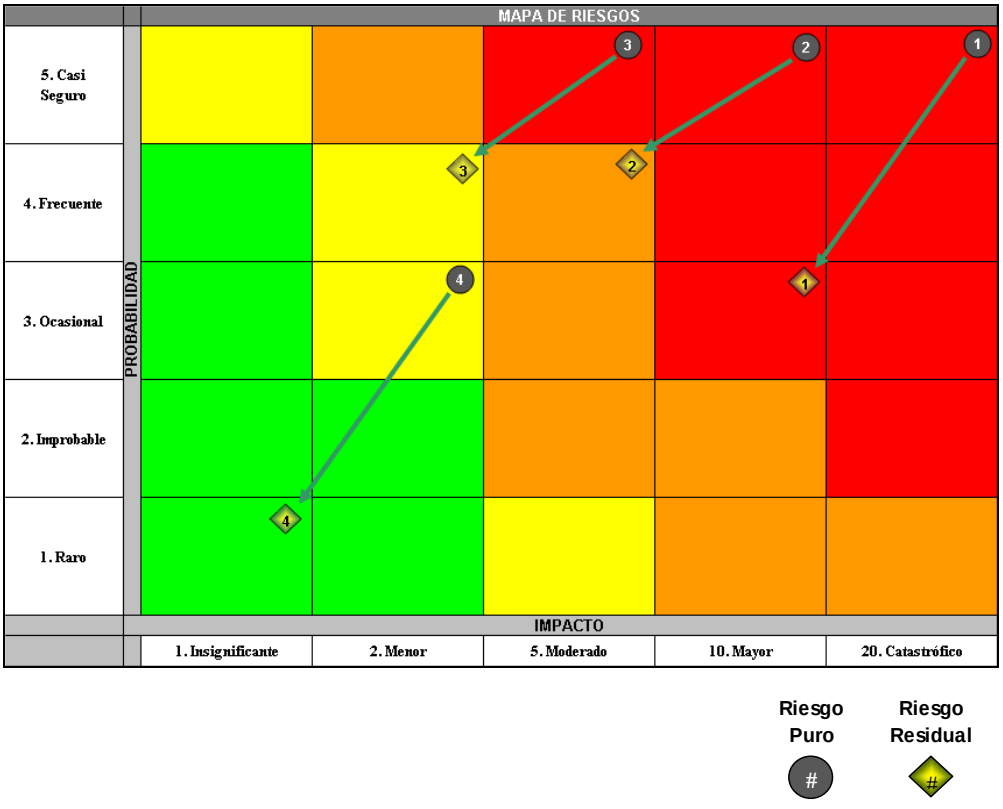
Riesgos en Infraestructura Física

- Carencia de planes de emergencia y administración de crisis.
- Exposición a incendios e inundaciones.
- Fallas de potencia eléctrica.
- Fallas del aire acondicionado.
- Construcción inadecuada de edificios y centros de cómputo.
- Falta de controles ambientales.

VALORACIÓN DEL RIESGO

Los riesgos encontrados son ordenados en una matriz de colores que representa el apetito de riesgo conocida como Mapa de Riesgos. Esta contiene escalas de probabilidad e impactos para el cálculo del riesgo puro y residual.

Figura 5. Mapa de riesgos



Los círculos grises con letra blanca representan el riesgo puro y los rombos amarillos con letra negra representan el riesgo residual.

Cuando se califica la probabilidad y el impacto inicial del riesgo se valora y clasifica la criticidad del riesgo en uno de los cuatro cuadrantes, como se describe a continuación:

Tabla 6. Riesgo en uno de los cuatro cuadrantes

EXTREMO	• Riesgo Extremo - Debe ser puesto en conocimiento de la alta dirección y ser objeto de seguimiento continuo. • Se debe aplicar inmediatamente medidas de control físico/lógico y financiero.
ALTO	• Riesgo Alto - Exige atención de directores y subdirectores. Se deben desarrollar actividades Inmediatas y prioritarias para la gestión de riesgos Control físico /lógico y financiero.
MODERADO	• Riesgo Moderado - Debe ser gestionado adecuadamente por jefes de nivel medio (coordinadores). Se deben desarrollar actividades para la gestión del riesgo.
BAJO	• Riesgo Bajo - Debe ser gestionado a nivel supervisor. El riesgo no representa una amenaza significativa.

Posteriormente se califica el control y dependiendo de la efectividad del mismo se puede dar el caso que disminuya la probabilidad y / o el impacto, esto conlleva a que el riesgo se reduzca, traslade o mitigue.

2.2.3 Análisis de impactos. El Análisis de Impacto del Negocio es una técnica de evaluación que se utiliza a nivel gerencial para determinar los impactos potenciales asociados con una interrupción significativa de las operaciones de la organización.

La realización de un análisis de impactos implica un entendimiento metodológico previo de la Compañía, con sus procesos, personas, tecnología soporte e instalaciones de operación. Este entendimiento busca respuesta a: ¿Qué es crítico para la Compañía?, ¿Qué pasa si?, ¿Cuáles son los recursos requeridos?, para lo

cual, se utiliza el “escenario del peor caso”, y así obtener del público objetivo su mejor estimativo.

El entendimiento de la Compañía es realizado mediante entrevistas, análisis de información, evaluación de riesgos, entre otras actividades. Además, para realizar el análisis de impactos se debe conocer la terminología y las actividades explicadas a continuación.

BASES CONCEPTUALES

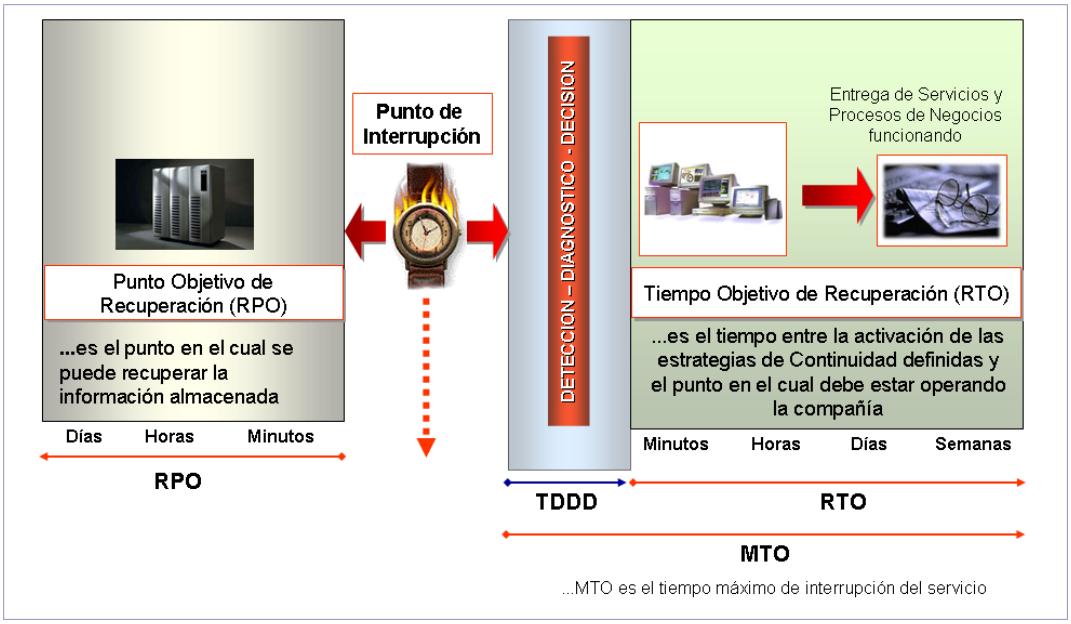
Impacto: es el efecto o consecuencia por una interrupción de las operaciones de la Compañía. El impacto se puede observar o medir mediante aspectos económicos, imagen de las personas o empresas, sanciones legales, disminución de capacidad de respuesta y competitividad, entre otros.

Tiempo máximo de interrupción (MTO): es el periodo máximo de tiempo que puede soportar un proceso o la Compañía sin el soporte de actividades, antes de ocasionar grandes impactos. Este tiempo es quien ayuda a delimitar y definir las estrategias de recuperación.

Tiempo objetivo de recuperación (RTO): es el periodo de tiempo dentro del cual un proceso, sistema o aplicación debe ser recuperado después de una interrupción. El RTO se utiliza principalmente para ayudar a definir las estrategias de recuperación.

Punto de recuperación de información (RPO): este es el punto en el cual la información o los datos de un proceso o aplicación deben ser recobrados tras una interrupción. El RPO se utiliza frecuentemente para ayudar a definir estrategias de respaldo de información.

Figura 6. Tiempos de recuperación



ACTIVIDADES DEL ANÁLISIS DE IMPACTOS

Identificar procesos y público objetivo: después de un entendimiento de la Compañía, sus procesos, actividades, servicios y productos, se debe definir las áreas que participarán de la encuesta de análisis de impacto. Por lo general, este público objetivo se encuentra en los niveles gerenciales de la Compañía, con un amplío conocimiento de los procesos, productos y servicios. Además, de este personal, se recomienda tener el acompañamiento de sus equipo de trabajo o colaboradores del área.

Identificar los requerimientos soporte del negocio: es muy importante en etapas previas a la realización del análisis de impactos, identificar aquellos recursos que hacen parte del soporte requerido por los procesos para ejecutar sus actividades. Dentro de los principales recursos se encuentran las aplicaciones y/o

servicios de TI, las personas, las instalaciones y todos aquellos suministros que son parte esencial en el funcionamiento de la Compañía.

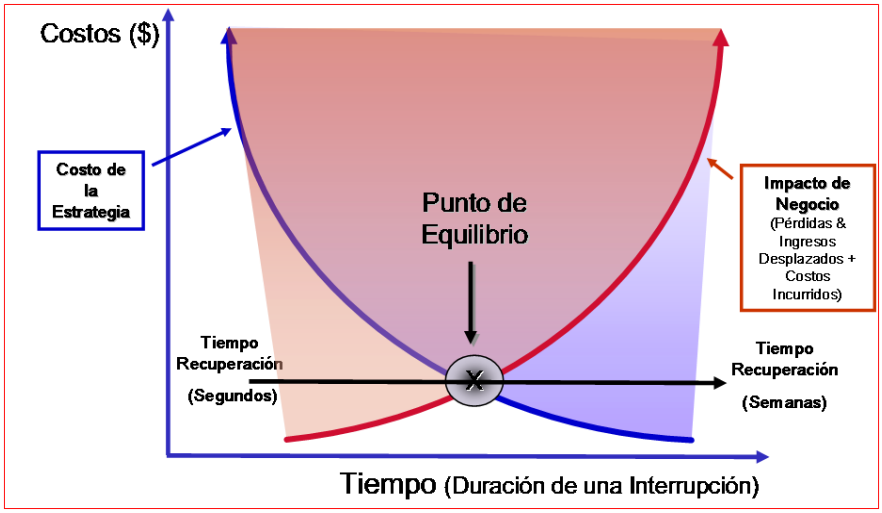
Elaborar la encuesta de análisis de impacto: teniendo en cuenta la información recolectada previamente, se procede a elaborar un cuestionario, donde cada una de las preguntas es ajustada a la situación actual de la Compañía y enfocadas a recoger la información más confiable posible de los potenciales impactos.

Validar información y elaborar el reporte de resultado: después de obtener las encuestas, la información es validada para obtener información veraz de los posibles impactos que se puedan presentar en la Compañía, y por último presentar el informe a la gerencia.

2.2.4 Definición de estrategias. La fase de definición y diseño de estrategias trata de establecer los controles necesarios para mantener la continuidad. En esta fase se establecen los recursos mínimos de operación, el gobierno para administrar la continuidad, los controles para mitigar los riesgos y todas aquellas estrategias requeridas que permitan mantener la continuidad del negocio. Las estrategias se establecen de acuerdo a las soluciones y las buenas prácticas del mercado que establecen los costos y el tiempo que se tardan en recuperar los servicios prestados.

En la siguiente gráfica se ilustra el punto de equilibrio entre impactos generados en el tiempo, y el costo de las estrategias requeridas para mantener o recuperar la operación:

Figura 7. Punto de equilibrio



Como se ve en la gráfica, a mayor tiempo de interrupción los impactos crecen exponencialmente (línea roja), mientras que a menor tiempo de recuperación (segundos) mayor el costo de la estrategia (línea azul).

Es importante en esta fase hacer una desagregación de componentes de servicio crítico que permita definir estrategias de continuidad, de acuerdo a los resultados de la evaluación de riesgos (RA) y el análisis de impactos (BIA):

- Recurso humano (personas, cultura).
- Recursos operativos (suministros, materia prima, proveedores).
- Procesos y procedimientos.
- Tecnología, Infraestructura, Aplicaciones.
- Instalaciones físicas, Centros de Cómputo, Oficinas.

ACTIVIDADES DE LA DEFINICIÓN DE ESTRATEGIAS

Identificación de estrategias de continuidad: está orientada a presentar los diferentes escenarios estratégicos que ayuden a mantener la continuidad requerida. Este diseño se basa en los resultados del diagnóstico de la situación

actual de continuidad, en la definición de recursos mínimos de recuperación, en las evaluaciones de riesgo (RA), en el análisis de impacto (BIA), y en los acuerdos de niveles de servicio (ANS) para los servicios ofrecidos.

Desarrollo de la arquitectura estratégica: esta actividad resume las estrategias de continuidad seleccionadas por la alta gerencia, y que permite definir una arquitectura de solución confiable que ayude a mantener los niveles de continuidad esperados por los clientes.

Determinar requerimientos de recursos mínimos: permite identificar los requerimientos de recursos mínimos necesarios para que los procesos críticos del negocio puedan seguir operando, bajo condiciones aceptables para el proceso o el cliente. En esta actividad se busca identificar recursos como: terceros, proveedores, aplicativos, infraestructura de TI, personal interno o externo, equipos de oficinas, instalaciones físicas, telecomunicaciones, programas especializados, datos, material impreso, y tecnología especializada (core) necesaria para cada área de negocio.

Diseño del programa de administración de continuidad: esta es sin duda una de las actividades marco que se deben adelantar para definir claramente las políticas de continuidad de la Compañía de acuerdo con los estándares actuales de continuidad, el programa mismo de gestión de la continuidad, y los elementos mínimos de estructuración de recursos orientados a un sistema continuo de continuidad de negocio (gobierno).

Diseño del plan de sensibilización y cultura: uno de los factores críticos de éxito en la implementación de un programa de continuidad de negocio es la gente. El recurso humano debe ser entendido como el eslabón más débil en la cadena de disponibilidad de un servicio, y es quien usualmente afecta los niveles de confiabilidad que se requieren mantener. El plan de sensibilización busca

incorporar al factor humano dentro del programa de continuidad, y busca crear cultura de riesgo que permita minimizar las situaciones incontrolables generadas por la gente.

2.3 RESULTADOS DEL MAPEO DE INTERDEPENDENCIAS

El mapeo de interdependencias es la primera actividad que se ejecuta para realizar el diagnóstico de continuidad de negocio, en esta se busca identificar la interrelación existente entre los procesos y la infraestructura tecnológica que permite entregar productos y/o servicios a los diferentes clientes/usuarios de UNE. Esta actividad se cataloga principalmente de entendimiento y análisis del modelo de prestación de servicios existente de UNE, y no se considera una actividad que generé un resultado visible del proyecto.

Los resultados de esta actividad están distribuidos a través de todo el diagnóstico, principalmente en las actividades de evaluación de riesgos y análisis de impactos. Las interrelaciones identificadas están constituidas principalmente por tablas de relaciones y gráficos, los cuales permitieron filtrar la información de los diferentes servicios de negocio, procesos y servicios informáticos para la identificación de la línea de continuidad.

2.4 RESULTADOS DE LA EVALUACIÓN DE RIESGOS

La evaluación de riesgos de continuidad se realiza mediante entrevistas a personas de los procesos de negocio, la cual incluye dueños de procesos y especialistas de los mismos; estudio de documentación de los procesos, visitas a instalaciones y toda aquella información suministrada donde se evidencien los compromisos de entrega de productos y servicios a los clientes de UNE.

La evaluación busca encontrar posibles riesgos que afecten la continuidad del servicio en las diferentes dimensiones de continuidad agrupadas en diferentes factores, así:

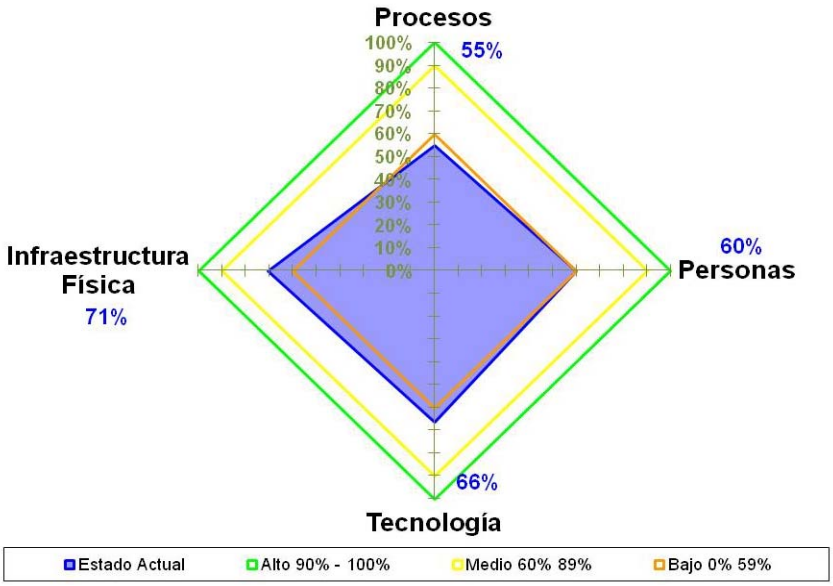
- Personas: Gestión del Conocimiento y Seguridad Física y Laboral.
- Procesos: Gestión del Proceso, Proveedores y Soporte de Tecnología.
- Tecnología: Confiabilidad, Disponibilidad y Recuperabilidad.
- Infraestructura Física: Preparación para Atender Emergencias, Preparación ante Incendio, Potencia Eléctrica, Seguridad y Accesos, Aire Acondicionado en los nodos y Estado General.

En cada uno de estos factores se realiza una evaluación mediante preguntas a líderes de procesos, especialistas de la infraestructura tecnológica y física, evaluación de la documentación existente. Con el cuestionario se valora el nivel de preparación de cada dimensión de continuidad.

Al final, la evaluación se realiza teniendo en cuenta todos los factores: respuestas de los entrevistados, las buenas prácticas en continuidad, los estándares definidos por el mercado y la asesoría de asesores externos experimentados. Esto permite hallar amenazas o falta de control sobre los factores que podrían ocasionar una interrupción de los servicios entregados a los clientes UNE.

También es importante anotar que el estado de madurez de continuidad al cual se quiere llegar es definido por la misma Compañía, de acuerdo a su planeación estratégica de negocio y su apetito de riesgo. Si UNE quisiera en su estrategia de negocio ser reconocido por tener un sistema que administra la continuidad, la recomendación es buscar un nivel de preparación del 100%; que implica un proceso de madurez a largo plazo (3 a 5 años) tal cual lo han hecho empresas como Vodafone.

Figura 8. Estado general de riesgos de continuidad



En la gráfica podemos observar que los valores generales hallados para mantener la continuidad se encuentran en niveles aceptables, debido a que se han implementado controles aislados para cada una de las dimensiones, como por ejemplo en las instalaciones físicas que representa la dimensión con mejor estado de preparación por la implementación de medidas como aires acondicionados redundantes, planes de emergencia, sistemas contra incendio, entre otros controles.

Las otras dimensiones con promedio del 60%, también han implementado o tienen proyectado implementar acciones (proyectos, inversiones) que permiten mantener la prestación del servicio, como por ejemplo la gestión por procesos que se realiza actualmente en la compañía, que busca documentar, gestionar y controlar cada uno de los procesos de la Compañía, la gestión integral de riesgos y sus riesgos estratégicos (*Risk Focus*), la confiabilidad de la tecnología también está siendo mejorada con proyectos que contribuirán a la gestión y control de las tecnologías

de información y comunicaciones, o el robustecimiento con redundancia de las plataformas de red que soportan los servicios de UNE.

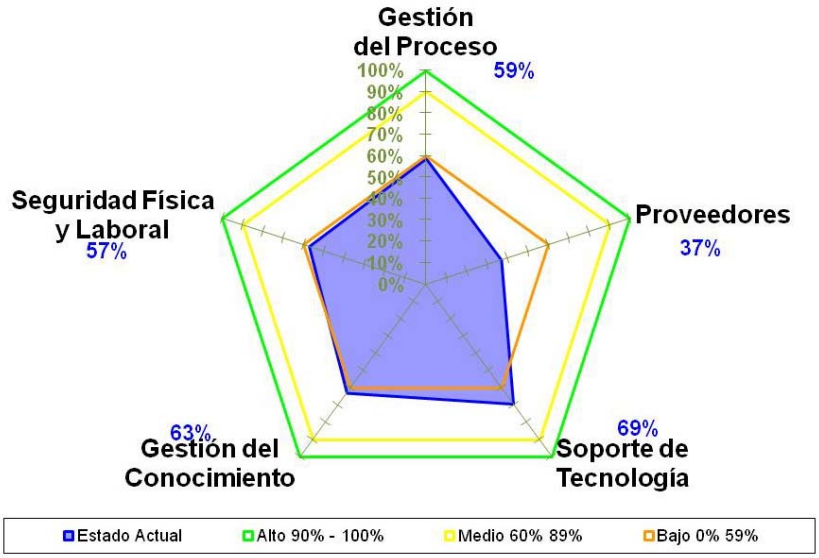
Sin embargo al analizar cada una de las dimensiones por separado y de acuerdo a los factores mencionados anteriormente, existen oportunidades de mejora para mantener la continuidad y factores en los cuales se debe trabajar para aumentar los índices de continuidad.

A continuación se realiza un análisis en cada una de las dimensiones, allí se pueden observar los posibles riesgos que podrían afectar la continuidad. Además se realiza un cruce con los riesgos estratégicos identificados por UNE en el estudio de Risk Focus.

2.4.1 Riesgos en personas y procesos. Al realizar la evaluación de riesgos de continuidad afectados en las dimensiones de procesos y personas, se estableció que existen oportunidades de mejora para lograr un nivel ideal en la administración de continuidad de negocio, esta evaluación se centró en los procesos que soportan los productos y servicios que entrega UNE a sus clientes.

Al realizar el recorrido por cada uno de ellos, se analizó la gestión del conocimiento, la gestión de los procesos, los proveedores que soportan los servicios, la percepción de los servicios de tecnología y las medidas preventivas adoptadas para mantener los niveles de seguridad y salud ocupacional, que ayuden a mitigar riesgos de continuidad. A continuación se ilustra el estado actual de preparación para esta dimensión:

Figura 9. Estado de riesgos de continuidad en personas y procesos



Al observar los factores que afectan la continuidad en la gráfica se puede decir que existen oportunidades de mejora de continuidad en personas y procesos estas oportunidades de mejora están relacionadas así:

GESTIÓN DEL CONOCIMIENTO

Pese a que UNE es una Compañía relativamente nueva, registra una alta socialización y conocimiento del sistema de gestión integral, lo cual representa una fortaleza para la gestión del conocimiento, ya que la información allí consignada es fundamental para la ejecución de los diferentes procesos, procedimientos e instructivos de trabajo de la Compañía. Además, se cuenta con proceso de selección de personal basado en perfiles, con habilidades y conocimientos necesarios para desempeñar los cargos asignados que permite mitigar riesgos de interrupción por falta de habilidades o conocimiento requeridos. Sin embargo, se observaron puntos importantes que permiten disminuir el riesgo y que pueden ser reforzados para mejorar la continuidad de las operaciones, como:

- Programas de capacitación y fortalecimiento del conocimiento.

- Personal crítico (indispensable) en algunos procesos.
- Manejo y almacenamiento de Información.

SEGURIDAD FÍSICA Y LABORAL

En estos factores que pueden afectar la continuidad de los funcionarios de UNE, se encontró que UNE ha trabajado temas de planes de emergencias, simulacro de evacuación, salud ocupacional, planes de vacunación, optometría y audiometría, chequeo médico general, capacitación para manejo de alturas, entre otros. Sin embargo se requiere trabajar en aspectos que fortalezcan la continuidad y seguridad del recurso humano de la Compañía, como:

- Manejo de situaciones de crisis.
- Manejo de enfermedades contagiosas.

GESTIÓN DE PROCESOS

- Indicadores de gestión.
- Procedimientos alternos de trabajo.

PROVEEDORES

- Manejo de proveedores.
- Acuerdos de niveles de servicio (ANS) con proveedores.

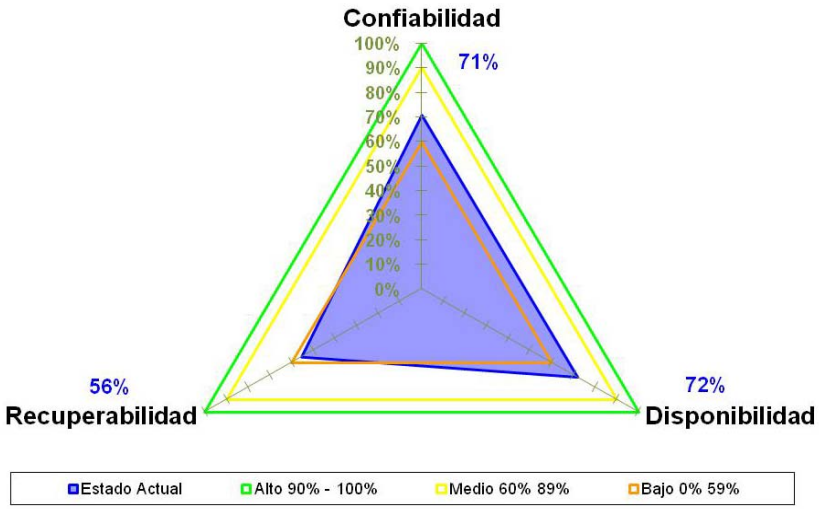
SOPORTE DE TECNOLOGÍA PARA LOS PROCESOS

|UNE es una empresa tecnológica que se integró con diferentes empresas del mercado de telecomunicaciones y adicionalmente viene adquiriendo otras empresas a nivel nacional. Toda esta integración trajo consigo un sin número de aplicaciones y servicios de TI que ayudan a soportar la operación de los procesos

de negocio, pero que a su vez vuelven compleja su operación y disminuye la confiabilidad, la cual podría generar interrupciones del servicio. Además, existen aplicaciones que soportan la operación de procesos de negocio que no son administradas directamente por UNE. Esta situación reduce el espacio de maniobra de UNE en relación con las actualizaciones y ejecuciones de procesos en los aplicativos que pueden afectar las actividades críticas del proceso.

2.4.2 Riesgos en tecnología. En el área de tecnología de información se evaluaron tres aspectos que afectan la continuidad de las operaciones que son: confiabilidad, disponibilidad y recuperabilidad. La confiabilidad evalúa aquellos procesos o procedimientos que sigue el área para administrar los servicios de tecnología, las plataformas, la capacitación y gestión del conocimiento. En disponibilidad se evalúa las acciones implementadas para proporcionar el nivel de servicio requerido por los clientes y usuarios de la Compañía. Y en recuperabilidad se evalúan las políticas y estrategias definidas para recuperar, resguardar o restablecer los servicios de tecnología en el tiempo requerido por UNE y sus procesos críticos. La siguiente gráfica ilustra el estado de preparación de la tecnología para afrontar la continuidad de negocio.

Figura 10. Estado de riesgos de continuidad en tecnología



CONFIABILIDAD

Problemas de integridad en los datos que procesan los sistemas de une: debido al crecimiento de la compañía, que ha llevado a la adquisición de nuevos sistemas de información, sumado a los diferentes proyectos de migración y unificación de plataformas y sistemas, se podrían presentar problemas de integridad a mediano y largo plazo que afectarían la continuidad del negocio. Se encontró que actualmente se presentan algunas inconsistencias de información entre ciertas aplicaciones del negocio.

No disponibilidad de proveedores críticos para atender emergencias o contingencias de tecnología: existe la posibilidad de que se presenten situaciones irregulares con proveedores de servicios, tales como quiebra, negación a prestar el servicio, alcance del contrato, no disponibilidad de recursos, entre otros, que sumado a la ausencia de un proveedor alterno como medida de contingencia, afectaría la prestación del servicio. Esta situación se observó en el caso del soporte de algunas aplicaciones críticas del negocio. Contractualmente, no se exige a los proveedores tener planes de contingencia probados que garanticen que siempre van a prestar el servicio a UNE con la calidad y oportunidad pactada en los ANS, aún cuando el tercero se encuentre en un estado de contingencia.

Posibles errores humanos en la administración y operación de la infraestructura de TI: no se evidencian procedimientos de recuperación documentados formalmente para recuperar toda la tecnología que soporta los servicios ofrecidos por UNE, con el riesgo de omisión o desconocimiento de actividades críticas para restaurar de forma efectiva y oportuna la operación; por áreas se tienen procedimientos informales para algunos servicios.

Caídas de los servicios prestados debido a fallas en la configuración de la infraestructura de TI: no se cuenta con el respaldo de configuración de todos los componentes; esto podría ocasionar demoras en el momento de una recuperación tecnológica por reprocesos en el levantamiento y re-configuración de los componentes tecnológicos; estas situaciones se podrían materializar en casos de cambios no exitosos, por ejemplo, cuando ocurren problemas de incompatibilidad en componentes nuevos (reemplazo, actualización, crecimiento) de las plataformas o actualizaciones erróneas de Software (Sistemas Operativos, aplicaciones, Firmware), y se hace necesario tener el backup de esta configuración para ejecutar el proceso de rollback. Sin embargo, de manera informal, los ingenieros se encargan de copiar y/o guardar la configuración de algunos de ellos en sus equipos de usuario, de acuerdo a las necesidades de sus áreas. La Compañía ha identificado falencias en este aspecto, y para ello se encuentra adelantando un proyecto para la implementación de una herramienta que les permita consolidar a través de formatos, toda la información de configuración de los componentes tecnológicos.

Posible incumplimiento de ANS: los acuerdos de nivel de servicio definidos a nivel estándar y con cada uno de los clientes corporativos pueden llegar a incumplirse por estar basados en información no confiable del porcentaje de disponibilidad. El indicador del porcentaje de disponibilidad del servicio es medido con base a los reportes de falla de de la mesa de ayuda (service desk), la cual refleja el tiempo de indisponibilidad percibido por los clientes, y no corresponde a un indicador medido con una herramienta de monitoreo que correlacione eventos de los componentes del servicio. Sin embargo, es importante anotar que la Compañía viene trabajando en un proyecto con el cual busca unificar el monitoreo de todos los componentes tecnológicos.

DISPONIBILIDAD

Bloqueo o fallas de la infraestructura TIC: algunas aplicaciones críticas no cuentan con redundancias que permita mantener la disponibilidad del servicio, situación que aumenta el riesgo de fallas intermitentes o totales de los sistemas cuando hay alto consumo de recursos o ante la falla de algún componente tecnológico.

RECUPERABILIDAD

Existe la posibilidad de no recuperar los servicios en los tiempos requeridos por el negocio: en la actualidad se cuenta con estrategias de redundancia de la red de telecomunicaciones (IAP, MPLS, IP) que por su tipología anillo permite recuperación del servicio de telecomunicaciones por rutas diferentes. En procesamiento de datos (ISP), se tiene estrategias de redundancia que permite recuperar el servicio de datos, y se ha comenzado a implementar un diseño de recuperación en sitio para los servicios ISP. Sin embargo, aunque existen iniciativas de recuperación y contingencia, estas son aisladas, no obedecen a análisis de impactos y no están definidas para recuperar los diferentes servicios tecnológicos en el tiempo requerido por el negocio (RTO, RPO), no se cuenta con esquemas de recuperación fuera de sitio para los servicios informáticos y la red de anillos nacional aun tiene puntos únicos de falla.

Existe la posibilidad de no recuperar la información respaldada en cintas: si bien existen procedimientos de copias de respaldo formales, no se realizan pruebas periódicas de restauración que aseguren la efectividad del procedimiento de copias de respaldo de datos, presentándose de esta forma posibles debilidades significativas en cuanto a la disponibilidad de la información vital y sensible de la Compañía, necesaria para la recuperación de servicios y operación de UNE.

Posible interrupción del servicio contratado con proveedores: dentro de los contratos realizados con proveedores de servicios no se exige planes de recuperación o contingencia para los servicios contratados, en caso de una falla en el proveedor, se puede ver afectado los servicios de UNE.

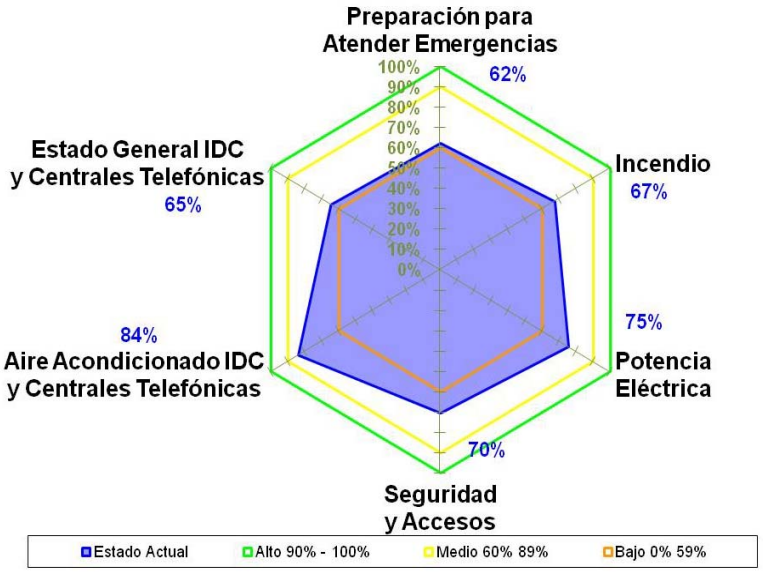
2.4.3 Riesgos en instalaciones físicas. A nivel de evaluación de riesgos en infraestructura física se deben realizar visitas a las sedes más representativas por concentración de personas, concentración de infraestructura tecnológica, aspectos administrativos y políticos, entre otros.

Durante el recorrido por las instalaciones se observan lugares como: oficinas, parqueaderos, archivos, subestaciones eléctricas, aires acondicionados, cuartos de plantas eléctricas, entorno del edificio, bodegas, nodos. El análisis del estado de preparación en aspectos físicos está dividido en seis componentes a evaluar:

- El estado de preparación para atender emergencias y administración de crisis.
- Los riesgos generadores de incendios importantes o catastróficos.
- El estado de preparación para atender un corte de energía importante.
- La preparación en temas de seguridad física y accesos.
- Aires acondicionados, falta de controles ambientales.
- Estado físico, seguridad, aspectos físicos de los nodos.

En el análisis, se compara el estado actual frente a buenas prácticas y estándares de seguridad física de edificaciones, estándares de construcción y preparación de emergencias y gestión de Data Center. Básicamente estos estándares ilustran un estado ideal y un estado mínimo deseable, dentro de los cuales se deben mantener las métricas de una organización para demostrar su estado de preparación en la administración de los riesgos.

Figura 11. Estado de riesgos de continuidad en instalaciones físicas



En la medición de riesgos realizada se puede observar que existen oportunidades de mejora, principalmente, en preparación para atender emergencias, prevención de incendios, y algunos temas puntuales por sede para algunos nodos; para los demás aspectos el estado de preparación se considera adecuado, sin embargo la Compañía debe trabajar para disminuir la brecha de riesgos físicos que existen la actualidad.

PREPARACIÓN PARA ATENDER EMERGENCIAS

Se encontraron problemas en algunas sedes relacionados a los siguientes aspectos:

- Demora en la atención de un conato de incendio.
- Imposibilidad de evacuar el edificio adecuadamente.
- Dificultad en el transporte de heridos en situaciones de emergencia.

INCENDIOS

En general en las sedes las construcciones cuentan con paredes sólidas que cortan el fuego y en su interior se observaron detectores de humos, roseadores (Sprinklers), extintores y en algunos casos pulsadores de emergencia manuales. Sin embargo, para prevenir un incendio; esto es insuficiente, y se detectaron los siguientes riesgos:

- Incendio inducido por gran cantidad de materiales combustibles
- Archivo Físico (lámparas sin protección)
- Incendio inducido por la planta de emergencia (combustibles)
- Incendios por edificaciones colindantes

POTENCIA ELÉCTRICA

- Interrupciones por corte de fluido eléctrico.

FLUJO DE AGUA

- Inundaciones en las sedes (tuberías en cielos rasos y lluvias)

ACCESO SEGURIDAD FÍSICA

- Foco de atentados terroristas y/o revueltas
- Imposibilidad de acceder a las instalaciones de las sede de UNE por terceros.

NODOS

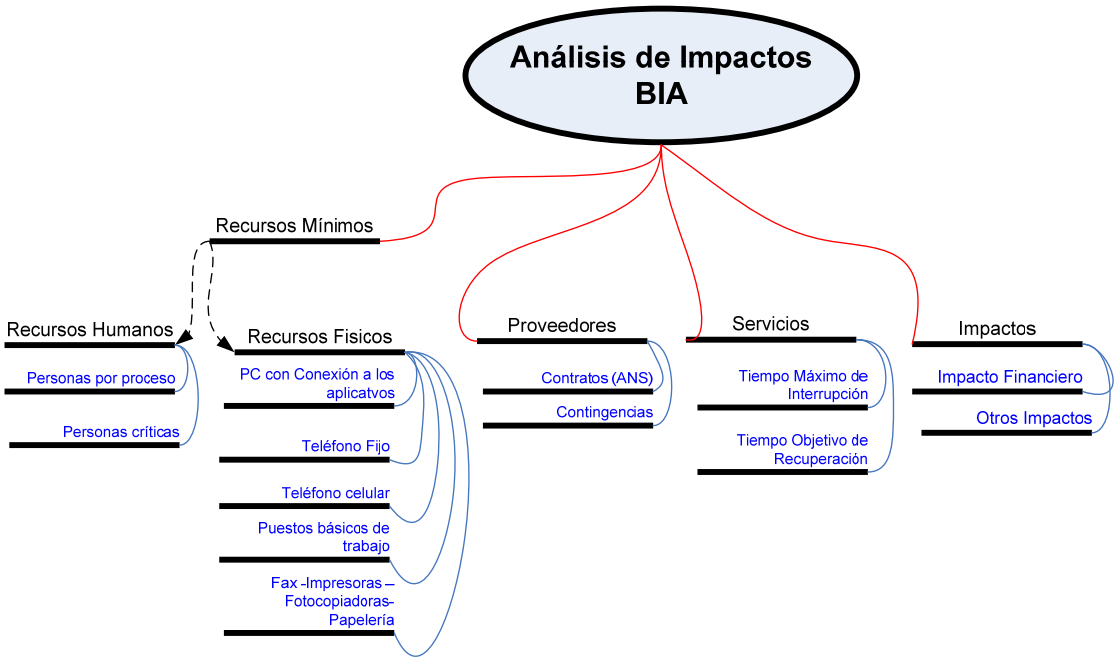
- Daños importantes o severos en equipos y/o plataforma Tecnológica.
- Demoras en la recuperación de conectividad (marcación de cableado y ausencia de piso falso).

- Pérdidas de medios con información respaldada en cintas.

2.5 RESULTADOS DEL ANÁLISIS DE IMPACTOS

El objetivo del análisis de impactos es identificar impactos que puedan generar un evento de interrupción sobre los servicios de UNE y sus procesos soporte e identificar los tiempos máximos de interrupción, en los cuales la Compañía esperaría seguir prestando sus servicios. El alcance del BIA de UNE abarcó los aspectos contenidos en el siguiente diagrama.

Figura 12. Analisis de impactos BIA



Para la realización del análisis de impacto se realizaron encuestas con los dueños y especialistas de procesos, y entrevistas con personal clave de las áreas impactadas.

La encuesta de Análisis de Impactos trata de ubicar a las personas en el escenario de la peor situación para cada una de sus operaciones, donde un evento de

interrupción puede afectar severamente la entrega de servicios de UNE. Bajo este escenario, las personas encuestadas dan su mejor estimativo, el cual se analiza y posteriormente se valida para obtener los resultados necesarios para determinar los posibles impactos generados por un evento de interrupción, los tiempos esperados para volver a la normalidad para cada uno de los servicios y procesos, y recursos mínimos requeridos (personas, equipos, tecnología) para mantener la operación.

Las encuestas realizadas se tabulan y analizan para determinar los posibles impactos por una interrupción del negocio y los tiempos en que debe seguir operando la Compañía para no incrementar los riesgos e impactos de la prestación de servicio a los clientes.

2.5.1 procesos críticos. Los procesos definidos como críticos se seleccionan con base en los resultados y análisis de las entrevistas realizadas a los dueños de procesos.

Los procesos que no se incluyeron en el análisis de impactos y la evaluación de riesgos son aquellos que tienen que ver con la estrategia y control y los procesos de planeación y factibilidad.

Los factores que primaron para seleccionar los procesos críticos son: la participación en la entrega directa de servicio a los clientes y como una interrupción en el proceso puede afectar esta entrega e incumplir los acuerdos de servicio pactados con los clientes actuales UNE.

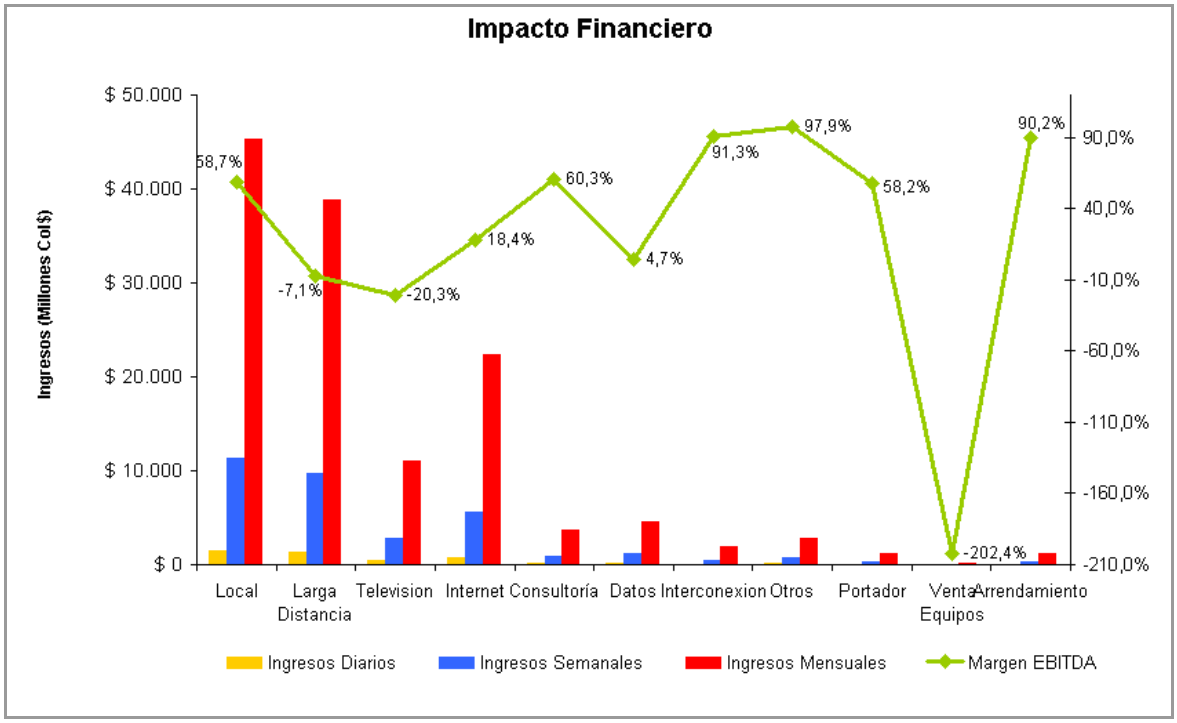
En un nivel de madurez mayor en gestión de continuidad los procesos que no tienen relación directa con la entrega del servicio deberán ser tenidos en cuenta y definirse estrategias que permitan mantener la continuidad de estos.

2.5.2 Impacto de una interrupción. Dentro del análisis de impactos se toman diferentes factores de riesgo que podrían ocasionar impactos a UNE, a nivel financiero, operacional y legal, entre otros.

IMPACTO FINANCIERO

El análisis de los impactos financieros de UNE se evalúa teniendo en cuenta el escenario del peor de los casos para cada uno de los servicios, productos o procesos enmarcado en un periodo de tiempo crítico. Estos impactos fueron hallados según el promedio de ingresos a marzo de 2009 para los productos y/o servicios macro de UNE. La siguiente gráfica ilustra el impacto financiero hallado:

Grafico 1. Impacto financiero



El impacto de una interrupción en la prestación de los servicios de telecomunicaciones varía según el tipo de cliente, la relación contractual que mantiene con la Compañía y la zona geográfica en la que está ubicado. Un cliente

de hogares, que tiene sus servicios empaquetados, probablemente no va a generar un mayor impacto financiero si ve el servicio de Internet interrumpido por un día, pero un cliente corporativo, para el que este servicio es fundamental para su *core*, tiene establecidos ANS con la empresa que incluyen el pago de multas en caso de incumplimiento de los mismos, lo que genera un mayor impacto financiero.

En la gráfica anterior se observa el impacto financiero de una interrupción en los servicios de UNE para periodos de tiempo de día, semana y mes. Como podemos observar los servicios local y larga distancia concentran el mayor impacto financiero representando el 63% de los ingresos de UNE, estos ingresos están acompañados del margen *EBITDA* por cada producto y/o servicio equivalentes al 59% y 7% respectivamente.

Es importante mencionar que una afectación del servicio de Internet impactaría financieramente en los ingresos de UNE en una gran cantidad y si se tiene en cuenta que el margen *EBITDA* de este servicio es del 18%, la magnitud sería mayor. Analizándolo mas detalladamente se ve que por cada $100 que se dejen de vender en UNE, existe una utilidad dejada de percibir de $18, la cual puede destinarse para el pago de impuestos y para el pago de dividendos a los accionistas de la Compañía.

Adicional a estos impactos que se reflejan en la afectación del ingreso, se pueden evidenciar impactos financieros por otros factores que son difíciles de cuantificar y serán tratados como otros impactos.

Indemnizaciones: en términos contractuales, el incumplimiento de los ANS, principalmente con los clientes corporativos, podría ocasionar multas que son fijadas en cada contrato. Para hogares, el incumplimiento de acuerdos comprometidos por la Compañía podría ocasionar quejas y reclamaciones que

afectan económicamente la Compañía, con pago de resarcimiento por aplicación de figura de silencio administrativo, la cual se presenta si al cliente no se le da respuesta en un máximo de 15 días.

Nómina ociosa: la interrupción en la operación normal de UNE generaría el pago de nómina sin que este pago esté asociado a la producción y prestación de servicios.

Sanciones: a nivel de regulación, los entes de control pueden imponer sanciones por la interrupción en de prestación de los servicios, la acumulación de sanciones puede acarrear intervenciones por parte de los entes de control y ser causales de retiro de la licencias. A nivel contractual, el incumplimiento en contratos con el estado podría ocasionar sanciones al servicio prestado (caducidad del contrato) e inhabilitar a UNE para prestar ese servicio por un periodo de tiempo (normalmente 2 a 5 años).

OTROS IMPACTOS

Durante el desarrollo de las encuestas se recolecta información sobre los posibles impactos que se presentan a causa de una interrupción de los servicios que pueden agregar pérdidas monetarias, humanas, legales, entre otras, pero que en su evaluación son difíciles de cuantificar, por lo que se evalúa de forma cualitativa. Los otros impactos que se dimensionaron por parte de los encuestados fueron:

Deterioro de servicio al cliente: el servicio al cliente se ve afectado desde el primer minuto de interrupción, podríamos clasificar, en el sector de severo, los clientes corporativos, que dependen totalmente de UNE como socio de negocio para los servicios contratados.

Pérdida de imagen y posicionamiento de marca: la imagen de la Compañía se ve afectada por una interrupción, principalmente en eventos mayores a un día. Para recuperar su posición en el mercado, se tiene que generar gasto en publicidad y resarcimientos a grandes clientes, lo que generará impactos económicos adicionales.

Pérdida de productividad: después de una semana de interrupción se afecta de manera importante la productividad de las personas, que puede aumentar el impacto económico percibido.

Pérdida de oportunidades y nuevos clientes: se puede llegar a presentar deserción de clientes o no ingresar nuevos clientes por interrupción de los servicios, esto principalmente se presenta en una semana de interrupción.

Penalizaciones y sanciones: el tema de multas o sanciones de los entes de control, es un tema delicado, que según el evento y la comunicación que haga la Compañía del mismo, podría llegar a ocasionar impactos severos en el tiempo.

Reprocesos y trascripción de documentos: en aquellos procesos donde se realizan planes alternos de trabajo manual, se puede ver transcripciones, para otros la pérdida de trabajo ejecutado según el evento ocasiona reprocesos significativos en una semana de interrupción.

Interrupción a otras áreas y/o entes externos: las interrupciones de otras áreas (clientes internos), que ocasionaría en cadena una interrupción a los clientes externos, además de afectar socios comerciales o filiales.

Afectaciones al estado de ánimo del personal: este es uno de los impactos que refleja menor grado de severidad en las primeras horas, sin embargo con eventos superiores a una semana, se vuelve crítico para encontrar soluciones.

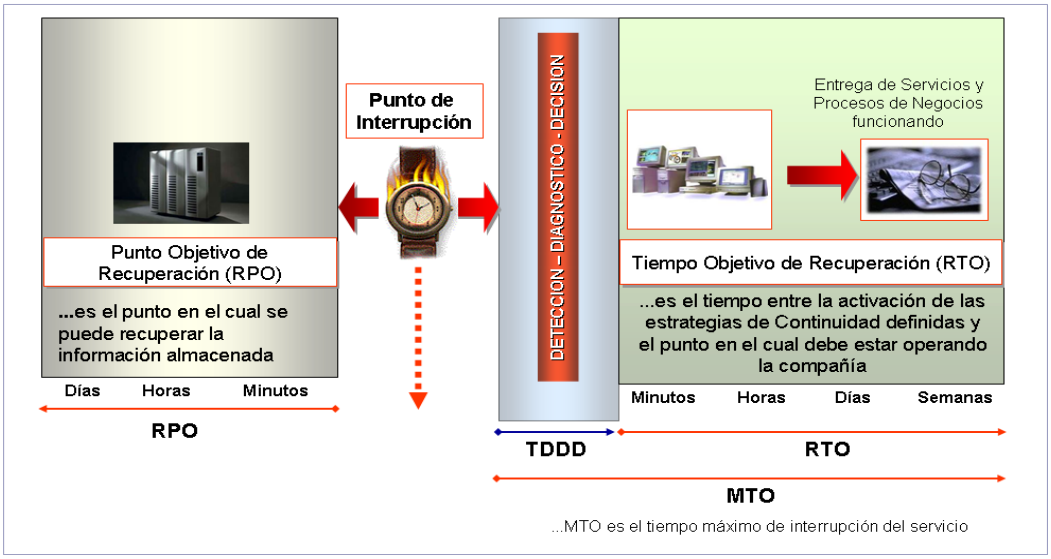
2.5.3 Dependencia de servicios informáticos. La operación normal de los procesos de negocio requiere de aplicaciones y servicios TIC que soporten las actividades del día a día, agilizando o simplificando el trabajo que las personas desempeñan. La dependencia de estas herramientas se ha vuelto crítica, y la falta de éstas podría impactar severamente la operación y los servicios de UNE.

A cada encuestado se le pregunta por los servicios de TI y su criticidad (aplicaciones de negocio, aplicaciones de escritorio, redes, almacenamiento en red) para soportar el día a día de su operación.

Esta criticidad, en conjunto con los tiempos de interrupción, permite definir las estrategias requeridas para mantener la operación tanto de los procesos de negocio como de los servicios que presta UNE a sus clientes.

2.5.4 Tiempos de recuperación. Los tiempos de recuperación fueron identificados de acuerdo al escenario del peor caso, en el cual los procesos se encuentran en una situación en que los recursos requeridos no deberían faltar para continuar prestando los servicios a los clientes.

Figura 13. Tiempos de identificacion



TIEMPO MÁXIMO DE INTERRUPCIÓN (MTO)

Hace referencia al tiempo máximo permitido para recuperar los recursos del servicio (MTO), este tiempo le indica al negocio cuanto tiempo podría tomarse para restablecer el servicio antes de que se materialicen los diferentes impactos sobre la Compañía.

Para hallar el tiempo Máximo de Interrupción de la Compañía se pregunta a los dueños y especialistas de los procesos críticos de negocio, acerca de los servicios informáticos (aplicaciones, telecomunicaciones, herramientas) utilizados para prestar los servicios normales de la Compañía. Con la experiencia y conocimiento de cada encuestado, a cada servicio informático se le relaciona el tiempo en el cual podría verse afectada la operación y generar impactos sobre la Compañía desde su proceso. Al analizar los resultados se identifican los servicios según su impacto.

Otros tiempos máximos de interrupción se deben hallar para la infraestructura TIC (plataformas) que soportan los servicios que presta UNE a sus clientes, estos tiempos se hallan mediante análisis de la información suministrada (mapeo de interdependencias), y de la evaluación de los ANS prometidos por la Compañía a sus clientes.

Se observa que casi la totalidad requiere tiempos de recuperación menor a un día, lo que requiere de estrategias que permita fortalecer los porcentajes de disponibilidad de cada uno de los componentes que hacen parte de los diferentes servicios.

TIEMPO OBJETIVO DE RECUPERACIÓN (RPO)

Hace referencia al tiempo en que los procesos de negocio se podrían reconstruir o volver a obtener información de su operación normal. Esto quiere decir, cuanta información se podría perder en un evento de interrupción o desastre, sin generar impactos a los procesos, servicio y en general a la Compañía.

Para los servicios con tiempos cortos de RPO se necesitan mantener estrategias robustas de respaldo de información, principalmente los servicios informáticos que soportan el mayor número de procesos de negocio.

Algunos servicios informáticos requieren de estrategias de respaldo complejas pero menos robustas ya que su apetito de riesgo es de un día de pérdida de información. Esto puede darse porque la información se puede reconstruir por otros medios o se puede solicitar de nuevo al remitente.

En todo caso para cada uno de los servicios informáticos se tiene que validar su criticidad y soporte a los procesos de negocio, para definirle estrategias costo/beneficio que permita mantener la información requerida por los usuarios y la Compañía.

2.5.5 Recursos mínimos. Los recursos mínimos o críticos hacen referencia a personas o elementos que son requeridos ante la ocurrencia de un evento de interrupción o desastre que afecte la operación normal de UNE. Estos recursos son tomados como base en la definición de estrategias de continuidad, deberán estar dispuestos y su utilización dependerá del evento ocurrido.

PERSONAS CRÍTICAS

Se pregunta a los líderes de procesos de negocio sobre las personas que normalmente ejecutan las actividades del día a día, luego se ubica bajo un escenario del peor caso, el cual permitiera hallar el número de personas mínimas (o críticas) requeridas para continuar una operación aceptable ante un evento que afecte críticamente la operación de su proceso.

Al realizar este análisis los encuestados manifiestan que el ejercicio de ubicarse bajo un escenario crítico y reducir el número de personas era complejo de resolver, porque el número actual de personas ya es bajo para cumplir con todas las actividades del proceso.

OTROS RECURSOS MÍNIMOS

Los elementos mínimos identificados son aquellos que requieren los procesos para continuar su operación bajo un escenario de interrupción de sus operaciones normales. Los elementos identificados son principalmente elementos de oficina que serán contemplados en la definición de estrategias y alternativas para mantener la continuidad.

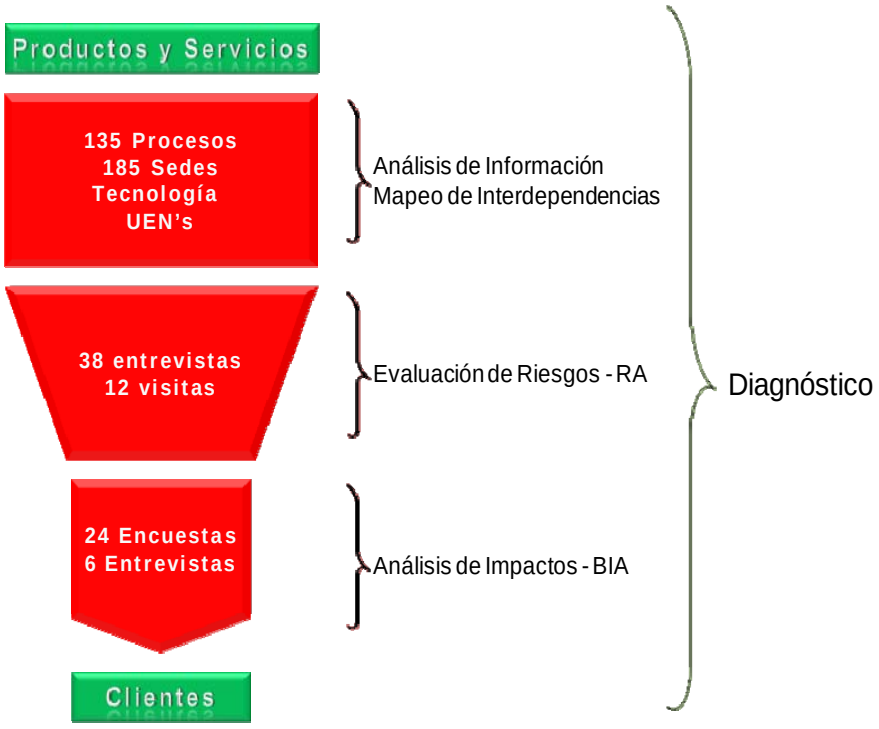
Los recursos mínimos, tanto en personas como en elementos de oficina, ayudan a soportar eventos de interrupción que afecten la operación de los procesos, pero que en el tiempo puede llegar a volverse críticos y no soportar un evento por mucho tiempo. Si el evento, por el cual fue activada la contingencia no es superado, la Compañía deberá asegurar la consecución de los recursos normales, que apoyan la ejecución de las actividades en el día a día.

2.6 DIAGNÓSTICO DEL ESTADO ACTUAL DE LA COMPAÑÍA

El diagnóstico de continuidad del estado actual de UNE, resume las resultados encontrados durante las actividades de evaluación de riesgos de continuidad, el mapeo de interdependencias y el análisis de impactos de negocio.

La fase de diagnóstico de continuidad pretende analizar cómo se ven afectados los productos y/o servicios que presta UNE a sus clientes y cuáles son las acciones, controles o estrategias que ha adoptado la Compañía para mantener la entrega de esos servicios. El diagnóstico inicia su análisis con la identificación del portafolio de productos y/o servicios de UNE, luego se analizan los procesos, la tecnología que soporta la entrega de esos servicios y las instalaciones donde se encuentran.

Figura 14. Filtro realizado en el diagnóstico de continuidad

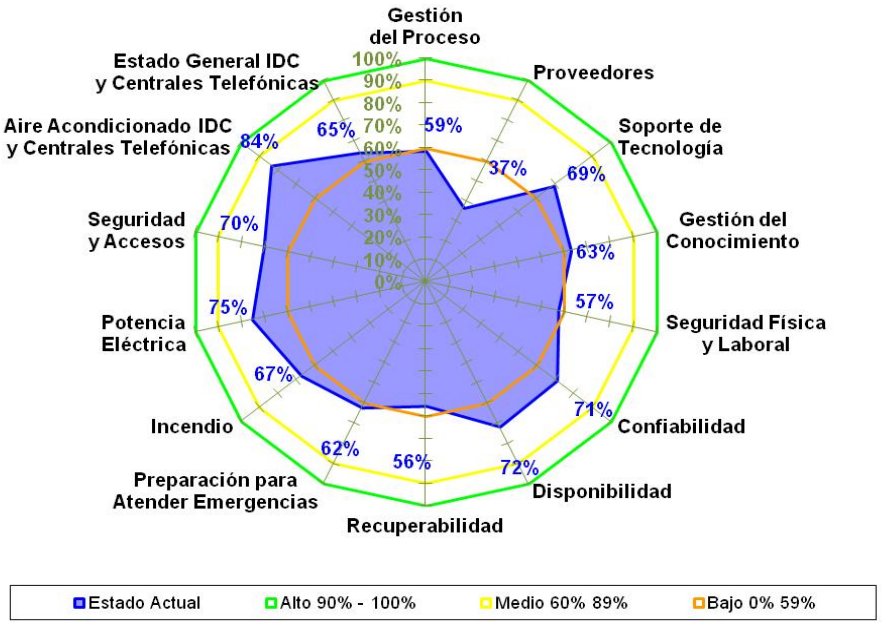


Estos análisis iníciales permitien identificar qué procesos, instalaciones y tecnología afectan directamente la continuidad de negocio y la prestación de servicios a los clientes UNE.

Es importante aclarar que el alcance del diagnóstico y la evaluación se limita a identificar el estado actual de elementos del Plan de Continuidad de Negocio (*BCP*) y no del estado actual de un sistema (programa, proceso) de administración de continuidad de negocio (*BCM)*

El estado general del diagnóstico es el resultado de analizar información existente, realizar entrevistas y encuestas a los líderes y especialistas de procesos, líderes de tecnología, líderes de áreas de apoyo (Jurídica, RRHH, Financiero) y visitas a instalaciones físicas de UNE. Estas actividades buscan responder una serie de preguntas que ayudan a ubicar a la empresa en un nivel de continuidad, frente a buenas prácticas y estándares del mercado. En la siguiente gráfica se ilustra el nivel en que se encuentra la Compañía en temas de continuidad:

Figura 15. Nivel de la compañía en temas de continuidad



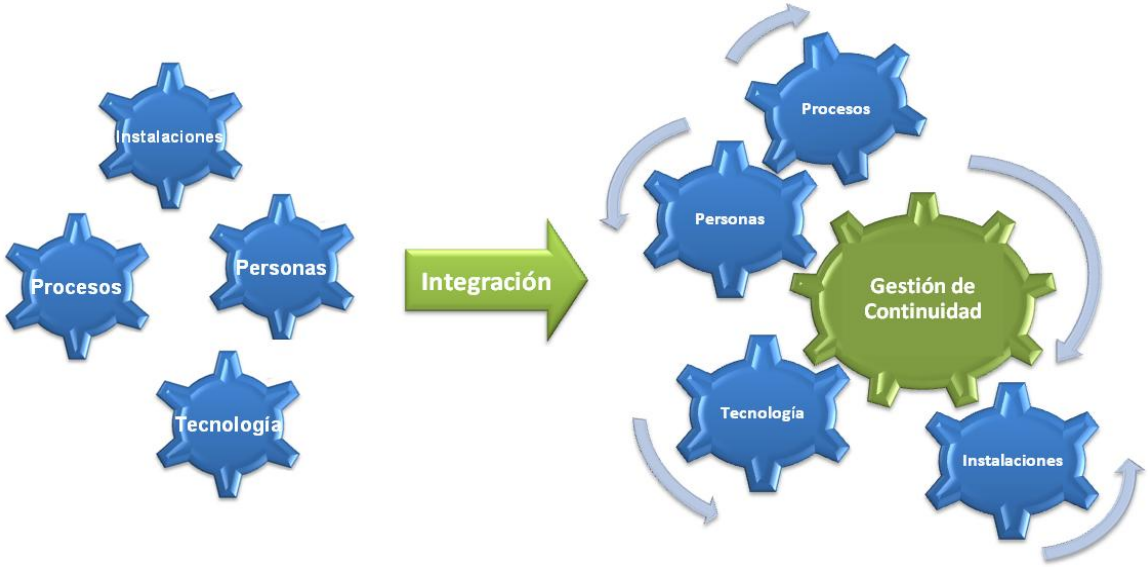
Es importante recordar que la evaluación obedece a una muestra estadística según la entrega de servicios a los clientes UNE y no se realizó para el 100% de la organización a nivel de personas, procesos, tecnología e instalaciones.

Se puede observar en la gráfica que el estado actual de continuidad de UNE se encuentra entre niveles bajo y medio. Los puntos medios se pueden explicar por la madurez de su implementación y la adopción de buenas prácticas que se han mantenido en el tiempo, como son las de velar por los adecuados controles en las instalaciones físicas (aires acondicionados redundantes, controles de acceso, acometidas eléctricas redundantes, entre otros), adquisiciones de equipos tecnológicos con características de tolerancia a fallas (*fault tolerance*), documentación de procesos, capacitaciones, entrenamientos, entre otros.

Los puntos bajos se explican por la dinámica normal de la Compañía, por ser relativamente nueva (escisión), por los proyectos en curso, por la adopción de nuevas tecnologías, pero que requiere de acciones que permitan aumentar su nivel.

En definitiva se encontró que UNE tiene implementados controles, definido estrategias y desarrollado proyectos que permiten mantener niveles de continuidad en las diferentes dimensiones. Pero que a su vez todas estas acciones obedecen a iniciativas aisladas en las diferentes dimensiones, que no tienen interrelaciones o pueden doblar esfuerzos, que al final no permiten mostrar un sistema de gestión de continuidad integro.

Figura 16. Iniciativas de continuidad



Con esta evaluación se puede concluir que UNE tiene oportunidades de mejora en aspectos de continuidad, los cuales permitan mantener niveles de continuidad esperados por la Compañía y sus clientes.

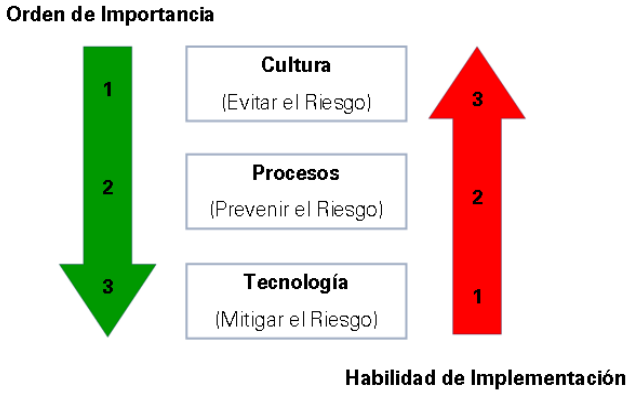
3. DEFINICIÓN DE ESTRATEGIAS PARA LA IMPLEMENTACIÓN DE CONTINUIDAD DE NEGOCIO

3.1 DEFINICIÓN DE ESTRATÉGIAS SEGÚN EL DIAGNÓSTICO OBTENIDO

La definición de estrategias se enmarca en las dimensiones de personas, procesos, tecnología e infraestructura física y se adecúa a las necesidades de UNE según el diagnóstico de la situación actual en continuidad, el cual incluye la evaluación de riesgos (*RA*) y el análisis de impactos (*BIA*). Adicional a los resultados del diagnóstico, las estrategias deben ser alineadas al plan estratégico de tecnología, y a los requerimientos de servicio de la compañía, por lo que las estrategias de continuidad definidas para cubrir las dimensiones principales son:

- Sistema de gestión de continuidad de negocio – SGCN.
- Estructura para el *BCP* (Manejo de crisis).
- Fortalecimiento de Acuerdos de Niveles de Servicio.

Figura 17. Orden de importancia y habilidad de implementación de las estrategias



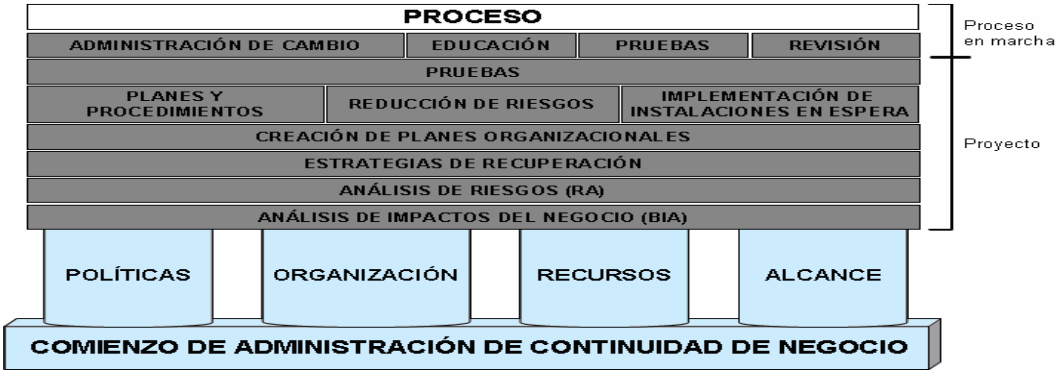
De acuerdo a la naturaleza de las estrategias definidas, estas pueden tener un orden de importancia y una habilidad de implementación que permitirá mitigar

riesgos de continuidad, siendo uno la más importante y tres la menos importante. Las estrategias definidas son consideradas las de mayor acercamiento a las necesidades de UNE y son abordadas como las más recomendables para su implementación siendo uno la más compleja de implementar y tres la más sencilla, sustentado en las buenas prácticas del mercado y propuestas de asesores expertos, según su conocimiento y experiencia; sin embargo, corresponde a UNE tomar la decisión de las estrategias que serán implementadas.

3.1.1 Estrategia 1: sistema de gestión de continuidad de negocio [SGCN]. Un sistema para administrar la continuidad se fundamenta en el ciclo de sistemas de gestión y mejora continua (PHVA) y define el conjunto de políticas, procesos, funciones y estructura que ayudan a establecer el marco de actuación bajo el cual se administra la continuidad.

Tanto las políticas como los procesos de administración de la continuidad, son base fundamental para alcanzar un ambiente mejorado y dispuesto en organizaciones que buscan constantemente mantener y facilitar la continuidad de sus operaciones claves que son soporte del negocio. Lograr mantener la continuidad del negocio es una habilidad que requiere la definición de un marco de referencia proactivo que facilite la alineación de las personas, los procesos, la tecnología y las actividades del día a día.

Figura 18. Comienzo de administracion de continuidad de negocio



El marco de referencia se establece mediante la implantación, adopción y cumplimiento de un sistema para administrar la continuidad, enmarcado en:

- Políticas para Administrar la Continuidad.
- Procesos para Administrar la Continuidad.
- Estructura organizacional para Administrar la Continuidad.
- Administración del Cambio en Continuidad (Cultura).

POLÍTICAS PARA ADMINISTRAR LA CONTINUIDAD

Las políticas referentes a las acciones y actividades que ayudan a mantener la continuidad deberán ser ampliadas en el sistema de gestión de continuidad –SGCN –a ser implementado por UNE. Estas políticas deberán estar definidas para cada una de las dimensiones que de alguna forma inciden o impactan la continuidad de las operaciones de los servicios y/o procesos críticos del negocio. A continuación se enuncian los componentes que deben de contener políticas que sirvan como base para establecer el programa de continuidad de negocio de UNE.

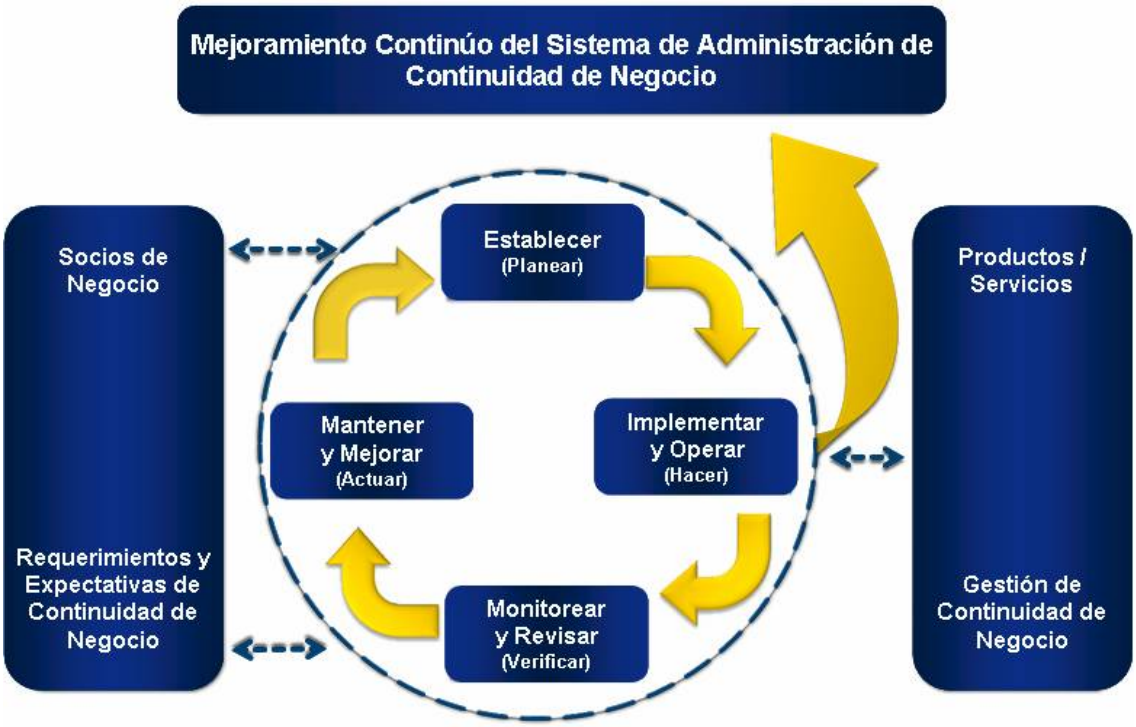
- Compromisos directivos y de participantes.
- Personas.
- Procesos de negocio.
- Instalaciones físicas.
- Infraestructura tecnológica.

PROCESOS DE ADMINISTRACIÓN DE LA CONTINUIDAD

Los procesos de administración de la continuidad se definen como la gestión disciplinada de mejoramiento y monitoreo continuo con el fin de proporcionar niveles de continuidad acorde con las necesidades del negocio.

Los procesos de administración de la continuidad se componen de cuatro fases basadas en el ciclo de sistemas de gestión de calidad, como ilustra la siguiente gráfica del marco de actuación del sistema de administración de la continuidad:

Figura 19. Mejoramiento continuo del sistema de administracion



Establecer (Planear): determinar que es importante para UNE, planear acciones para mantener la continuidad, definir roles y responsabilidades, y mejorar la cultura organizacional en temas de continuidad.

Implementar y Operar (Hacer): determinar el estado actual de la continuidad, aspectos que representan riesgos e impactos para la continuidad de UNE identificar y desarrollar soluciones de continuidad, definición de arquitecturas, políticas, normas y procedimientos orientados a elevar los niveles de continuidad.

Monitorear y Revisar (Verificar): verificar el cumplimiento de las políticas y procedimientos definidos para mantener la continuidad. Monitoreo de los acuerdos de servicio que permitan mejorar y mantener la continuidad de la operación de

UNE. Realizar las revisiones (Auditorias) al Sistema de Administración de Continuidad.

Mantener y Mejorar (Actuar): actualizar, probar y entrenar los planes de continuidad de negocio y respuesta a incidentes. Definir acciones correctivas y de mejoramiento al sistema de continuidad, y a los productos y servicios de UNE.
El sistema de gestión o el procesos para administrar la continuidad al interior de UNE debe estar alineado a la estructura actual de procesos, en el cual se integre de forma transparente y transversal a la operación del día a día.

ESTRUCTURA ORGANIZACIONAL PARA ADMINISTRAR LA CONTINUIDAD DE NEGOCIO

Generalmente, la gestión relacionada a temas de riesgos, continuidad o seguridad expresada bajo la responsabilidad y adopción de cada área o persona de la organización tiende al fracaso, a menos que exista al interior de la organización un nivel de madurez y proceso capas de afianzar y fortalecer la cultura en la disciplina de los individuos que la componen.

La administración de la continuidad requiere del esfuerzo y compromiso de cada una de las personas y de la estructura organizacional que hoy opera en UNE. La continuidad de los servicios, y en general del negocio, es responsabilidad de todos y cada uno de los funcionarios de UNE; sin embargo, debemos ser claros que la administración de la continuidad requiere de la presencia de un líder con visión holística de la organización, que motive y desarrolle las condiciones necesarias para lograrlo el éxito de la gestión de la continuidad.

El responsable de la administración de la continuidad, entendiendo administración como el liderazgo a ejercer sobre los temas relacionados con la continuidad, debe estar lo suficientemente capacitado para ejercer su función, contar con el apoyo y patrocinio del comité directivo de la compañía, y estar acompañado de un pool de

personas que ayuden a mantener la continuidad en la operación en cada una de las áreas.

La definición de una estructura que permita administrar la continuidad debe cumplir con unos requerimientos mínimos que facilite la administración efectiva de la continuidad en UNE, estos requerimientos son los siguientes:

Independencia

Quienes tengan la responsabilidad de administrar continuidad deben tener la suficiente independencia en responsabilidad, funcionalidad y autonomía para lograr los siguientes objetivos:

- Velar por el cumplimiento de las políticas de continuidad.
- Opinar y advertir sobre el incumplimiento o desajuste de los procesos definidos para administrar la continuidad.
- Asesorar en la planeación, diseño y ejecución de pruebas de cumplimiento relacionadas con los planes de continuidad.
- Asesorar a la Alta Gerencia en la implementación de políticas, normas, procedimientos y estrategias de continuidad.

Direccionamiento

La administración de la continuidad debe contar con un direccionamiento permanente que facilite el ajuste y actualización de las estrategias de continuidad previamente definidas por la compañía.

Oportunidad

La independencia y direccionamiento requeridos para una efectiva administración de la continuidad deben ir acompañados de acciones oportunas, directas y rápidas

que le permitan a UNE mantener el control proactivo y preventivo orientado a mantener la continuidad.

Responsabilidad

La administración de la continuidad exige el compromiso permanente de los individuos responsables de su direccionamiento y manejo, y es por ello que sus funciones, roles y responsabilidades deben primar sobre cualquier otra responsabilidad asignada, sea esta temporal o no.

Liderazgo

La continuidad debe tener un responsable de su administración con capacidad de:

- Sensibilizar a líderes de servicio, gerentes de producto, o funcionarios en la importancia de aplicar siempre los lineamientos de continuidad en la planeación y ejecución de los servicios y/o procesos.
- Propender por la alineación de las estrategias de continuidad con los diferentes planes de emergencias, manejo de crisis, comunicación de crisis, recuperación de procesos de negocio, planes de recuperación de desastres, entre otros.

Las alternativas de estructura de continuidad de negocio que se definen para ser implementadas al interior de UNE, están acordes a las buenas prácticas, estudios de mercado y la estructura organizacional de UNE. Estas buenas prácticas establecen que la estructura que administre y vele por la continuidad dentro de las organizaciones, ***debe actuar de forma independiente y reportando directamente de la presidencia***, en otros casos y debido a la similitud de actividades y objetivos, ***se involucra la administración de continuidad bajo la dirección de la gestión de riesgos empresarial***. La decisión dependerá de la compañía y el nivel de madurez que tengan para asimilar el tema.

A continuación se presentan dos alternativas recomendadas por las buenas prácticas y utilizadas por las organizaciones:

Alternativa 1: Área de continuidad reportando al área de gestión de riesgos de la compañía

Una de las buenas prácticas que se viene desarrollando en las organizaciones es integrar la gestión de continuidad, con la gestión de riesgos empresarial.

Las interpretaciones de los modelos de riesgo varían ampliamente por industria y entre organizaciones, pero coinciden en que es un enfoque desde arriba hacia abajo, basado en y soportado por una estrategia organizacional, que se centra en nuevas formas de administración y optimización de riesgos de mayor importancia para la alta gerencia (Presidencia, Junta Directiva).

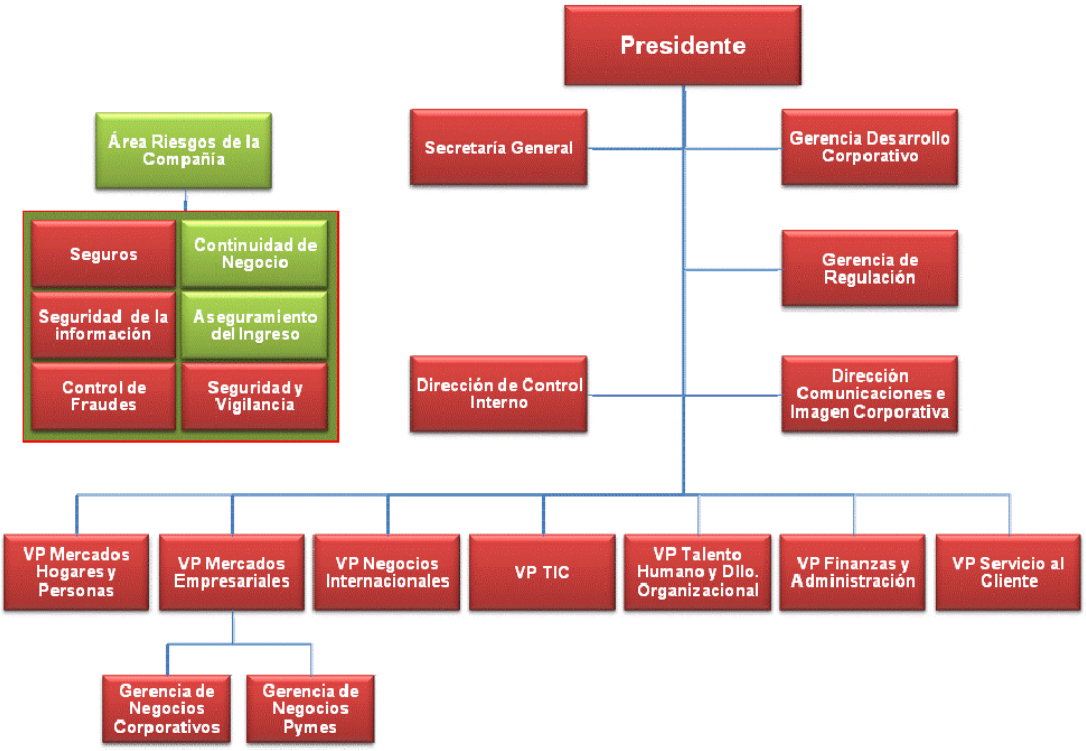
Estos modelos de gestión de riesgo empresarial – ERM - buscan la efectividad y eficiencia en la gestión integral de riesgos, reduciendo complejidad y costos, soportando los nuevos productos y servicios de la compañía, quitando barreras por baja cultura y entrenamiento en gestión de riesgos, incrementando los recursos para desempeñar las actividades, y ayudando a la compañía a realizar sus objetivos, estrategias y visión de negocios.

La administración de riesgo introduce rutinas orientadas a identificar, medir y administrar activamente las amenazas que puedan desviar la consecución de las estrategias de negocio, avanzando cada vez en el desarrollo de la cultura de riesgos al interior de la compañía. Como consecuencia, la gestión de riesgo está comenzando a ser percibida como una nueva forma de administración estratégica de negocios, relacionando la estrategia del negocio con los riesgos cotidianos.

Los modelos de administración de riesgos actuales se desarrollan en un contexto de gestión integral (visión holística) que permita optimizar y capitalizar oportunidades dentro de un portafolio de riesgo y no solo establecer controles de mitigación para los riesgos encontrados en las diferentes áreas. Esta gestión integral permite identificar los riesgos críticos que la compañía y no solamente riesgos financieros, crediticios o asegurables incluyendo, sino también: reputación, operativo, regulatorio, continuidad, salud, seguridad, o medio ambiente.

Con este contexto de gestión de riesgos empresarial, se define entonces una alternativa de la estructura de continuidad que apalanque las buenas prácticas de gestión de riesgos al interior de UNE, y permita no solo administrar la continuidad de negocio, sino los riesgos con visión holística e integra, acorde a las buenas prácticas para la gestión de continuidad. La estructura que resultó de este análisis fue la siguiente:

Figura 20. Estructura de continuidad reportando al área de riesgos



En la gráfica anterior se ilustra una estructura con un área de riesgos que contiene áreas afines de gestión de riesgos, y la cual se encuentra como una isla, sin conexiones a la estructura actual de UNE. En esta isla podemos encontrar áreas en rojo para diferenciar áreas existentes (áreas dispersas en otros niveles), y en áreas en verde que son las áreas que actualmente no existen. Es deber de UNE establecer según su cultura y madurez de gestión, la dependencia o el área del cual deberá depender el área de gestión de riesgos, de acuerdo a los siguientes requerimientos de la estructura:

- Visión Holística.
- Independencia.
- Direccionamiento.
- Oportunidad.

La alternativa y la definición de gestión de riesgos se toman como base de la concepción de gestión por procesos, en la cual podemos decir que la compañía es un sistema de sistemas, cada proceso es un sistema de funciones, y las funciones o actividades se agrupan por departamento o áreas. Así la estructura definida sería la ideal dentro de las buenas prácticas para administrar la continuidad.

Esta permitiría agrupar actividades y compartir información dentro de la gestión de riesgos, disminuir esfuerzos, definir estrategias más ajustadas para mitigar riesgos no solo de continuidad sino de la operación del día a día y monitorear en conjunto la gestión de riesgos al interior de la compañía. Sin embargo, esté análisis no pretende modificar la estructura organizacional actual de UNE (esta fuera del alcance), y solo se define como una posible alternativa para la creación del sistema de gestión de continuidad de negocio.

Ventajas:

- Alineación de la estrategia de riesgos con la estrategia de negocio, que permite crear valor.
- Una sola área con una visión global de riesgos que permite definir acciones integradas para optimizar recursos, tiempo y controles para mitigar riesgos de la compañía.
- Interacción de las áreas de riesgo de la compañía, que comparte información y provee claridad en los riesgos claves de la organización.
- Definir oportunamente estrategias o controles de manera integral sobre riesgos de la compañía.
- Se tiene una gestión de riesgos más asertiva y mejora la eficiencia de los controles.
- Ser proactivos en la detección de riesgos (detectar los riesgos antes de que ocurran)
- Se obtiene mejores fundamentos para la toma de decisiones y asignación de presupuesto para controlar las diversas clases de riesgo (financiero, operativo, seguros, reputación, entre otros.

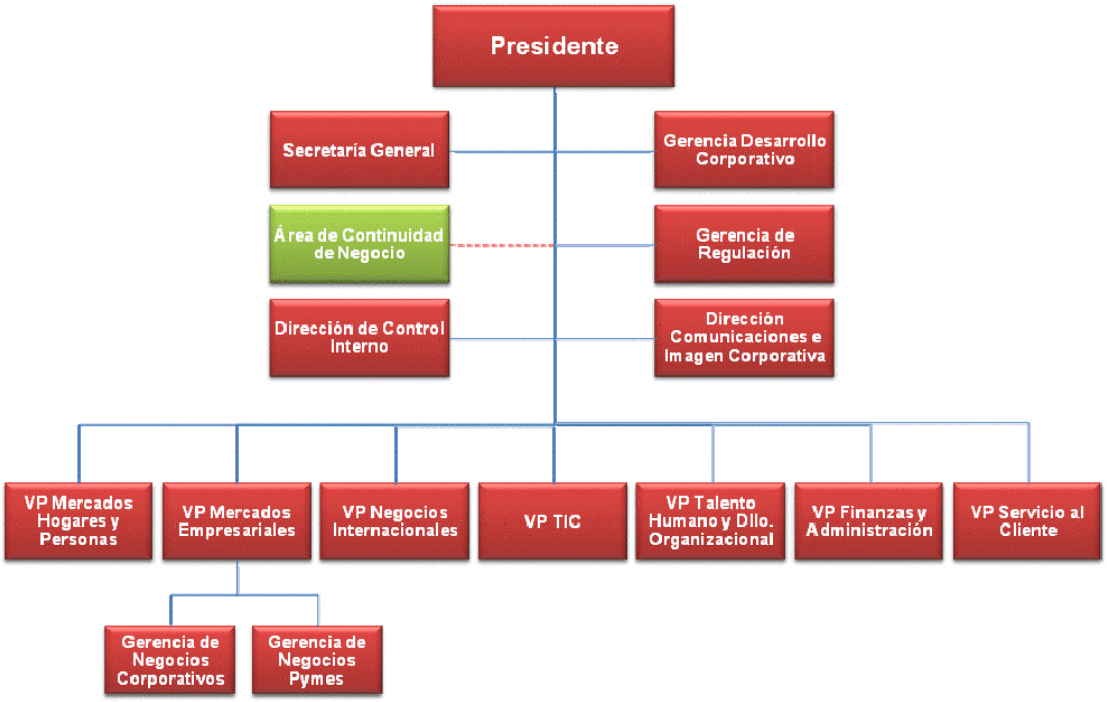
Desventajas

- La gestión de continuidad puede perder independencia y autonomía, frente a diversas evaluaciones de riesgos que afectan la compañía.
- Posible pérdida de liderazgo en la gestión transversal de la continuidad.
- Crea conflictos entre la importancia y la urgencia de los controles para mantener la continuidad, frente a controles de otras áreas de riesgo.

Alternativa 2: Área de continuidad reportando a la presidencia

Esta alternativa se presenta como la más recomendada por las buenas prácticas para mantener la *independencia* requerida por el proceso de gestión de la continuidad, el cual requiere que cada uno de los funcionarios de la compañía interiorice la continuidad de negocio como un factor apalancador de la estrategia de negocio y permitirá fortalecer la prestación de servicios de la compañía a sus clientes. La estructura sería la siguiente:

Figura 21. Estructura reportando a la presidencia



Ventajas

- Independencia de otras áreas de control.
- Independencia para gestionar la elaboración de planes de respuesta a cualquier área.
- Visión global (holística) de la compañía.

- Reporte y patrocinio directo del comité de presidencia y la presidencia.
- Interrelación de primera mano para conocer, apoyar y generar valor a las estrategias de negocio.
- Obtención de recursos para definir estrategias y controles adecuados a la organización, sin generar conflictos en su importancia.

Desventajas

- Diferencias, oposición o discrepancia entre áreas comunes de riesgos
- Trabajo aislado o duplicado de las actividades de procesos de continuidad, principalmente en evaluación de riesgos.
- Información fragmentada de riesgos de la compañía.

REQUERIMIENTOS DE LA ESTRATEGIA: SISTEMA DE GESTIÓN DE CONTINUIDAD DE NEGOCIO [SGCN]

Para la implementación de esta estrategia en cualquiera de sus alternativas es requerido que UNE defina los siguientes aspectos:

- Definir y publicar las políticas necesarias para administrar la continuidad de UNE, con el patrocinio de la Alta Gerencia.
- Incluir la estructura de continuidad dentro de la estructura organizacional actual.
- Implementar de acuerdo al sistema de gestión integral de procesos de UNE, los procesos requeridos para gestionar la continuidad de negocio en un ciclo de mejoramiento continuo del PHVA.
- Seleccionar las personas responsables de administrar y mantener una mejora continúa del Sistema de Gestión de Continuidad Negocio (SGCN).

- Asignar un presupuesto de operación al Sistema de Gestión de Continuidad, que permita ejecutar las tareas pertinentes para mantener la continuidad e incrementar el nivel de cultura en continuidad de negocio dentro de UNE.

ROLES Y RESPONSABILIDADES PARA EL SISTEMA DE GESTIÓN DE CONTINUIDAD SGCN

Dadas las definiciones de las alternativas por parte de UNE, se debe proceder con la identificación de los participantes y dueños del sistema. Independientemente de la alternativa de estructura elegida por UNE, el equipo de continuidad es el encargado de definir las políticas de continuidad en todos sus aspectos (procesos, personas, tecnología e infraestructura física), participar en las definiciones de estrategias de continuidad a ser incorporadas en UNE, advertir sobre riesgos que afectan la continuidad y motivar acciones de control que disminuyan el impacto de interrupciones, además de asesorar en los temas de continuidad.

Este equipo, según las características de UNE y los procesos del SGCN, podrá estar conformado por un líder de continuidad de negocio y de tres a seis analistas de continuidad, con fortalezas en los diferentes temas y dimensiones de continuidad (riesgos, impactos, procesos, cultura, tecnología, infraestructura física, proveedores); sin embargo, en la implementación del sistema de gestión de continuidad se determinará el número más adecuando de personas. Los roles se describen a continuación:

Líder del sistema de continuidad de negocio (LSCN)

El Líder del Sistema Continuidad es el encargado de dirigir y liderar todas las actividades relacionadas con el Sistema de Gestión de Continuidad de Negocio (SGCN).

Perfil: el líder del sistema de continuidad de negocios debe contar con experiencia certificada en temas de continuidad de negocio y debe tener conocimientos detallados de la metodología para gestión de continuidad de negocio implementada en UNE. El rol requiere de habilidades administrativas y técnicas, comunicación intensa e información precisa sobre todos los aspectos de continuidad implementados en UNE, contar con la visión integral del negocio y liderazgo en cada uno de los niveles de la organización. **Responsabilidades:**

- Planear las actividades periódicas ejecutadas por el proceso.
- Velar por la definición y aplicación de las políticas de continuidad de negocio de UNE.
- Servir de guía metodológica a los líderes de los procesos, cuando estos quieran actualizar, mantener, mejorar, probar y auditar el plan de recuperación de cada proceso.
- Coordinar la actualización y mantenimiento del SGCN.
- Liderar el presupuesto y aprobación de inversiones requeridas para establecer y mantener las estrategias del SGCN.
- Ejecutar las tareas de administración de los recursos (tiempo, personas, equipos, oficinas, sedes, y suministros) y la logística del SGCN.
- Direccionar la planificación y control del SGCN.
- Realizar seguimiento a los indicadores de gestión de los planes del SGCN.
- Mantener el compromiso y participación del equipo de trabajo.
- Delegar de manera expresa en los líderes de los procesos la responsabilidad de actualizar, mantener y probar el Plan de Continuidad.
- Propender por mantener actualizado y vigente el Plan de Continuidad.
- Advertir sobre nuevos riesgos que afectan la continuidad de la operación normal de UNE y que ponen al descubierto debilidades del Plan de Continuidad.

Analistas del sistema de continuidad de negocio (ASCN)

Los analistas del sistema de continuidad serán responsables por la coordinación y ejecución de las actividades relacionadas con el sistema de gestión de continuidad de negocio.

Perfil: los analistas del sistema de continuidad de negocios deben tener conocimientos detallados de la metodología implementada para la gestión de continuidad de negocio en UNE, ser líderes en ejecución de actividades, tener conocimiento del funcionamiento de los procesos, la tecnología, los productos y servicios entregados por UNE.

Responsabilidades

- Alinear y orientar a los dueños de los procesos para alcanzar los resultados de continuidad proyectados y finalizar adecuadamente las actividades definidas en la planeación.
- Ejecutar, en trabajo de campo las actividades específicas definidas en el plan de trabajo, diseñado por el líder de continuidad, con su asesoría y liderazgo.
- Diseñar, coordinar las pruebas de continuidad y monitorear los planes de continuidad.
- Motivar la actualización permanentemente de los planes de continuidad, debido a que estos son dinámicos y se deben alinear continuamente con los cambios presentados dentro de la organización.
- Capacitar y liderar campañas de sensibilización constantes que se dirijan al personal, tanto interno como externo, para asegurar el entendimiento de la relevancia de las prácticas de continuidad y reforzar la habilidad de uso de los planes definidos.
- Acompañar a los dueños de los procesos en la Identificación y desarrollo de las estrategias de continuidad.

VENTAJAS DE LA IMPLEMENTACIÓN DEL SGCN

Las ventajas que se destacan en la implementación del Sistema de Gestión de Continuidad son las siguientes:

- Ayuda a la organización a establecer estrategias para mantener la continuidad, según los requerimientos del mercado.
- El sistema se convierte en un diferenciador de mercado, la compañía estará preparada para superar importantes interrupciones.
- Mantenerse en cumplimiento de las diferentes leyes y exigencias de los entes reguladores.
- Ayuda a UNE a convertirse en un proveedor estratégico.
- Apalanca las estrategias para establecer una cultura de continuidad de negocio dentro de UNE.
- Permite mantener actualizados los planes de respuesta (continuidad, contingencia, crisis, emergencias) de UNE.
- Mayor confianza en las actividades de cumplimiento como resultado del seguimiento y la actualización continúa de los planes de respuesta.
- Soporta la estrategia organizacional al apoyar el cumplimiento de la MEGA de la compañía, ya que disminuye la afectación por interrupciones disminuyendo el impacto financiero.
- Mejoramiento en la toma de decisiones debido a mayor disponibilidad de información.
- Mayor flexibilidad frente a los cambios del entorno.

ASPECTOS A CONSIDERAR

Los siguientes ítems son fundamentales para la implementación del Sistema de Gestión de Continuidad de Negocio:

- Se requiere de personas con una asignación de tiempo completo, que velen por el cumplimiento y mantenimiento del sistema.
- Se puede ver afectada la estructura organizacional actual.

El sistema requiere de un presupuesto para ejecutar las actividades de entrenamiento, sensibilización y mantener actualizado los planes de respuesta.

3.1.2 estrategia 2: establecer la estructura para el manejo de crisis del plan de continuidad de negocio – BCP. La estructura para el manejo de crisis del Plan de Continuidad busca definir los equipos y el personal responsable por ejecutar las actividades de administración de crisis, recuperación y contingencias de tecnología y negocio. Se debe asegurar que todos los participantes asignados tienen el perfil adecuado para ejecutar las actividades asignadas.

La estructura contiene los siguientes equipos:

- Comité Gerencial de Continuidad – Nivel Estratégico.
- Comité de Administración de Crisis – Nivel Táctico.
- Equipos de Recuperación – Nivel Operativo.

EQUIPOS DEL PLAN DE CONTINUIDAD

A) COMITÉ DE PRESIDENCIA

El Comité de Presidencia es el nivel estratégico del plan y está encargado de tomar las decisiones frente al manejo de situaciones de crisis que al presentarse interrumpan las operaciones normales de la compañía. Igualmente, valida y aprueba las estrategias planteadas para afrontar este tipo de situaciones.

En el momento de declaración de contingencia velará por el cumplimiento del plan, la salvaguarda de la vida y activos de la compañía, además solicitará los informes del manejo del evento al Comité de Administración de Crisis. Este comité está conformado por:

- Presidente.
- Vicepresidente Servicio al Cliente.
- Vicepresidente Finanzas y Administración.
- Vicepresidente Talento Humano y Desarrollo Organizacional.
- Vicepresidente Tecnologías de Información y Comunicaciones.
- Vicepresidente Mercados Empresariales.
- Vicepresidente Mercados Hogares y Personas.
- Vicepresidente Negocios Internacionales.
- Gerente de Desarrollo Corporativo.
- Secretario General.
- Director de Control Interno.

B) COMITÉ DE ADMINISTRACIÓN DE CRISIS (CAC)

Es el encargado del nivel táctico del plan, es quien realiza la evaluación inicial de los eventos de interrupción o crisis que se presenten y que afectan la operación normal de la compañía. Además, velará por actualizar y probar el Plan de Continuidad en cada una de sus componentes, además de capacitar al personal que hace parte del plan. Este comité está conformado por:

- Director de Continuidad.
- Director de Continuidad Alterno.
- Representante de Dirección de Control Interno.
- Representante de la Secretaría General.

- Asesor de Gestión de Seguros.
- Coordinador de Recuperación de Negocio Administrativo (CRNA).
- Coordinador de Recuperación de Negocio Cliente (CRNC).
- Coordinador de Recuperación de Tecnología (CRT).
- Coordinador de Comunicaciones en Crisis.
- Jefe de Emergencias.

C) EQUIPOS DE RECUPERACIÓN

Estos equipos componen el nivel operativo del plan de continuidad, están encargados de la ejecución de los procedimientos y actividades necesarias para salvaguardar la vida de las personas, los activos de la compañía y recuperar las operaciones de los procesos críticos del negocio, administrativo y de la tecnología.

Además, deben colaborar con el Comité de Administración de Crisis (CAC) para mantener actualizado y probado el Plan de Continuidad. Estos equipos se conforman así:

Equipo de Recuperación de Negocio Administrativo

- Coordinador de Recuperación de Negocio Administrativo.
- Líder Facturación y Recaudo.
- Líder Gestión Financiera Y Contable.
- Líder Administrativo.
- Líder Talento Humano.

Equipo de Recuperación de Negocio Cliente

- Coordinador de Recuperación de Negocio Cliente.
- Líder de Manejo de órdenes.

- Líder de Aprovisionar soluciones.
- Líder de Atender clientes.
- Manejo de Incidentes.

Equipo de Recuperación de Tecnología

- Líder de Operar y mantener la infraestructura TIC- Agregación y Backbone.
- Líder de Operar y mantener la infraestructura TIC- IDC.
- Líder de Operar y mantener la infraestructura TIC- Equipos auxiliares.
- Líder de Operar y mantener la infraestructura TIC- Servicios de voz.
- Líder NOC.

Equipo de Comunicaciones

- Coordinador de Comunicaciones en Crisis.
- Líder de Comunicación con Empleados y sus Familias.
- Líder de Comunicación con Clientes, Proveedores y Prensa.
- Líder de Comunicación con Junta Directiva.
- Líder de Comunicación entes de control.

Equipo de Manejo de Emergencias

- Jefe de Emergencias.
- Comandante Operativo en el Sitio.
- Brigada de emergencias.
- Líder de Seguridad Física.

ROLES Y RESPONSABILIDADES

A continuación se describen los roles y responsabilidades de los integrantes de los equipos del Plan de Continuidad, las personas nombradas como principales y sus suplentes (alternos) quienes tienen las mismas responsabilidades.

Director de Continuidad para el Manejo de Crisis

El Director de Continuidad para el manejo de crisis es el encargado de dirigir y liderar todas las actividades relacionadas con el diagnóstico y evaluación del incidente que provoca la crisis, activación, operación en contingencia, retorno a la normalidad (restauración) pruebas y capacitación del Plan de Continuidad.

Es el responsable de declarar la contingencia con base a las decisiones tomadas por el Comité de Gerencia o en su defecto por el comité Administración de Crisis (CAC). Igualmente podrá declarar la contingencia en situaciones donde amerite realizar su activación inmediata. Esta persona debe ser líder, tener poder de convocatoria, mantener la tranquilidad en caso de eventos de crisis y tener una visión amplia y clara del negocio, debe ser una persona de carácter directivo.

Responsabilidades:

- Coordinar la actualización, distribución, documentación y mantenimiento del Plan de Continuidad.
- Establecer los objetivos de recuperación y activar el Plan de Continuidad bajo el escenario resultado de la evaluación de la interrupción.
- Delegar de manera expresa en el Comité de Administración de Crisis (CAC), la responsabilidad de actualizar, mantener y probar el Plan de Continuidad.
- Liderar la aprobación de inversiones requeridas para establecer y mantener la estrategia de recuperación y contingencia de la compañía.

- Liderar las reuniones del Comité de Administración de Crisis (CAC), para diagnosticar y evaluar las interrupciones que están afectando la prestación del servicio.
- Advertir sobre nuevos riesgos que afectan la continuidad de la operación normal de la compañía y que ponen al descubierto debilidades del Plan de Continuidad.
- Propender por mantener actualizado y vigente el Plan de Continuidad.
- Monitorear los reportes sobre el estado de recuperación o evaluación.
- Velar por la ejecución del debido análisis causa – raíz del evento.
- Realizar las recomendaciones requeridas al plan.

Director Alterno de Continuidad

- Asumir el rol y cumplir con las responsabilidades de Director de Continuidad cuando este no se encuentre disponible.
- Asistir a las reuniones del Comité de Administración de Crisis (CAC).
- Realizar las actividades asignadas por el Director de Continuidad.

Asesor Control Interno

La persona de control interno tiene la responsabilidad de reportar riesgos que puedan afectar a la compañía

Responsabilidades:

- Asistir a las reuniones del Comité de Administración de Crisis (CAC).
- Advertir sobre riesgos que puedan afectar la continuidad en la prestación del servicio o la funcionalidad del plan.
- Acompañar a los participantes del plan durante la declaración de contingencia, para hacer más efectivas las actividades de su área.

- Facilitar la operación contingente, entendiendo que se trata de una situación especial.
- Advertir sobre la ausencia de controles en la operación en contingencia

Asesor Secretaria General

El Representante de la Secretaría General es el encargado de brindar asesoría jurídica en el momento de la crisis, principalmente en el manejo de relaciones con los clientes, terceros y organismos del Estado. Su labor se centrará en facilitar la operación contingente, atenderá de manera prioritaria todos los requerimientos que el comité de administración de crisis requiera para facilitar su operación.

Responsabilidades:

- Asistir a las reuniones del Comité de Administración de Crisis (CAC).
- Mantener informado al Comité de Administración de Crisis (CAC) sobre posibles demandas, acciones populares, otros requerimientos de los entes de control, accionistas, prensa o ciudadanía en general, por la declaratoria de contingencia.
- Atender de manera inmediata los requerimientos realizados por el comité de crisis, relacionados con la activación, operación y retorno de una contingencia.
- Advertir sobre riesgos de tipo jurídico que puedan afectar la continuidad en la prestación del servicio o la funcionalidad del plan.
- Acompañar a los participantes del plan durante la declaración de contingencia, para hacer más efectivas las actividades de su área.
- Brindar asesoría jurídica en la crisis.

Coordinadores de Recuperación

Los coordinadores de recuperación son personas encargadas de liderar la recuperación de procesos de negocio, tecnología soporte, comunicación y edificios, basados en las estrategias de continuidad implementadas. Serán el contacto directo entre los procesos de negocio, el área tecnológica y el Comité de Administración de Crisis; además, colaboran con las decisiones tomadas por el director de continuidad durante la declaración y activación de la contingencia.

Responsabilidades:

- Asistir a las reuniones del Comité de Administración de Crisis (CAC).
- Liderar las reuniones del Equipo de Recuperación, para diagnosticar y evaluar las interrupciones que están afectando la prestación del servicio.
- Velar por la actualización del Plan de Continuidad en los casos que se presenten situaciones como: modificaciones en la operación, cambio en la estructura, roles y responsabilidades, cambios en la infraestructura tecnológica, disponibilidad de los recursos, entre otros.
- Identificar los posibles riesgos que afectan la continuidad de la operación normal de la compañía y que ponen al descubierto debilidades del Plan de Continuidad.
- Mantener comunicación constante entre Coordinadores de Recuperación durante el estado de contingencia.
- Liderar la puesta en el funcionamiento de los servicios en los centros alternos de procesamiento y operación.
- Verificar que el área física destinada como centro alterno cumpla con los requerimientos mínimos para el normal funcionamiento, al controlar confirmar las condiciones de control ambiental, acceso y administración.
- Colaborar en la comunicación a los proveedores y clientes directos de negocio, sobre el estado de contingencia en que se encuentra la compañía,

esto previa decisión y autorización del Comité Gerencial de Continuidad y el Director de Continuidad, mediante comunicado elaborado por el área de comunicaciones.

- Entregar los reportes correspondientes al Comité de Administración de Crisis (CAC) sobre el estado de la recuperación de sus áreas.
- Velar por la realización de actividades de entrenamiento al personal involucrado en el plan.
- Velar por la realización de las pruebas del Plan de Continuidad y revisar los resultados obtenidos en la misma.
- Verificar que las actividades de ajuste sobre el plan, resultado de las pruebas, hayan sido ejecutadas e implementadas.
- Velar por la actualización del plan, y distribución a cada uno de los involucrados.
- Liderar los procedimientos de restauración a la normalidad con el apoyo del Equipo de Recuperación.

Líderes Recuperación

Son encargados de coordinar equipos específicos de recuperación a nivel de procesos administrativos, procesos de cara al cliente y tecnología, deben velar por la ejecución de procedimientos tendientes a mantener o recuperar las operaciones normales de la compañía. En caso de ser requeridos deben participar del Comité de Administración de Crisis.

Responsabilidades:

- Identificar y diagnosticar las interrupciones de los servicios.
- Velar por la disponibilidad de los recursos mínimos básicos.
- Velar por la disponibilidad de los formatos y archivos necesarios para operar.

- Recibir la notificación del Coordinador de Recuperación y entregar un reporte sobre el estado de la situación de contingencia.
- Definir el personal mínimo que debe operar bajo los diferentes estados de contingencia según los planes de recuperación.
- Reportar al Coordinador de Recuperación observaciones, inquietudes y sugerencias de cualquier evento que se presente en ambiente de contingencia.
- Liderar las actividades contingentes para cada proceso de los diferentes planes.
- Programar y liderar las pruebas a los diferentes componentes del plan de continuidad a su cargo.
- Identificar los riesgos potenciales en los componentes del plan de continuidad que pueden afectar la efectividad en su ejecución.

Estructura Coordinador de Comunicaciones

La coordinación de la comunicación en crisis se debe realizar de manera permanente durante toda las fases de la contingencia, para esta se deben definir unos canales de comunicación con el fin de divulgar de manera efectiva a los interesados, quienes pueden ser los empleados y Familias, Clientes y Proveedores, Entes de control y integrantes de la junta directiva.

Las comunicaciones buscan demostrar que la compañía está manejando la crisis de manera apropiada

Responsabilidades:

- Asistir a las reuniones del Comité de Administración de Crisis (CAC).
- Buscar la aprobación del comité de crisis antes de autorizar cualquier comunicado.

- Crear y mantener actualizado el plan de comunicaciones en crisis, así mismo los diferentes comunicados prediseñados.
- El Coordinador de comunicaciones en crisis consulta los diferentes informes del evento de interrupción. Utiliza los reportes generados por cada uno de los equipos de recuperación.
- El Coordinador de comunicaciones en crisis consulta el manual de comunicaciones y dependiendo de los afectados por el evento designa la elaboración del comunicado (empleados y Familias, Clientes y Proveedores, Entes de control y integrantes de la junta directiva)

ESTRUCTURA PLAN DE MANEJO DE EMERGENCIAS

Los roles del Jefe de Emergencias y el Comandante Operativo en el Sitio, hacen parte del Plan de Manejo de Emergencias de la compañía, sin embargo a continuación, se realiza una breve descripción de la responsabilidad y la interacción con el Plan de Continuidad de Negocio. Para una mayor descripción de los roles y responsabilidades remitirse a los Planes de Manejo de Emergencias de la empresa.

Adicionalmente a los roles considerados en los Planes de Emergencias de la compañía, se describe un nuevo rol que no se menciona en dichos documentos, el de Líder de Seguridad Física. Además, se explica el rol de la Brigada de Emergencias, el cual, se menciona pero no se describe, en los respectivos planes de manejo de emergencias. Para ampliación de las responsabilidades remitirse al Plan de Manejo de Emergencias de la compañía.

Jefe de Emergencias

Es el máximo responsable de dirigir las acciones de respuesta en situaciones de emergencias en la empresa y de coordinar los requerimientos entre el sitio del siniestro y la estructura corporativa de crisis.

El Jefe de Emergencias es el Director de UNE EPM Telecomunicaciones, pero se establecen delegaciones, de acuerdo a la disponibilidad y a la gravedad de la emergencia, según la sede afectada.

Comandante Operativo en el Sitio (Coordinador Operativo en el Sitio)

Es la "persona a cargo" de las acciones de control del siniestro en la sede, responsable de implantar las decisiones tomadas por el Jefe de Emergencias, así como de supervisar la ejecución de dichas acciones y alcanzar los objetivos propuestos en el Plan de Emergencia de la instalación.

Durante la fase de control de un siniestro, el funcionario encargado de actuar como Coordinador Operativo en el Sitio dependerá de la disponibilidad y a la gravedad de la emergencia.

BRIGADA DE EMERGENCIA

- Revisión diaria de salidas de emergencia y del personal de su área
- Responder primero que las demás personas
- Agilizar y organizar proceso de salida
- Verificar que nadie quede en su área cuando se dé la orden de evacuación.
- Realizar verificación en puntos de encuentro.
- Conocer las instalaciones y los riesgos que puedan generar emergencias, realizando un mapa de riesgos físicos que entrega al jefe de edificio.

- Tener conocimiento de los equipos con que cuenta la empresa para atender una emergencia, su ubicación y estado.
- Realizar seguimiento permanente a las condiciones de riesgo de la empresa.
- Hacer inspección periódica a sistemas de extinción, recursos para primeros auxilios y demás elementos con que cuente la empresa para una emergencia.

Líder de Seguridad Física

Es una persona del proceso de Adecuación y Mantenimiento de Instalaciones, su función es mantener y facilitar las condiciones de seguridad necesarias para las personas, instalaciones y bienes. Dentro de sus funciones específicas se cuenta:

- Controlar periódicamente el buen estado y funcionamiento de los elementos de detección alarmas y control de incendios, extintores, señalización, vías de evacuación e iluminación.
- Su coordinación con los brigadistas y jefe de edificio, permitirá la salida segura de las personas que habitan el edifico en el momento de una evacuación.
- Entregar el mando de la operación de seguridad física a las entidades del estado entrenadas para tal fin, en el momento de la crisis.

Este rol debe ser asumido por una persona por cada una de las sedes incluidas en este Plan de Continuidad.

LÍNEA DE SUCESIÓN EN EL MANEJO DE CRISIS

La línea de sucesión identifica los responsables asignados a los diferentes roles de los participantes en la estructura de los diferente planes de continuidad y sus alternos en caso de que estos no puedan asumir las actividades y/o tareas. Estas personas deben ser asignadas de acuerdo a los roles y responsabilidades definidas para este plan.

3.1.3 Estrategia 3: fortalecimiento de acuerdos de niveles de servicio. La dependencia de proveedores externos manifestada en el diagnóstico de continuidad requiere que la organización fortalezca la definición y sobre todo la administración de los acuerdos de nivel de servicio (ANS) dentro su proceso normal de contratación, para lo cual se deberá exigir en los contratos con proveedores, la inclusión de cláusulas que permita gestionar la continuidad de negocio en todo el servicio.

Los proveedores actuales o los que se incorporen a la organización, que soporten funciones críticas del negocio, deben asegurarle al respectivo dueño de proceso y/o área responsable de la contratación, la implementación de las políticas del Modelo de Gestión de Continuidad del Negocio antes de la formalización y/o prórroga de los respectivos contratos y acuerdos de servicio; con el fin de garantizar que dichos servicios no se verán interrumpidos ante eventos de desastre o interrupciones mayores. Tanto los proveedores actuales como los próximos a contratar, deben facilitar la evaluación y auditoria periódica en el momento de su vinculación o prórroga de sus contratos.

La siguiente cláusula debe ser revisada por el área jurídica de la compañía, y dependerá del servicio contratado entre las partes:

Cláusula de Continuidad: *El Proveedor manifiesta que tiene cubierto mediante planes de respuesta a incidentes, la continuidad de los servicios prestados a la Compañía en los tiempos y mediante las condiciones establecidas en el contrato. Estos planes de respuesta cuentan con el personal idóneo y necesario para atender cualquier evento, incidente o situación que perturbe la operación normal de la Compañía*

Reporte de Incidentes: *El Proveedor se obliga a informar oportunamente a la Compañía, cualquier incidente de en la operación que se presente sobre los*

productos / servicios, recursos tecnológicos o sus instalaciones y que, como consecuencia, pueda generar alteraciones de funcionamiento en la prestación de sus servicios a la Compañía.

Auditoría: *La Compañía se reserva el derecho de verificar cuando lo considere oportuno, directamente o por intermedio de otra persona que señale libremente, el cumplimiento de las disposiciones legales, reglamentarias y convencionales, de carácter administrativo, comercial y técnico por parte del Proveedor, así como la calidad comercial y técnica de los servicios prestados por el Proveedor y en particular, su ejecución a los parámetros de desempeño indicados por la Compañía. Al respecto, la Compañía podrá inspeccionar los trabajos, las instalaciones, equipos, registros e inventarios del Proveedor y solicitarle informes, que deberán ser presentados por éste en el lapso que le señale para el efecto. Los costos que se ocasionen por la inspección que lleve a cabo la Compañía, en ejercicio de la facultad acá consagrada, serán asumidos, íntegramente por la Compañía."*

Esta estrategia busca fortalecer los acuerdos de nivel de servicio con aquellos proveedores (socios estratégicos) con los cuales se tiene dependencia, y cuyo bien o servicio hace parte de los insumos de los procesos críticos.

El contenido de los Acuerdos de Nivel de Servicio debe ser claro, al tener acceso al acuerdo el lector "siempre" deberá poder contestar las siguientes preguntas:

Figura 22. Nivel de servicio

La definición de los ANS debe considerar la madurez del servicio que se está contratando, por lo tanto se debe conocer en qué estado se encuentra con el fin de saber las condiciones bajo las cuales se negociará. Cuando se va a definir un ANS la persona responsable de proveer el servicio debe evaluar los niveles de servicio que puede cumplir antes de comprometerlos de acuerdo que refleje la capacidad de entrega de servicio, el cual permita tener expectativas ajustadas a la realidad.

El éxito en la implantación, administración y ejecución de un ciclo de Acuerdos de Niveles de Servicio (ANS), depende de la puesta en marcha de cinco pasos metódicos que deben realizar cliente y proveedor con el objeto de satisfacer las expectativas de todas las partes interesadas y a su vez permitan generar una dinámica de mejoramiento, comunicación y trabajo en equipo.

Figura 23. Pasos metodicos que deben ser realizados por cliente / proveedor

REQUERIMIENTOS PARA FORMALIZAR ANS

Dentro de los principales requerimientos para formalizar los acuerdos de nivel de servicio se encuentra:

- Definir claramente las métricas y los criterios de evaluación del servicio.
- Verificar el objetivo de nivel de servicio requerido antes de ser firmado el acuerdo.
- Establecer el enfoque, los recursos y los tiempos del servicio a ser contratado.
- Definir los entregables del servicio (no el proceso), y especificar los ítems que no hacen parte del servicio.
- Definir los límites claramente.
- Se debe medir la disponibilidad, los tiempos de respuesta, la confiabilidad, la satisfacción de los usuarios, entre otras.
- La medición del servicio debe reflejar los requerimientos iníciales.
- Cargos de la prestación del servicio o penalidades por incumplimiento.

VENTAJAS DE ESTABLECER ANS

- Los ANS establecen la base y el ambiente que facilita la prestación de un servicio de excelente calidad a los clientes, razón fundamental del negocio.
- Negociar niveles de servicio bajo premisas de gana-gana entre las partes teniendo en cuenta el respeto mutuo permite prever una mejor negociación del ANS.
- Mejorar la satisfacción de los usuarios y clientes en la entrega de los servicios.
- Monitorear y controlar los servicios para identificar las áreas débiles y proponer acciones de mejora.

ASPECTOS A CONSIDERAR EN LA DEFINICIÓN DE ANS

- Se puede presentar mala definición basadas sobre deseo de servicio y no sobre objetivos alcanzables.
- Los costos de acuerdos de servicio se pueden tornar como gastos recurrentes y no como cargos de servicio, por incumplimiento del ANS.

COSTOS

- Costos de personal (salarios, entrenamiento y consultoría si es requerido).
- Herramientas soporte para la administración de los acuerdos, aplicativos.
- Posible adquisición de hardware y software (PCs, software de oficina, almacenamiento).

3.2 LISTA DE CHEQUEO PARA REALIZAR EL DIAGNÓSTICO DE PREPARACIÓN PARA LA CONTINUIDAD DE NEGOCIO

El diagnóstico proporciona la evaluación de la situación actual en que se encuentra UNE para responder ante una interrupción que pueda afectar la continuidad de la operación, esta evaluación se soporta en las siguientes actividades realizadas:

- Mapeo de Interdependencias: en el cual se identifica los componentes que intervienen en la cadena del servicio de la operación de UNE.
- Evaluación de Riesgos (RA): en la cual se identifican aquellos factores que puedan afectar la continuidad del servicio, teniendo en cuenta las personas, los procesos, la infraestructura tecnológica y las instalaciones físicas.
- Análisis de Impacto: por medio del cual se conoce cómo se ve afectado o impactado UNE en caso de una interrupción de en la prestación o entrega de servicios.

Los resultados arrojados por estas actividades, son el insumo principal de la siguiente fase de definición de estrategias de continuidad que permitan mantener los niveles de servicio requeridos por la operación.

Para realizar un diagnóstico apropiado se deben tener en cuenta las consideraciones mencionadas a continuación.

DEFINICIÓN DE LAS CUATRO DIMENSIONES CONSIDERADAS DENTRO DE LA CONTINUIDAD DE NEGOCIO

- Personas: identificación de todo el personal que participa en los procesos y servicios en los cuales la compañía quiere aplicar Continuidad de Negocio.
- Procesos: selección de los procesos críticos y generadores de valor que están relacionados directamente con el negocio de la compañía (operación).
- Tecnología: identificación de los elementos de las tecnologías de la información y comunicación sobre los cuales se soportan los procesos y los servicios en los cuales se enfoca la continuidad.
- Infraestructura física: áreas, recursos y edificaciones de la compañía que son críticos en el funcionamiento de la Compañía.

MAPEO DE INTERDEPENDENCIAS

- Realizar el mapa de interdependencias de procesos.
- Realizar el mapa lógico de tecnologías.

EVALUACION DE RIESGOS

- Clasificación de riesgos según la probabilidad de ocurrencia.
- Clasificación de riesgos según el impacto.
- Clasificar el control aplicado sobre los riesgos identificados.
- Categorizar los riesgos basados en las cuatro dimensiones definidas.
- Valorar los riesgos según el apetito del mismo.

ANÁLISIS DE IMPACTOS

- Identificar procesos y público objetivo.

- Identificar los requerimientos soporte del negocio.
- Elaborar las encuestas de análisis de impacto.
- Validar la información y elaborar el reporte de resultado.

Finalmente, basados en la información obtenida en los procesos anteriores se procede a desarrollar una serie de estrategias que deben ser implementadas en la ejecución del plan de continuidad de negocio. Estas estrategias deben ser definidas según las indicaciones del modelo de continuidad escogido.

Con esta lista de chequeo se cubren los aspectos más importantes en el diagnóstico de preparación del proceso de la Continuidad de Negocio.

CONCLUSIONES

Con la nueva regulación que el gobierno ha estado implementando para las compañías prestadoras de servicios; especialmente en el mercado de las TIC, donde se exigen ciertas garantías y características de calidad en la entrega de sus productos y donde las penalizaciones por no cumplir con la promesa de venta exigen a las compañías compensar el cliente, algunas veces, hasta con grandes cantidades de dinero; se ha vuelto necesario que las compañías adquieran conciencia de la importancia de garantizar una operación continua.

UNE EPM TELECOMUNICACIONES al ser una empresa en el mercado de las TIC es en gran parte dependiente de la tecnología y por lo tanto, tiene importantes vulnerabilidades las cuales se pueden ver fácilmente amenazadas generando grandes daños, al grado de afectar fuertemente la operación y hasta dejarla fuera del mercado. Para la compañía, mantener continuidad y estabilidad en sus servicios administrando la continuidad del negocio, se debe convertir en un elemento estratégico y táctico le que permitirá mantenerse en su mejor nivel competitivo y por supuesto, mantener un crecimiento sostenible y rentable.

Un sistema de Administración de la Continuidad de Negocio debe ser asimilado y totalmente integrado en la organización como uno más entre sus procesos de gestión. Con este plan se revisan los procesos críticos de la operación en la empresa, se clasifican, se priorizan y se determina cuáles son los más sensibles y cuáles no pueden dejar de operar para que el negocio continúe su funcionamiento. Siguiendo las pautas explicadas a lo largo de este proyecto, la Alta Gerencia de la Compañía puede ejecutar un buen plan de Continuidad de negocio en los procesos críticos de la Dirección de Operaciones.

BIBLIOGRAFIA

CERULLO, Virginia; CERULLO, Michael J. Business continuity planning: a comprehensive approach. Fuente: Information Systems Management; Summer2004. Vol. 21 Issue 3. p. 70-78, 9, 3 charts, 3 graphs.

CLAS, Ellen. Business Continuity Plans. Fuente: Professional Safety, Sep2008. Vol. 53 Issue 9. p. 45-48, 4.

GPG 2008 – The BCI Good Practice Guidelines.

GROTH, Paul; DON, Rozek. Business Continuity Planning. Fuente: Health Management Technology. Mar2008. Vol. 29 Issue 3, p. 10-12, 3.

GTC 176:2009, Guia Tecnica Colombiana de Sistema de Gestión de Continuidad de Negocio.

NFPA 1600:2007, Normas de desastres. Gestión de emergencias y continuidad de negocio.

NTC *5254:2005,* Norma Técnica Colombiana de Gestión de Riesgo.

TOTTY, Patrick, Business Continuity Planning. Fuente: Credit Union Magazine; Apr2006. Vol. 72 Issue 4. p. 80-84, 3.

CIBERGRAFIA

Ministerio de Comunicación de de Colombia, Gobierno en Línea (2008), http://programa.gobiernoenlinea.gov.co/