Universidad de San Carlos de Guatemala

Facultad de Ingeniería

Escuela de Ingeniería Mecánica Eléctrica

"GUÍA PARA EL DISEÑO DE ESTRATEGIAS DE RECUPERACIÓN DE CENTRALES DE TELEFONÍA CELULAR EN EL CASO DE DESASTRES"

Eddy Augusto Medinilla Rodríguez

Asesorado por el Ing. Marlon Giovanni Rojas Cancinos

Guatemala, abril de 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

GUÍA PARA EL DISEÑO DE ESTRATEGIAS DE RECUPERACIÓN DE CENTRALES DE TELEFONÍA CELULAR EN EL CASO DE DESASTRES

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA

FACULTAD DE INGENIERÍA

POR

EDDY AUGUSTO MEDINILLA RODRÍGUEZ

ASESORADO POR EL ING. MARLON GIOVANNI ROJAS CANCINOS

AL CONFERÍRSELE EL TÍTULO DE INGENIERO ELECTRÓNICO

GUATEMALA, ABRIL DE 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia Garcia Soria
VOCAL II	Inga. Alba Maritza Guerrero de León
VOCAL III	Ing. Miguel Angel Dávila Calderón
VOCAL IV	Br. Luis Pedro Ortiz de Léon
VOCAL V	Br. José Alfredo Ortiz Herincx
SECRETARIA	Inga. Marcia Ivonne Véliz Vargas

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Jorge Mario Morales González
EXAMINADOR	Ing. Edwin Ramón Rodas Solares
EXAMINADOR	Ing. Luis Alfonso Muralles Calderón
EXAMINADOR	Ing. Julio César González Sáenz
SECRETARIO	Ing. Edgar José Aurelio Bravatti Castro

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

GUÍA PARA EL DISEÑO DE ESTRATEGIAS DE RECUPERACIÓN DE CENTRALES DE TELEFONÍA CELULAR EN EL CASO DE DESASTRES,

tema que me fuera asignado por la Dirección de la Escuela de Mecánica Eléctrica, con fecha 26 de febrero de 2010.

Eddy Augusto Medinilla Rodríguez

Guatemala, 12 de Abril del 2010

Ing. Julio César Solares Peñate
Coordinador de Electrónica
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Ingeniero Solares:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **"GUIA PARA EL DISEÑO DE ESTRATEGIAS DE RECUPERACIÓN DE CENTRALES TELEFONÍA DE CELULAR EN EL CASO DE DESASTRES"**, desarrollado por el estudiante **Eddy Augusto Medinilla Rodríguez**, ya que considero que cumple con los requisitos establecidos, por lo que el autor y mi persona somos responsables del contenido y conclusiones del mismo.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

Ing. Marlon Giovanni Rojas Cancinos
ASESOR

FACULTAD DE INGENIERIA
Escuelas de Ingeniería Civil, Ingeniería Mecánica Industrial, Ingeniería Química, Ingeniería Mecánica Eléctrica, Técnica y Regional de Post-grado de Ingeniería Sanitaria.
Ciudad Universitaria, zona 12
Guatemala, Centroamérica

Guatemala, 14 de abril de 2010

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC.

Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **"GUIA PARA EL DISEÑO DE ESTRATEGIAS DE RECUPERACIÓN DE CENTRALES DE TELEFONIA CELULAR EN EL CASO DE DESASTRES"**, desarrollado por el estudiante **Eddy Augusto Medinilla Rodríguez**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

Ing. Julio César Solares Peñate
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
DE GUATEMALA

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

REF. EIME 24. 2010.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; Eddy Augusto Medinilla Rodríguez titulado: "GUÍA PARA EL DISEÑO DE ESTRATEGIAS DE RECUPERACIÓN DE CENTRALES DE TELEFONÍA CELULAR EN EL CASO DE DESASTRES", procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA
MECANICA ELECTRICA
DE GUATEMALA

GUATEMALA, 15 DE ABRIL 2,010.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG. 125.2010

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **GUÍA PARA EL DISEÑO DE ESTRATEGIAS DE RECUPERACIÓN DE CENTRALES DE TELEFONÍA CELULAR EN EL CASO DE DESASTRES,** presentado por el estudiante universitario **Eddy Augusto Medinilla Rodríguez,** autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olympo Paiz Recinos
DECANO

Guatemala, abril de 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

/gdech

AGRADECIMIENTO

Este trabajo de graduación es la conclusión de mi etapa de estudiante de ingeniería, siendo un momento tan trascendente en mi vida, no lo puedo dejar pasar sin reconocer la ayuda y apoyo que he recibido durante toda mi vida y en este momento para poder realizar esta meta personal.

Le doy gracias a Dios, por darme muchas bendiciones y pruebas, por darme la fuerza y la oportunidad de concluir esta meta personal.

La primera gran bendición que Dios me dio fueron mis padres, quienes lucharon por darnos siempre lo mejor, muchas gracias por haber tomado la decisión de criarnos y educarnos basado en principios y valores.

A mi hermano Everest por motivarme siempre para cerrar esta etapa de mi vida. Muchas gracias por mostrarme cómo se vive la vida con alegría y optimismo, y por ayudarme cuando siempre lo necesito.

Encontrar a la persona indicada para compartir la vida y envejecer juntos es una enorme bendición que Dios me dio hace 20 años. Ladish, tu motivación y ayuda hizo que este trabajo de graduación fuera una experiencia mucho más fácil y satisfactoria.

La mayor bendición de todas es que Dios me haya permitido ser padre, de crear vida y dejar un legado a través de mis hijas; Krushy y Nicky muchas gracias por hacerme sentir orgulloso de ser su papi y recordarme la ilusión de ser joven al compartirme sus sueños.

Poder vivir una vida familiar ha sido una bendición de Dios donde aprendí el valor de de recibir apoyo y cariño en los momentos difíciles o compartir la dicha de los momentos felices, gracias a hermanos, a mis suegros, mis cuñadas, y cuñados, sobrinas y sobrinos por compartir conmigo este momento.

También le agradezco a Dios el que me haya permitido encontrar personas que me han acompañado en el camino de mi vida, a mis amigos de la Universidad, con quienes compartí desvelos y la ilusión de cumplir con esta meta, a mis hermanos de la comunidad con quienes he aprendido a compartir lo que soy y lo que siento, a mis amigos del trabajo con quienes he compartido el afán diario y en ese camino hemos conseguido crecer juntos y forjar una gran amistad.

Le agradezco a mi asesor el Ing. Marlon Rojas, por su tiempo y dedicación para la elaboración de este trabajo de graduación.

Le agradezco especialmente al Ing. Giovanni Salazar, por compartir todas esas horas de estudio durante los primeros años de la carrera y a Johanna Pérez de Ortiz, por la ayuda en la realización de este trabajo.

DEDICATORIA

Graduarme de Ingeniero Electrónico es la conclusión de una importante etapa como estudiante, siendo un momento tan trascendente, quiero reconocer el apoyo y la ayuda que he recibido para realizar esta meta a través de la dedicatoria de este trabajo de graduación.

Como cristiano católico le dedico a Dios este trabajo por estar siempre presente en mi vida, por cuidarme y mostrarme que buscar "Ser" es el camino para la felicidad en esta vida y preparación para la vida eterna.

A mis padres quienes se esforzaron porque sus hijos tuviéramos las oportunidades que ellos no tuvieron, mi Padre que nos mostró a sus hijos el valor del esfuerzo y el trabajo bien hecho, mi madre que con su sacrificio diario para que siempre tuviéramos lo necesario nos mostró el valor del amor abnegado para los hijos.

A mi esposa Ladishbá por acompañarme en el camino de la vida, por hacerme sentir amado durante este trayecto, por apoyarme a buscar mis sueños y mis metas y por siempre buscar ser la mejor madre para nuestras hijas.

A mis hijas, Krushy y Nicky, en mi vida siempre han sido una motivación para ser mejor y enseñarles con el ejemplo. El que formen parte de mi vida es fuente de las mayores alegrías y fuerza para seguir creciendo.

A mis hermanos, Ericka, Everest, Gisela y Eljaerk, por contar con la solidaridad y ayuda de nuestra vida en familia.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

GLOSARIO

APG	Grupo de procesadores adjuntos
ATM	Una tecnología de conmutación y multiplexación denominada Modo de Transferencia Asíncrona, con características de alta velocidad para transmisión de información a través de área local. ATM divide la información en celdas de tamaño fijo, capaces de transmitir diferentes tipos de tráfico simultáneamente, incluyendo voz, video y datos.
AUC	Centro de autentificación verifica la identidad de cada tarjeta SIM que intenta conectarse a la red GSM
BC	Continuidad del negocio
BCM	Administración de la continuidad del negocio
BCMS	Sistema de gestión de la continuidad del negocio
BCP	Planeación de la continuidad del negocio
BHCA	Intentos de llamada en la hora pico
BIA	Análisis de impacto del negocio
BSC	Controlador de estación base
BSI	Instituto Británico de Normas

BSS	Subsistema de estación base
BTS	Estación transceptor base
Buffer	Cola o espera
BVC	Canal de voz hacia atrás
CCD	Dispositivo de conferencia telefónica
CP	Procesador central
Desastre	Un evento súbito no planificado, que ocasiona un gran daño o pérdida
DR	Recuperación de desastres
DTMF	Tonos multifrecuencia
EIR	El registro de identidad del equipo guarda la lista de las estaciones móviles que están prohibidas para operar en la red GSM
Ethernet	El protocolo de capa dos de mayor uso en las redes LAN
FVC	Canal de voz hacia adelante
GARP	Aplicación genérica de los recursos del procesador

Gateway	Una combinación de hardware y software que interconecta redes o dispositivos de red que son incompatibles
GCP	Protocolo de control de Gateway
GEM	Tablero genérico
GESB	Tarjeta de conmutación de gigabit ethernet
GoS	Grado de servicio
GPG	Guía de buenas prácticas
GS	Grupo de conmutación
GSM	Sistema global para comunicación móvil
Handover	Traspaso de llamadas entre MSCs
HLR	Registro de localización base
Hot site	Lugar alternativo
HSL	Enlace de alta velocidad
Hub	Elemento central de una red con topología de estrella. Típicamente usado en las primeras redes Ethernet y Token Ring.

IP	Protocolo de internet, opera en la capa tres del modelo OSI, es usado en el conjunto de protocolos TCP/IP los cuales operan en Internet y la mayoría de redes privadas.
IPN	Red de plataformas interconectadas
ISDN	Red digital de servicios integrados
ISO	Organización Internacional de Normas
IT	Tecnología de la información
LAN	Red que interconecta todos los dispositivos que están en una localidad.
ME	Equipo terminal
MGW	Nodo independiente de medios
MMS	Servidor de multimedia
MS	Estación móvil
MSC	Central de telefonía móvil
NSS	Subsistema de conmutación de red
Off-site	Afuera del sitio de trabajo
On-site	En el sitio de trabajo

PAS	Especificación pública aceptada
PLMN	Red móvil pública terrestre
PSTN	Red pública de telefonía conmutada
RAN	Red de acceso por radio
RCC	Canal de control inverso
RNC	Controlador de la red de radio
Roamming	Recepción de llamada en otro país
RPG	Grupo regional de procesadores
RTO	Tiempo objetivo de recuperación
SCP	Punto de control de señalización
SIM	Módulo de identificación del abonado
SLI	Interfase de SIGTRAN del enlace
SMS	Mensaje de texto
ST	Terminales de señalización
STEB	Tablero mejorado de terminal de señalización
STP	Punto de transferencia de señalización

TDM	Acceso múltiple por división del tiempo
VLR	Registro de localización del visitante
WAP	Protocolo de aplicaciones inalámbricas

RESUMEN

En este trabajo de graduación se presentan los orígenes, la evolución y los estándares internacionales de la Continuidad del Negocio. El estándar BSI 25999 presenta la metodología para crear un programa de Continuidad del Negocio en las empresas dividido en cuatro partes, primero entender la empresa por medio de un análisis de impacto al negocio y una evaluación de riesgos. En segundo lugar, una definición de las estrategias de recuperación tomando en cuenta los recursos clave. Luego desarrollar e implementar las estrategias para asegurar la respuesta en caso de desastre. Por último, se debe ejercitar, probar, mantener y revisar periódicamente el plan para asegurar que la organización esta preparada ante cualquier tipo de desastre.

La telefonía celular se ha convertido en un servicio de comunicación esencial de consumo masivo, por lo que es prioritario contar con planes de Continuidad del Negocio. La tecnología de la red de telefonía móvil más popular es GSM. Para las centrales de telefonía móvil o MSC, desde el punto de vista de Continuidad del Negocio se presentan tres tipos de topologías: Independiente o *Stand Alone*, en espera o *Standby* y en grupo o *In Pool*. Cada una de estas topologías tiene su forma de funcionamiento, dimensionamiento, modelo de tráfico y características de servicio.

Para la definición de las estrategias de recuperación se deben tomar en cuenta cuatro recursos clave: personal, localidades, tecnología e información. Para cada uno de estos existe una guía de estrategias genéricas que se deben analizar para definir cuál es la mejor de acuerdo a criterios de costo beneficio, el nivel de madurez del negocio y la factibilidad técnica.

OBJETIVOS

- **General**

  Este trabajo de graduación tiene como propósito presentar un marco de referencia para la definición de las posibles estrategias de recuperación de centrales de telefonía celular en el caso de desastre.

- **Específicos:**

  1. Presentar los criterios fundamentales para el diseño de estrategias de recuperación en centrales de telefonía celular en caso de desastre.
  2. Presentar las opciones genéricas de estrategias de recuperación de centrales de telefonía celular en caso de desastre.
  3. Crear una referencia para el diseño de topologías de sistemas de comunicación que sean robustas para soportar un desastre natural.
  4. Contribuir en la difusión y aplicación de las normas internacionales de Continuidad del Negocio, para estudiantes de ingeniería.

INTRODUCCIÓN

En los últimos años se ha despertado la conciencia de lo frágil que puede ser la humanidad al recibir los embates de la naturaleza a través de desastres naturales tales como el tsunami del océano índico en el 2004, o los terremotos de Haití y Chile en el 2010, también de lo vulnerable a los desastres provocados por el hombre como el ataque terrorista a las torres gemelas del 11 de septiembre de 2001 o los ataques al metro de Moscú en el 2010 a nivel empresarial y de gobierno este entendimiento ha provocado la necesidad de contar con planes para responder en forma ordenada, coherente y rápida ante este tipo de desastres, además de trabajar en la mitigación de los riesgos que los producen. Respondiendo a esta exigencia se ha desarrollado la metodología conocida como la Administración de la Continuidad del Negocio o BCM por sus siglas en inglés.

La telefonía celular se ha convertido en un servicio de comunicación esencial de consumo masivo, por lo que es prioritario que los operadores cuenten con planes de Continuidad del Negocio, en algunos países de Latinoamérica como Colombia y Perú está regulado que deben contar con este tipo de planes y asegurar cierto nivel de servicio a pesar de desastres naturales o provocados por el hombre, por lo que contar con estrategias de recuperación de centrales de telefonía en el caso de desastre se convierte en algo fundamental.

Este trabajo de graduación tiene como propósito presentar un marco de referencia, para la definición de las posibles estrategias de recuperación de centrales de telefonía celular en el caso de desastre.

Se inicia con la presentación de los antecedentes de la Continuidad del Negocio como metodología para responder ante desastres y mitigar los riesgos de la organización de sufrir un desastre.

Luego se presenta la norma BSI 25999, que es el estándar de facto de la administración de la Continuidad del Negocio incluyendo el código de práctica y la guía de implementación.

Se presenta también la arquitectura de una red celular GSM con sus partes principales, así como la teoría sobre el funcionamiento y dimensionamiento de las centrales de telefonía móvil, conjuntamente con las topologías de las centrales desde el punto de vista de Continuidad del Negocio.

Además, se presentan las estrategias genéricas de continuidad para el personal, las localidades, la tecnología y la información que servirán de base para el desarrollo de las estrategias de recuperación.

Por último, se presentan los criterios de selección de la estrategia de recuperación ante desastres basado en un análisis de que las estrategias se pueden utilizar de acuerdo a la etapa en que se encuentra la empresa dentro del ciclo de vida del negocio, además del análisis costo beneficio de las estrategias posibles y el análisis de la factibilidad técnica.

A pesar de que este trabajo se enfocó para la industria de las telecomunicaciones, se puede utilizar como guía para cualquier empresa sin importar el giro del negocio, el tamaño o la ubicación geográfica.

La Continuidad del Negocio es una industria que está creciendo donde se necesitan profesionales certificados que puedan ayudar a las empresas en sus iniciativas de Continuidad del Negocio.

1. ANTECEDENTES DE LA CONTINUIDAD DEL NEGOCIO

1.1. Historia de la Continuidad del Negocio

La Continuidad del Negocio tiene sus raíces en los planes para Recuperación de Desastres, que surgieron entre las décadas de los años 50 y 60, en esa época las empresas empezaron a almacenar copias de seguridad de sus datos críticos en papel y/o formato electrónico *(tapes, diskettes)*, en lugares alternativos. Al principio no fueron muy frecuentes, luego la copia de seguridad y los procedimientos de almacenamiento fuera del sitio de trabajo donde operaban se hicieron más frecuentes y regulares en la década de los años 70, hasta que una tercera parte de la capacidad de las instalaciones de almacenamiento era en un lugar alternativo o *"Hot Site"*.

La Recuperación de Desastres tuvo auge en Estados Unidos durante los años 80 cuando el mercado de *"Hot Sites"* creció a más de un centenar de proveedores. El hot site se convirtió en una solución popular de recuperación de datos para empresas financieras, con grandes ordenadores centralizados.

La Continuidad del Negocio se puede definir como la habilidad de una empresa para recuperarse de un evento de tal forma que las funciones críticas del negocio continúen sin importar las circunstancias. Proceso de desarrollar acuerdos y procedimientos anticipados que le permiten a una empresa responder ante un evento de tal forma que las funciones del negocio continúen operando con los niveles de interrupción o bajo cambios primordiales planificados. Esto incluye los procesos del negocio críticos.

"La Continuidad del Negocio es la capacidad estratégica y táctica de la organización para planear y responder a las interrupciones incidentales del

negocio con el fin de continuar con las operaciones de la empresa en un nivel previamente aceptado", según la definición de la norma Británica o BSI 25999 *(British Standard Institute).*

En 1983, la Oficina Federal de la Contraloría de la Moneda o OCC, *(Federal Office of the Comptroller of Currency)* ordenó que las instituciones financieras elaboraran planes documentados de recuperación de los datos, esta fue la primera regulación gubernamental sobre Continuidad del Negocio en los Estados Unidos. Con las directrices específicas, la Directiva fue ampliamente vista como responsable de la copia y recuperación de la base de datos. De conformidad con la mayoría entró la forma de transportar las cintas de respaldo a lugares fuera del sitio de almacenamiento. No fue hasta 1989 que la mejor documentación, mantenimiento y prueba de planes de recuperación fueron requeridos por la Ley Federal de Instituciones Financieras del Consejo de Exámenes o FFIEC *(Federal Financial Institutions Examinations Council).*

La década de los 90 vió quizás la mayor revolución de la informática para impactar a la industria de la Recuperación de Desastres, como los sistemas informáticos llevados a los centros de información o centros de datos. La mayoría de las empresas pasó de una estructura centralizada a vastas redes de servidores y computadoras de escritorio distribuidas en toda la organización. Esto cambió la forma de Recuperación de Desastres, así como el entorno informático descentralizado abrió la puerta para la recuperación de los medios que abarcan un conjunto mucho más amplio de posibles combinaciones de hardware y de software.

A mediados de la década de los 90, la Continuidad del Negocio se convirtió en un sustituto popular para el término de Recuperación de Desastres, fue así como los planificadores de recuperación empezaron a disminuir las vulnerabilidades de los sistemas, el error humano en la actividad de la red y la intrusión a fallas de las telecomunicaciones como resultado de la operación descentralizada.

El término de Recuperación de Desastres se utiliza para describir los medios tradicionales de la Tecnología de la Información o IT, *(Information Technology)* relativas a la recuperación y almacenamiento de datos, mientras que la Continuidad del Negocio se convirtió en el término para describir la necesidad de mantener la continuidad en toda la empresa, desde las instalaciones hasta las personas y las comunicaciones.

También entre la década de 1990 y el 2000, las presiones reguladoras y normas de la industria comenzaron a impactar a las organizaciones, especialmente a las de servicios financieros y la industria de los cuidados de la salud. Estas directrices y normas gubernativas, no obstante impulsaron las iniciativas para la continuidad y recuperación y contribuyeron enormemente a la evolución de la disciplina de la Continuidad del Negocio.

Después de los ataques y atentados terroristas, incidentes de ántrax, los huracanes, las inundaciones que afectaron a los Estados Unidos y otros incidentes importantes en todo el mundo, la mayoría de los profesionales de la tecnología de la información entienden ahora que las copias de seguridad fuera de sitio *(off site)* es sólo una pequeña parte de una estrategia general para la Recuperación de Desastres.

A medida que la tecnología continúa siendo una parte integral de las operaciones de la organización en cada nivel, el trabajo de IT se ha ampliado para convertirse en un todo. En la actualidad es difícil encontrar rincones de una empresa en que la tecnología no esté. Como resultado de la necesidad de planificar las posibles alteraciones, los servicios de tecnología han aumentado de manera exponencial. Los planes de la Continuidad del Negocio y Recuperación de Desastres o BC / DR *(Business Continuity / Disaster Recovery)* fueron sin duda puestos para examinar a muchas empresas financieras después de los ataques terroristas en los Estados Unidos el 11 de septiembre de 2001, pero aún después de varios años, hay muchas empresas que aún no tienen ningún tipo de Continuidad del Negocio o plan de

Recuperación de Desastres. Parece difícil pensar que no se cuente con un plan en el lugar, pero las estadísticas muestran que muchas empresas ni siquiera tienen planes de copias de seguridad de datos sólidos. La falta de tiempo y de recursos, la falta de un sentido de urgencia, la falta de un proceso para desarrollar y mantener un plan son algunas de las causas.

1.2. Razón de ser de la Continuidad del Negocio

Actualmente, la Continuidad del Negocio es una industria en crecimiento motivada por los constantes desastres naturales y las regulaciones que los gobiernos están adoptando para asegurar los bienes y derechos de sus ciudadanos.

Existen riesgos inherentes en el día a día de las operaciones de la empresa, los puntos únicos de fallo que pueden no ser obvios, pero que un análisis de riesgos activo puede descubrir. Entender las dependencias y las interdependencias de las ubicaciones, las funciones de negocios, la cadena de valor y sistemas de tecnología pueden identificar los riesgos que nunca han sido reconocidos de otro modo.

En la actualidad las empresas se enfocan principalmente en la protección de los procesos críticos de la organización y no como antes a la protección del centro de cómputo.

Las causas de la interrupción del negocio tienen muchas facetas pueden ser operacionales como el error humano o error del proveedor de servicios; y/o técnicas como fallas de luz y fallas de hardware y software.

El incremento de las interrupciones son debido a:

- Cambios de localidad.

- Ataques de denegación de servicios los cuales pueden ser de dos formas comunes:
    - Forzar a la computadora de la víctima a inicializar o consumir sus recursos de tal forma que no pueda continuar proporcionando su servicio.
    - Obstaculizar el medio de comunicación entre los usuarios potenciales y la víctima, para que no puedan seguir comunicándose en forma adecuada.
- virus y gusanos computacionales como los ataques electrónicos terroristas.

Un desastre es un evento súbito, no planificado que ocasiona un gran daño o pérdida.

Se definen como funciones críticas las actividades o información del negocio que no pueden ser interrumpidas o no están disponibles por varios días hábiles sin poner en riesgo en forma significativa la operación de la empresa.

La infraestructura crítica son los sistemas cuya incapacidad o destrucción pueden tener un impacto de debilitamiento en la seguridad económica de una empresa, comunidad, nación, etc.

Los registros críticos son los datos o documentos que si son dañados o destruidos pueden causar una inconveniencia considerable y/o requerir reemplazo o re-creación a un costo considerable. También llamados registros vitales.

Dentro los registros vitales o críticos están los datos e información requeridos para soportar una función de negocios (por ejemplo histórica, requerimientos reguladores) y deben ser mantenidos fuera en una localidad externa y estar disponibles. Los registros vitales pueden ser, entre otros, las políticas y manuales de procedimientos, documentos o datos de entrada, manuales de software y otras aplicaciones, lista de proveedores, pólizas de seguro, etc.

La Planificación de la Continuidad del Negocio o BCP *(Business Continuity Planning)* es una metodología utilizada para crear y validar un plan para mantener las operaciones comerciales continuas antes, durante y después de los desastres y acontecimientos destructivos. A finales de 1990, la Planeación de la Continuidad del Negocio llegó a la vanguardia de las empresas tratando de evaluar la probabilidad de falla en el sistema de negocios a partir del 1 de enero 2000.

La Planificación de la Continuidad del Negocio tiene que ver con la gestión de los elementos operativos que permiten que un negocio funcione con normalidad, a fin de generar ingresos. Es a menudo un concepto que se utiliza en la evaluación de diversas estrategias de tecnología. Por ejemplo, algunas empresas no pueden aceptar interrupciones como las instituciones financieras, procesamiento de tarjetas de crédito, algunas empresas de alto volumen de operaciones en línea y las compañías de telecomunicaciones, especialmente las de telefonía celular. Ellos pueden decidir que el costo del total de los sistemas redundantes es una inversión que vale la pena porque el costo de tiempo de inactividad, incluso para cinco o diez minutos podría costar millones de dólares. Estas empresas requieren funcionar continuamente y sus planes operativos reflejan esta prioridad.

La Continuidad del Negocio tiene que ver con el mantenimiento de la empresa en funcionamiento, independientemente del riesgo potencial, amenaza o causa de la interrupción.

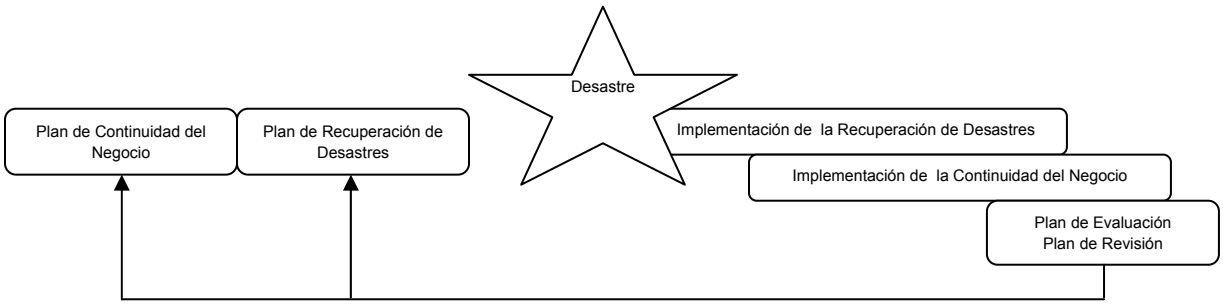
La disponibilidad continua es un subconjunto de la Continuidad del Negocio. Es también conocido como un requisito de tiempo inactivo y es muy caro para planificar e implementar. Para algunas empresas, puede ser una buena inversión porque el costo de tiempo de inactividad es mayor que el costo de la aplicación de medidas de disponibilidad continua.

El plan de Recuperación de Desastres debe ser apropiado al tamaño de la organización, presupuesto y otras restricciones.

La Recuperación de Desastres es parte de la Continuidad del Negocio y se ocupa de los efectos inmediatos de un evento. Recuperarse de una falla del servidor, brechas de seguridad, o de un huracán entran dentro de esta categoría. La Recuperación de Desastres por lo general tiene varios pasos en las etapas de la planificación, aunque estos rápidamente pueden cambiar durante la ejecución, porque la situación durante una crisis no es exacta al plan.

La Recuperación de Desastres implica detener los efectos del desastre tan rápido como sea posible y hacer frente a las consecuencias. Estas incluyen el cierre de los sistemas que han sido violados, la evaluación de los sistemas que están afectados por una inundación o un terremoto y determinar la mejor manera de proceder. Al mismo tiempo durante la Recuperación de Desastres, las actividades de la Continuidad del Negocio comienzan a traslaparse, como se muestra en la Figura 1, además del ciclo de planeación, implementación y evaluación que es parte de su comportamiento.

Figura 1. Continuidad del negocio y planeación de la recuperación de desastres, implementación y revisión



Fuente: Snedaker, Susan.
Continuity & Disaster Recovery for IT Professionals.
Pág. 5

1.3. Situación actual de la Continuidad del Negocio

La Gestión de la Continuidad del Negocio es la actividad que se lleva a cabo en una organización para asegurar que todos los procesos de negocio críticos estarán disponibles para los clientes, proveedores y otras entidades que deben acceder a ellos. Estas actividades incluyen un gran número de tareas diarias como gestión de proyectos, copias de seguridad de los sistemas, control de cambios y escritorio de ayuda. La Gestión de la Continuidad no se implanta cuando ocurre un desastre, si no que hace referencia a todas aquellas actividades que se llevan a cabo diariamente para mantener el servicio y facilitar la recuperación.

La base de la Gestión de la Continuidad son las políticas, lineamientos, estándares y procedimientos implementados por una organización. Todo el diseño, implementación, soporte y mantenimiento de los sistemas debe estar fundamentado en la obtención de un buen plan de Continuidad del Negocio, Recuperación de Desastres y en algunos casos, soporte al sistema. En ocasiones la Gestión de la Continuidad se confunde con la gestión de la recuperación tras un desastre, pero son conceptos diferentes. La Recuperación de Desastres es una pequeña parte de la Gestión de la Continuidad.

El término Continuidad del Negocio describe una filosofía o metodología de desarrollar la actividad del negocio, mientras que la planificación de la Continuidad del Negocio es la actividad que determina cuál debe ser esta metodología. El Plan de Continuidad del Negocio puede ser visto como la metodología utilizada por los usuarios de la organización diariamente para asegurar el desarrollo normal del negocio.

La preparación de la Recuperación de Desastres o DR *(Disaster Recovery)* sigue siendo un tema importante de IT, particularmente para las empresas de América del Norte, quienes determinaron a través de una

encuesta que el 21 por ciento de las empresas de América del Norte y el 14 por ciento de las empresas europeas identificaron "mejorar significativamente las capacidades de Recuperación de Desastres" como una prioridad crítica de IT.

La Recuperación de Desastres supone que se cuenta con un sitio alternativo en el que puede recuperarse las operaciones del centro de datos primarios. De acuerdo a *Forrester´s Business Data Services Enterprise and SMB Hardware Survey,* Norte América y Europa, Q3 2007, el 65 por ciento de los encuestados tienen al menos una alternativa de centro de datos.

Debido a las limitaciones de capacidad, modernización y consolidación de centros de datos muchas empresas están reevaluando la ubicación de centros de datos existentes y re-examinando sus perfiles de instalación de centros de datos. Esta reevaluación y reexamen conducen a menudo a la inversión de un centro de datos de nueva construcción, o al menos el arrendamiento de un espacio para el centro de datos dentro de una localidad del proveedor, que ya ha realizado la inversión en una instalación de un centro de datos. Esta reevaluación y nuevo examen proporcionan una oportunidad para abordar algunas de las consideraciones más fundamentales de Recuperación de Desastres en el centro de datos de diseño y construcción de la integridad del sitio, la selección del sitio y la recuperación del sitio.

- Centros de datos actuales que no tiene integridad del sitio adecuado. La mayoría de veces, los centros de datos son situados cerca de o en instalaciones de la empresa, como la sede. A menudo, los centros de datos comenzarán dentro de una o dos salas de informática y luego se expanden a otras salas de emergencia conforme al crecimiento de la empresa.

  Estas no tienen suficiente integridad, energía de reserva, o refrigeración, por lo general pueden ser localizadas en algunas partes del edificio, muy susceptibles a las inundaciones.

- Centros de datos actuales situados en zonas de alto riesgo. Los centros de datos rara vez son cuidadosamente planificados o situados en un sitio que tiene el menor riesgo posible de desastres naturales o artificiales. Están normalmente ubicados en la empresa o cerca de la misma o en otro lugar de operaciones, que son a menudo en los grandes centros urbanos que pueden ser blanco de desastre e interrupciones.
- Empresas que no aprovechen los centros de datos actuales para actuar como sitios de recuperación interna. Las empresas a menudo tienen múltiples centros de datos a nivel regional e internacional, pero un grupo IT decidirá encargar la Recuperación de Desastres a un proveedor de servicios cuando se podría haber utilizado otro centro de datos de la empresa como un sitio de recuperación y mantener el control de la preparación para la Recuperación de Desastres en casa.

Un tercer nivel del centro de datos tiene algunas de las características siguientes: sistemas de alimentación ininterrumpida, la generación de energía de reserva, diversas conexiones a la red eléctrica, un edificio independiente, al mismo tiempo de mantener la infraestructura (sistemas redundantes y rutas de distribución) y el personal de sitios en el monitoreo y corregir los problemas de instalación.

Un tercer nivel del centro de datos va a mitigar muchos de los hechos evitables, como cortes de energía eléctrica, red de fallas y errores de hardware. Las empresas a menudo se preparan para los desastres más extremos como los huracanes o atentados terroristas, pero en realidad son mucho más comunes los eventos tales como cortes de electricidad o una inundación en el edificio. La declaración de desastre y el sitio de recuperación son costosas y arriesgadas y las empresas deben evitar la declaración de desastre a menos que sea absolutamente necesario.

Un estudio reciente, patrocinado por el *Wall Street West Center for Organizational Continuity* y conducido por la Revista *Continuity Insights* tuvo

como fin determinar las habilidades, la educación y la experiencia que se requerirán en la próxima generación de profesionales de la Continuidad del Negocio y los resultados fueron sorprendentes.

"La Continuidad del Negocio parece ser un creciente campo de especialización con los recursos existentes, aparentemente experimentados", ya que casi el 48 por ciento de los encuestados tienen más de 51 años de edad, con respecto a la próxima generación de talentos que necesitan ser cultivados," dice Glenn W. Tyranski de *NYSE Regulation:* "Curiosamente, casi el 42 por ciento de los encuestados tienen sus grados de licenciatura en negocios y sólo el 12 por ciento en la ingeniería, lo que parecería dar a entender que la Continuidad del Negocio es un campo que atrae a profesionales de variados orígenes y no sólo de la comunidad de IT ya que sólo el 21 por ciento de la población tenía experiencia previa sobre IT en su trabajo de Continuidad del Negocio".

"Además, casi dos tercios de los encuestados encontró su camino a la Continuidad del Negocio y no estaban contratados directamente en el campo. Un poco más del 87 por ciento de los encuestados coincidieron en que la Continuidad del Negocio seguirá evolucionando como una función de negocio distinta e integral. Ochenta y ocho por ciento cree que los profesionales de la Continuidad de Negocios requieren de una educación continua, más habilidades y más experiencia funcional transversal. Y el 77 por ciento piensa que la demanda de profesionales de la Continuidad del Negocio para ser certificados irá en aumento."

"Es evidente que la certificación profesional es muy importante, ya que casi tres cuartas partes de los encuestados están actualmente certificadas en la Continuidad del Negocio o trabajando activamente en la adquisición de este conjunto de habilidades especializadas," dice Tyranski, agregando que él cree que "la encuesta también pone de relieve que los conocimientos críticos para los profesionales en la búsqueda de esta posible carrera son habilidades

interpersonales, la escritura, la planificación y la capacidad de gestión es muy importante como una base firme a la experiencia de la Continuidad del Negocio."

A los encuestados se les preguntó cuáles son los cinco rasgos más importantes de la personalidad para ser un eficaz profesional de Continuidad del Negocio. Los cinco primeros fueron: colaboración, analítico, adaptable, flexible y articulado, seguido de cerca por persuasivos. Los rasgos que recibieron menos votos fueron: espontáneo, tolerante, implacable, independiente y capaz de soportar las críticas.

Los encuestados también identificaron el conjunto de habilidades específicas que habrían de buscar estos candidatos para puestos de trabajo en la Continuidad del Negocio en sus propias organizaciones. Las habilidades fueron: la experiencia de Continuidad del Negocio, la planificación de capacidades, habilidades interpersonales, experiencia organizacional y liderazgo y habilidades de escritura. Las menos importantes fueron: Título universitario en la Continuidad del Negocio o de una relación importante, la experiencia en el sector público, las habilidades bilingües, y la experiencia empresarial internacional.

La encuesta también preguntó a los encuestados sobre una nueva iniciativa, un "centro de excelencia" en la Continuidad del Negocio que surgirá del Consorcio de Educación Superior o WSW *(The Wall Street West Higher Education Consortium)*. El consorcio tiene por objeto mejorar la competitividad global de la región occidental de *Wall Street* vinculando la seguridad de la nación y la garantía de los líderes de información de la industria con las instituciones de la región de educación superior. En consulta con los miembros del consorcio, las cuestiones operacionales clave, las tendencias nacionales y las oportunidades se identificaron alrededor de los temas del programa a ser desarrollado por el futuro consorcio. Basándose en esta información y el

análisis, la disciplina de la Continuidad del Negocio surgió como enfoque principal del consorcio.

Con un enfoque en la Continuidad del Negocio, el consorcio debe abordar tres áreas principales del mercado primario: 1) La brecha creciente de calificaciones y la escasez general de los profesionales calificados en la Continuidad de Negocio, 2) empleados de todos los sectores de la industria carece de un conocimiento general y conciencia de los problemas de Continuidad del Negocio, las tendencias, las mejores prácticas, estrategias y tácticas relacionadas con sectores específicos de la industria y 3) organizaciones públicas y privadas carecen de las estructuras internas de funcionamiento, las herramientas, procedimientos y certificaciones para garantizar la continuidad de las operaciones.

A la luz de las demandas del mercado identificadas, la naturaleza de la WSW y el análisis de las mejores prácticas nacionales, un plan de operaciones en curso basado en un "centro de excelencia" como modelo fue propuesto. Estos centros ofrecen apoyo a la investigación crítica y la fuerza de trabajo de las agencias federales, los líderes del Congreso y la industria.

En cuanto a los lectores de cómo se sentía sobre el nuevo Centro de Continuidad Organizacional, les gustaría verlo proporcionando información sobre las mejores prácticas (15.76 por ciento), mediciones y otras herramientas (12.23 por ciento), programas de capacitación (11.50 por ciento), investigación de la industria (10.96 por ciento) y estudios de casos (10.10 por ciento).

El estudio revela la importancia de crear el Instituto que servirá como un recurso permanente para los solicitantes de empleo y los proveedores de educación y la industria para compartir las mejores prácticas, promover sus cursos y realizar investigaciones en esta área crítica de bastante demanda", dice Chris Harán, el Centro Nacional para la organización y la continuidad del Nordeste Instituto de Tecnología de Pensilvania. "El Centro Nacional para la Organización de la Continuidad está bien posicionada para seguir adelante con

la misión original del *Wall Street / Wired* para ayudar tanto a la actual y próxima generación de estos profesionales en la búsqueda de oportunidades de educación, formación y especialización de la industria. La fuerza de trabajo formada y comprometida no sólo beneficiará a los propios individuos, sino también a las comunidades donde viven y trabajan y de las empresas que los emplean", Tyranski añade.

Cerca del 85 por ciento de los encuestados cree que la Continuidad del Negocio ha ganado más apoyo a la gestión y la participación. Y el mismo porcentaje que respondió creen que la Continuidad del Negocio se ha involucrado más de forma inter funcional en las empresas. Cerca del 30 por ciento predijo que agregando más personal en la Continuidad del Negocio la economía de la misma mejorará.

2. NORMAS Y ESTÁNDARES DE LA CONTINUIDAD DEL NEGOCIO

Los programas de Continuidad del Negocio son más efectivos cuando se basan normas generalmente aceptadas y se rigen por los objetivos del negocio. Los objetivos del negocio y las normas aceptadas forman el cimiento que agrega credibilidad y viabilidad al programa de Continuidad del Negocio.

Sin embargo, en el grupo de normas, leyes o lineamientos regulatorios que existen en el mundo, muchos hacen referencia a la gestión de la continuidad de los negocios, aunque no usen necesariamente la misma terminología. Algunas de las normas que existen son:

NFPA 1600 – la *National Fire Protection Association* de los Estados Unidos. Ha sido desarrollado desde la práctica de combate de incendios y enfoca la continuidad de los negocios desde una perspectiva de la negación del acceso, con algunas condiciones prescriptivas, a diferencia de la norma 25999.

ISO 17799 – una norma de sistemas de gestión de la seguridad de la información, la que gestiona y minimiza las amenazas a la información.

ISO 22399 – lineamientos para la toma de conciencia de los incidentes y la gestión de la continuidad operativa.

HB 221 y HB 292/293 – la norma y la guía australianas sobre la gestión de la continuidad de los negocios.

AS/NZS 4360:2004 – compartida por Australia y Nueva Zelanda, la que en conjunto con la HB 436 proporciona lineamientos sobre la gestión de riesgos.

SPRING TR 19 – la referencia técnica de Singapur sobre la gestión de la continuidad de los negocios, la que trata principalmente los aspectos técnicos de los sistemas.

El reporte King II sobre Gobernanza Corporativa – estos lineamientos de Sudáfrica para la gestión de riesgos, enfocan la gestión de la continuidad de los negocios desde la perspectiva del gobierno.

El *Civil Contingencies Act 2004* – esta acta recibió la aprobación real en 2004 en el Reino Unido, proporcionando lineamientos sobre la gestión de la continuidad de los negocios.

Debido a que la Continuidad del Negocio es un concepto nuevo hay pocas normas que la regulen en este capitulo revisaremos las siguientes instituciones internacionales: el Instituto Internacional de Recuperación de Desastres o DRII *(Disaster Recovery International Institute)*, el Instituto de Continuidad del Negocio o BCI *(Business Continuity Institute)* y el Instituto Británico de Normas o BSI *(British Standard Institute)*.

2.1. Instituto Internacional para la Recuperación de Desastres – DRII

El Instituto Internacional para la Recuperación de Desastres, fue fundado en 1988 con el fin de desarrollar una base de conocimientos en la planificación de contingencias y la gestión de riesgos.

Hoy en día el Instituto Internacional para la Recuperación de Desastres administra la principal industria de los programas educativos y de certificación para los que trabajan en la práctica de la planificación de la Continuidad del Negocio y de gestión.

Más de 3,500 personas en todo el mundo realizan la certificación profesional a través de este Instituto. La certificación individual y el establecimiento de un órgano común para mejorar el conocimiento de la profesión de la Gestión de la Continuidad del Negocio. Con este fin, los objetivos del Instituto son los siguientes:

- Promover una base de conocimientos básicos para la planificación de la Continuidad del Negocio o industria de recuperación de desastres mediante la educación, la asistencia y la publicación de la norma de recursos básicos.
- Certificar a individuos calificados en la disciplina.
- Promover la credibilidad y la profesionalidad de las personas certificadas.

El Instituto establece la norma internacional de la industria con las Prácticas Profesionales para los planificadores de la Continuidad del Negocio. Desde 1988, el Instituto ha proporcionado oportunidades de calidad de la educación superior para los profesionales de la Continuidad del Negocio. También establece criterios para evaluar el nivel mínimo aceptable de conocimientos y experiencias para el logro de la certificación profesional. Las prácticas "profesionales de los planificadores de la Continuidad del Negocio" son la base de estos cursos.

Las Prácticas Profesionales son ampliamente aceptadas como la base sólida para la planificación de la Continuidad del Negocio y han sido adoptados para los programas mundiales de muchas compañías. En un mundo incierto, la comprensión y la gestión del riesgo son un componente crítico, no sólo de éxito, sino también de supervivencia.

2.1.1. Las mejores prácticas: temática general

2.1.1.1. Programa de iniciación y gestión

Establecer la necesidad de un programa de gestión de Continuidad del Negocio o BCM *(Business Continuity Management)*, incluyendo las estrategias de resistencia, los objetivos de recuperación, Continuidad del Negocio, las consideraciones de gestión de riesgos operacionales y los planes de gestión de crisis. Los requisitos previos dentro de este

esfuerzo incluyen la obtención de apoyo a la gestión y organización y gestión de la formulación de las funciones o procesos necesarios para construir el marco de BCM.

2.1.1.2. Evaluación y control de riesgos

Determinar los riesgos (eventos o alrededores) que pueden afectar negativamente a la organización y sus recursos (personas, instalaciones, tecnologías), debido a la interrupción del negocio, la pérdida potencial de estos fenómenos y los controles necesarios para evitar o mitigar los efectos de esos riesgos. Como resultado de lo anterior, un análisis de costo-beneficio será necesario para justificar la inversión en controles.

2.1.1.3. Análisis del impacto en el negocio

Identificar los impactos resultantes de la interrupción de los negocios que pueden afectar a la organización y las técnicas que pueden ser utilizados para cuantificar y calificar dichos impactos. Identificar las funciones críticas de tiempo, sus prioridades de recuperación y la interdependencia para recuperar los objetivos de tiempo que pueden ser establecidos y aprobados.

2.1.1.4. Estrategias de Continuidad del Negocio

Aprovechar el resultado del Análisis del Impacto del Negocio o BIA *(Business Impact Analysis)* y Evaluación de Riesgos para desarrollar y recomendar estrategias de Continuidad del Negocio. Las bases de estas estrategias son tanto el tiempo de recuperación como los objetivos de apoyo de las funciones críticas de la organización.

2.1.1.5. Respuesta de emergencia y operaciones

Identificar la disposición de una organización para responder a una emergencia de manera coordinada, oportuna y eficaz. Desarrollar y aplicar los procedimientos de respuesta inicial y estabilización de las situaciones hasta la llegada de autoridades que tienen competencia.

2.1.1.6. Planes de continuidad

Diseñar, desarrollar e implementar Planes de Continuidad que dan continuidad y/o recuperación de lo establecido en los requisitos de la organización.

2.1.1.7. Programas de sensibilización y entrenamiento

Preparar un programa para crear y mantener la conciencia en las empresas y mejorar las habilidades necesarias para desarrollar e implementar la Gestión de la Continuidad del Negocio.

2.1.1.8. Ejercicio de planificación de la Continuidad del Negocio, mantenimiento y auditoría

Establecer un programa de ejercicio o prueba de los documentos; planeando los requisitos del ejercicio incluyendo la planificación, programación, la facilitación, las comunicación, auditoría y revisión posterior de la documentación. Establecer programa de mantenimiento para mantener los planes actuales y pertinentes. Establecer un proceso de auditoría que valide el cumplimiento con las normas, soluciones de

revisión, verificar los niveles adecuados de mantenimiento y ejercicio de las actividades y validar los planes actuales, precisos y completos.

2.1.1.9. Comunicación de crisis

Desarrollar y documentar los planes de acción para facilitar la comunicación de la información continua indispensable. Coordinar y ejercer con las partes interesadas y los medios de comunicación para garantizar la claridad en la comunicación de crisis.

2.1.1.10. Coordinación con las agencias externas

Establecer procedimientos y políticas aplicables para la coordinación continua y las actividades de restauración con las agencias externas (local, regional, nacional, servicios de emergencia, defensa, etc.), que cumplan con los estatutos y reglamentos aplicables.

2.2. Instituto de Continuidad del Negocio – BCI

El Instituto de Continuidad de Negocios (BCI) se creó en 1994 para permitir que los miembros individuales obtengan orientación y apoyo de los profesionales de la Continuidad del Negocio. El BCI tiene actualmente más de 4,800 miembros en 85 países. Su sede se encuentra en el Reino Unido.

Los miembros profesionales de este Instituto obtienen un estatus reconocido internacionalmente como la certificación que demuestra las competencias para llevar a cabo la Gestión de la Continuidad del Negocio (BCM), con un alto nivel.

Los titulares de la CBCI han logrado el éxito en el Certificado de BCI demostrando un profundo conocimiento y comprensión de las Directrices de Buenas Prácticas de la BCI.

En el año 2007 también la Asociación de BCI permitió a las organizaciones trabajar más estrechamente con el Instituto de Continuidad del Negocio para cumplir la misión de “Promover el arte y la ciencia de la Gestión de la Continuidad del Negocio en todo el mundo”.

El rol más amplio de la BCI y la Asociación de BCI es promover los más altos estándares de competencia profesional y la ética comercial en el suministro y mantenimiento de la planificación de la Continuidad del Negocio y de los servicios.

El BCI es el instituto más eminente del mundo y su nombre es inmediatamente reconocido como representante de las buenas prácticas y profesionalidad.

El BCI publicó su primera Norma de Buenas Prácticas o GPG *(Good Practices Guide)* en el año 2002. Esto jugó un papel importante en el desarrollo de especificación pública de la Gestión de la Continuidad del Negocio Especificación Pública Aceptada 56 o PAS 56 *(Public Acceptance Specification 56)* del Instituto de Normas Británico. El GPG05 se publicó seguido por una extensa reescritura para tomar en cuenta las ideas internacionales más recientes en BCM y el reconocimiento cada vez mayor en la práctica de BCM en los sectores públicos y privados.

Esta norma para la aplicación de la Gestión de la Continuidad del Negocio se ha preparado para apoyar el lanzamiento de BS 25999-1 un Código de Prácticas para la Gestión de la Continuidad del Negocio de la BSI. Fue vista como una norma de aplicación para BS25999 y como texto definitivo para aquellos que quieran entender los principios y las prácticas de BCM de forma más integral. Existe una estrecha relación entre la estructura de estas Buenas Prácticas y BS 25999-1. En ningún caso, sin embargo, es necesario que el

GPG sea visto como un reemplazo de aquellas normas o como una garantía de cumplimiento de esas normas.

El Instituto de Continuidad del Negocio define la Gestión de la Continuidad del Negocio como: “un proceso de gestión global que identifica los impactos potenciales que amenazan a una organización y proporciona un marco para el desarrollo de la resistencia y la capacidad para una respuesta eficaz que salvaguarde los intereses de las partes clave, la reputación, la marca y el valor de la creación de actividades.”

La Norma fue preparada en seis secciones, que están en línea con las versiones anteriores y también con la nomenclatura BS25999.

La sección 1: Información introductoria incluyendo la Política de la Gestión de la Continuidad del Negocio y la Gestión de Programas.

La Sección 2: Entender a la organización.

La sección 3: Determinar la Estrategia de la Continuidad del Negocio.

Sección 4: Desarrollar e implementar Respuestas al BCM.

Sección 5: Ejercitar, mantener y revisar los acuerdos de BCM.

Sección 6: Incluir la Gestión de la Continuidad del Negocio en la Cultura de la Organización.

2.3. Instituto Británico de Normas - BSI

El Instituto Británico de Normas es el equipo nacional de normas del Reino Unido, con una reputación reconocida a nivel mundial por la independencia, la integridad y la innovación en la producción de estándares que promuevan las mejores prácticas. Desarrolla y vende normas y soluciones de estandarización para satisfacer las necesidades de las empresas y de la sociedad.

Fue fundado en 1901 como el Comité de Normas de Ingeniería o ESC *(Enginnering Standards Committee)*. El equipo se ha convertido en una

organización de servicios independiente proporcionando soluciones basadas en la norma en más de 120 países.

Este Instituto representa los intereses económicos y sociales de las organizaciones de las normas europeas e internacionales a través del desarrollo de soluciones de información para las organizaciones británicas de todos los tamaños y sectores. Esta institución trabaja con las industrias de servicios, manufactura, gobierno y consumidores.

Esta organización desarrolla normas privadas, nacionales e internacionales, certifica productos y sistemas de gestión, proporciona servicios de pruebas de productos, proporciona formación e información sobre normas internacionales y el comercio internacional y por último proporciona soluciones de software para la gestión del desempeño.

La norma BSI 25999-1 de la Administración de la Continuidad del Negocio fue publicada y entró en vigencia el 30 de noviembre de 2006. Fue preparada por el Comité Técnico de la Administración de la Continuidad del Negocio. Fue elaborada considerando las experiencias educativas, técnicas y prácticas de la Gestión de la Continuidad del Negocio, proporcionando un sistema basado en buenas prácticas de esta gestión, sirve como punto de referencia para más situaciones donde la Gestión de la Continuidad del Negocio es llevada a cabo y para ser usada en las organizaciones grandes, medianas y pequeñas en los sectores industrial, comercial, público y voluntario.

La norma BS 25999 provee una base para el entendimiento, desarrollo e implementación de la Continuidad del Negocio en una organización o empresa, integra las disciplinas de manejo de riesgo y procesos con la Continuidad del Negocio dando como resultado una mejora en la confianza en las relaciones comerciales entre empresas o con el consumidor final.

La norma BS 25999 fue escrita en dos partes. La Parte 1, el código de práctica, esboza los objetivos, guías y recomendaciones de la norma. La Parte 2, la especificación, detalla las actividades que deberían ser completadas para

cumplir con los objetivos de la Continuidad del Negocio dentro del contexto de una filosofía de administración de riegos de una organización o empresa. Esta diseñada para ser “Auditable”, lo que significa que solo objetivos y requerimientos medibles son incluidos en la especificación.

La Continuidad del Negocio es una disciplina que está madurando rápidamente que se ha movido del campo de la recuperación de sistemas de IT a un campo de la resistencia y recuperación del negocio completo. Con estos cambios la terminología relacionada a la Continuidad del Negocio también maduro. Hace unos años, la planificación de la Continuidad del Negocio fue el término último para expresar el rol creciente que jugaba la continuidad en la protección contra la falla de procesos críticos del negocio. Conforme esta practica creció y se estableció como una disciplina clave para la administración de riesgos, ocurrió un movimiento hacia la normalización, similar a la iniciativa de la normalización de la calidad surgida en los años 90. Como resultado, “Sistemas de pensamiento” han sido aplicados a la Continuidad del Negocio, resultando en un nuevo término: Sistema de Gestión de la Continuidad del Negocio o BCMS *(Business Continuity Management System)*. BCMS se refiere al programa que abarca el desarrollo y gestión de políticas y procedimientos para proteger a las personas, los procesos y tecnología de una organización o empresa.

Antes de la publicación oficial se habían bajado un promedio de 250 copias del borrador de la norma BS 25999 del sitio del BSI. Sin embargo, luego del lanzamiento del BS 25999-1, el código de práctica, se han bajado 5,000 copias. Este extraordinario número de copias demuestra lo importante que es esta norma para un gran número de organizaciones. Otra importante consideración es que las dos más grandes compañías de corretaje de seguros en Estados Unidos, *Aon Corporation y Marsh Inc,* participaron en el comité de redacción de la norma. Este interés y participación son únicos y es una

indicación que la norma y certificación tiene un apoyo de la industria de seguros.

La BS 25999 provee la orientación y los detalles necesarios para que una organización o empresa pueda construir o mejorar su BCMS.

BS 25999 es una norma internacionalmente aceptada, desarrollada por la organización mundialmente reconocida como la líder en normalización, pruebas, registro y certificación de normas.

Una norma es necesaria para ayudar a enfocar un programa en las actividades principales encaminadas a aumentar la capacidad de respuesta, flexibilidad y capacidad de recuperación. BS 25999 proporciona un marco de trabajo y especificaciones a seguir y centra la atención en las actividades más críticas del negocio. Cuando se desarrolla un programa de Continuidad del Negocio, es esencial saber la diferencia entre un Sistema de Administración de la Continuidad del Negocio y un Plan de la Continuidad del Negocio. Por definición, los Planes de Continuidad del Negocio son documentos enfocados sólo en la recuperación de una interrupción, dejando los riesgos residuales de la interrupción ocurrida sin mitigar. La BS 25999 esboza un sistema para atender y reducir el riesgo de la interrupción ocurrida, así como responder a los riesgos que ocurren después de una interrupción.

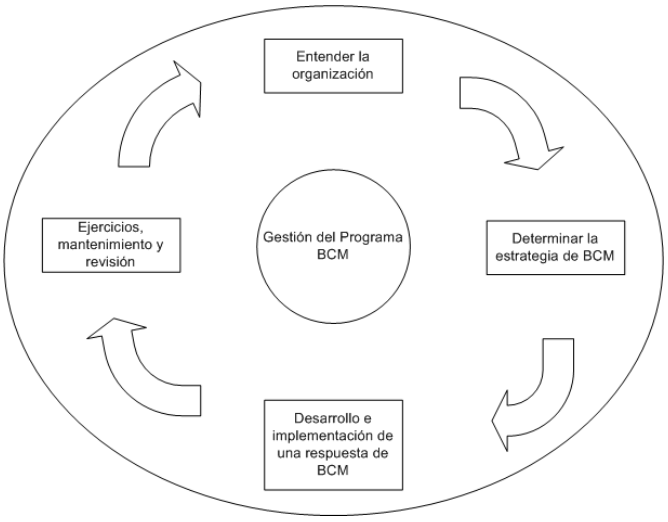
Una organización debe seleccionar una norma que refleje el enfoque actual de la entidad para la gestión de riesgos. La norma debería estar orientada a lograr una gestión de riesgos, mediante la evaluación de actividades críticas y objetivos de la entidad. Si estos objetivos no están alineados con el enfoque de la organización, los intentos de modificar la norma debilitaran la estructura del sistema. Similarmente, si los esfuerzos son hechos para modificar el enfoque de la organización en la administración de riesgos para cumplir con la norma, la organización puede resistirse a cambiar su cultura.

Aunque el uso de la terminología es inevitable, el uso extensivo de acrónimos y terminología debe evitarse, en vez, cualquier término usado debería ser descrito y requiere una pequeña explicación.

Las normas pueden ser confusas, como son generalizadas y proveen una explicación de alto nivel sobre los resultados esperados, la BS 25999 se desarrolló en dos partes, el Código de Práctica y la Especificación, para hacerla mas fácil de entender e implementar. La Parte 2, la Especificación, establece los objetivos mínimos requeridos para un BCMS efectivo y proporciona el marco de trabajo para su implementación, gestión y mejora continua. Fue escrito de tal forma que pueda medirse el cumplimiento. La Parte 1 de la norma describe una "Buena Práctica", va más allá de los requisitos mínimos y las oportunidades de gestión de riesgos y los métodos para cumplir los objetivos del negocio.

La BS 25999 describe un enfoque continuo del ciclo de vida del BCMS que busca la mejora continua, definiendo el sistema como un programa dinámico que evoluciona continuamente. Ver Figura 2.

Figura 2. Ciclo de vida del sistema de gestión de la Continuidad del Negocio



Fuente: **Business continuity management. Part 1: Code of practice.** Pág. 9

2.3.1. Descripción de la norma BS 25999

La especificación de la norma BS 25999 está organizada en cuatro fases: Planificación del BCMS, Implementar y Operar el BCMS, Seguimiento y Revisión del BCMS y Mantenimiento y Mejora del BCMS. Dentro de cada fase, las actividades principales son anotadas para llevar a cabo la implementación de la norma. Cada una de esas actividades es listada a continuación.

2.3.1.1. Planificación del BCMS

a. Requerimientos del Programa. Identificar el alcance y objetivos del BCMS, tomar en cuenta los objetivos estratégicos de la organización, productos y servicios principales, tolerancia al riesgo y cualquier obligación regulatoria, contractual o de las partes interesadas en el negocio.
b. Política de BCM. Documenta el compromiso gerencial para el BCMS e identifica los objetivos y alcance, estableciendo los intervalos de revisión requeridos y las políticas de comunicación para todos los empleados de la compañía.
c. Suministro de recursos y competencia del personal. La asignación de recursos suficientes para implementar, supervisar y mantener el BCMS, incluida la formación necesaria para reforzar y continuar con la competencia de los recursos asignados.
d. Incorporación de BCM. La creación de la conciencia y el entrenamiento continuo en funciones especificas para garantizar que todos los empleados entiendan la política y

objetivos de BCMS, así como su papel en la consecución de los objetivos de BCM para la organización.

e. Documentación y Registros. El desarrollo de los procesos para gestionar la documentación y los registros creados como parte del BCMS, para garantizar la integridad, disponibilidad, exactitud y seguridad de los mismos.

2.3.1.2. Implementación y operación del BCMS

a. Análisis del Impacto al Negocio. Determinar el impacto de una interrupción de una de las actividades críticas de la organización en orden de asignar los objetivos de recuperación.

b. Evaluación del Riesgo. Entender las amenazas y vulnerabilidades de las actividades críticas de la organización y los recursos de apoyo.

c. Determinar la Opciones. Identificar los posibles tratamientos para el riesgo, con el fin de mitigar el riesgo al reducir la probabilidad de una interrupción, limitando su plazo o reduciendo su impacto.

d. Determinar la Estrategia de Continuidad del Negocio. Definir como la organización responderá y se recuperará de una interrupción, incluyendo la relación con los partes interesadas internas y externas.

e. Estructura de Respuesta a Incidentes. Identificar al personal, desarrollar los planes y asignar los recursos para responder a los incidentes, generar una respuesta adecuada de la

Continuidad del Negocio y comunicar con las partes interesadas.

f. Los Planes de Manejo de Incidentes y Continuidad del Negocio. Documentar cómo la organización se encargará de un incidente y recuperará o mantendrá las actividades a un nivel predeterminado.

g. Ejercitar. Validar que los planes y los preparativos cumplen los requerimientos del negocio y generar los planes de acciones para mejorar y actualizar los planes.

h. Mantenimiento y Revisión de los Acuerdos de BCM. Revisar los acuerdos de BCM a intervalos definidos para garantizar la continua adecuación, idoneidad y eficacia de los mismos.

2.3.1.3. Seguimiento y revisión del BCMS

a. Auditoria Interna. El aseguramiento que la organización lleva a cabo revisiones independientes del BCMS a intervalos definidos para determinar si cumple con los planes, si se han implementado y mantenidos adecuadamente y cumple con la política de la organización y los objetivos.

b. Revisión de la Gestión. La revisión del BCMS de la organización a intervalos definidos para garantizar la adecuación, idoneidad y eficacia.

2.3.1.4. Mantenimiento y mejora del BCMS

a. Acciones Preventivas y Correctivas. La mejora del BCMS a través de la aplicación de acciones preventivas y correctivas.

b. Mejora Continua. La mejora continua de la efectividad del BCMS a través de la revisión de la política y objetivos, resultados de auditoria, análisis de eventos supervisados, las acciones preventivas y correctivas y la revisión de la gestión.

La norma BS 25999 establece los procesos, principios, y terminología para hacer frente a la Continuidad del Negocio y el riesgo de disponibilidad. También proporciona un amplio conjunto de controles basados en las prácticas líderes en la industria que ayuda a las organizaciones a desarrollar, implementar, mantener y madurar los procesos de Continuidad del Negocio. La norma se puede usar como un marco de trabajo para que las organizaciones sin un BCMS puedan efectivamente establecer un programa viable y los que ya tienen un programa puedan garantizar que se cumplen las mejores prácticas en su caso. El creciente consenso respecto a la BS 25999, junto con la oportunidad de certificarse en su uso, ofrece beneficios sin igual para empresas de cualquier tamaño cuyos clientes confían en los productos y servicios de la organización.

3. TOPOLOGÍAS DE LAS CENTRALES DE TELEFONÍA CELULAR

3.1. Historia del sistema global para comunicación móvil o GSM

Debido al incremento de la demanda de nuevos servicios y la necesidad de cobertura de comunicaciones móviles, surgió la idea de implementar un sistema normado y estandarizado de comunicaciones móviles. A principios de la década de los ochentas la CEPT *(Conférence Européenne des Postes et Télécommunications)* formo un grupo de especialistas para realizar la definición de un sistema de telefonía móvil que fuera común para los países de Europa Occidental. Este grupo fue llamado *Group Speciale Mobile* y el sistema que desarrollaron fue lo que hoy conocemos como GSM *(Global System for Mobile Communications)*. Las características debían de ser la compatibilidad y la transparencia internacional, el sistema debe ser regional o semiglobal y los usuarios del sistema tendrían acceso a él desde prácticamente cualquier punto de la región definida. Desde el punto de vista del usuario, las redes de GSM de comunicaciones móviles ofrecen un paquete más atractivo porque además del servicio de voz tradicional, incluían algunos servicios de datos y otros servicios adicionales más sofisticados.

El sistema GSM tuvo tanto éxito que otras regiones voluntariamente lo adoptaron, fue así como se convirtió en el más popular del mundo con una cantidad alrededor de los dos billones de usuarios en más de 212 países. Debido a la gran presencia del sistema ha hecho que este estándar ofrezca el servicio de *Roamming* Internacional y movilidad entre diferentes operadores, posibilitando a los abonados hacer uso de su equipo en diferentes partes del

mundo, creando una economía de red que nunca antes otro sistema la había alcanzado.

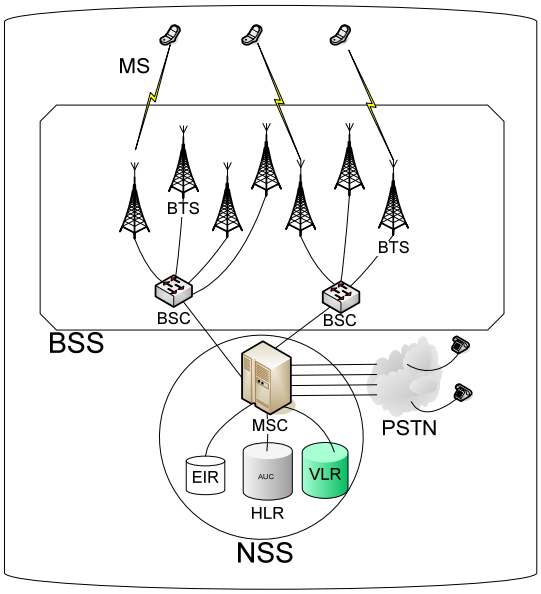
Las redes celulares de los operadores en Guatemala, no fueron la excepción, siendo GSM la tecnología que adoptaron por lo que se ha seleccionado esta tecnología para desarrollar la propuesta para desarrollo de estrategias de recuperación de centrales de telefonía celular.

3.2. Arquitectura

Una red celular se divide en tres partes importantes: la primera es el teléfono o cualquier otro dispositivo que se puede conectar a una red celular referido como una estación móvil o MS *(Mobile Station)*. La segunda es la responsable por el control del enlace de radio con el subsistema de estación base o BSS *(Base Station Subsystem)* y la tercera es la encargada de gestionar y conmutar las llamadas entre usuarios móviles subsistema de conmutación de red o NSS *(Network Switching Subsystem)*. A la red celular también se le conoce comúnmente como red móvil pública terrestre o PLMN *(Public Land Mobile Network)*.

La figura 3 ilustra los componentes de la arquitectura de una red celular.

Figura 3. Arquitectura GSM



Fuente: **GSM Alcatel.**
Pág. 5

EL MS es la combinación del equipo terminal o ME *(Mobile Equipment)* y los datos del abonado que guardan una tarjeta llamada módulo de identificación del abonado o SIM *(Subscriber Identity Module)*. Por lo que el MS es la unión del ME y el SIM.

3.2.1. Subsistema de estación base o BSS

Estación transceptor base o BTS *(Base Transceiver Station)*: un transmisor/receptor usado para transmitir/recibir señales de la sección de radio de la red.

Controlador de estación base o BSC *(Base Station Controller)*: controla las comunicaciones entre un grupo de BSTs y un único MSC.

Las BTSs y sus BSC controlantes a menudo se refieren colectivamente como el subsistema estación base o BSS *(Base Station Subsystem)*. Como se explicó antes, la topología celular de la red es un resultado del limitado espectro de radio. Para usar en forma eficiente el espectro de radio, se reutilizan las mismas frecuencias en celdas no adyacentes. Una región geográfica se divide en celdas. Cada celda tiene una BST que transmite datos a través de un vínculo de radio a las MSs dentro de la celda. Un grupo de BSTs están conectadas a una BSC. Un grupo de BSCs están a su vez conectadas a un centro conmutador móvil a través de vínculos de microondas o líneas telefónicas.

3.2.2. Conmutación de red o NSS

El subsistema de conmutación de red o NSS *(Network Switching Subsystem)* es el componente del sistema GSM que lleva a cabo las funciones de conmutación y administra las comunicaciones entre teléfonos móviles y la red pública de telefonía conmutada o PSTN *(Public Switched Telephone Network)*. Los operadores de telefonía móvil son los dueños y encargados de desarrollar este subsistema que permite a los teléfonos móviles comunicarse entre si y con otros teléfonos de la red de telefonía. La arquitectura se parece mucho a la de una central telefónica fija, pero hay funciones adicionales que son necesarios porque los teléfonos no están fijos en un solo lugar.

La central de telefonía celular o MSC *(Mobile Switching Center)* es el componente fundamental de la red la cual establece y mantiene las llamadas que se hacen en la misma. El MSC se conecta a la red de telefonía pública conmutada la cual deriva las llamadas a otras estaciones móviles o teléfonos terrestres. La red de telefonía pública conmutada o PSTN *(Public switched telephone network)* es la sección terrestre de la red.

También existe una superposición en la arquitectura de la red básica GSM para proporcionar servicios de conmutación de datos y se conoce como la red de servicios de radio generales por paquetes o GPRS *(General Packet Radio Services)*, la cual permite a los teléfonos móviles tener acceso a los servicios como WAP, MMS y acceso a Internet. Todos los teléfonos fabricados actualmente tienen capacidad para manejar ambos servicios, basados en paquetes y en circuitos, es por eso que la mayoría de los operadores celulares tienen una red GPRS adicional a la red principal GSM.

La central de conmutación móvil (MSC) es el nodo principal para la prestación de servicios GSM, responsable del enrutamiento de llamadas de voz y mensajes de texto (SMS), así como otros servicios propios de GSM como conferencias telefónicas y fax. El MSC establece y libera la conexión de extremo a extremo, se ocupa de la movilidad y el traspaso de las necesidades durante la llamada y se encarga de la carga y monitoreo en tiempo real de la cuenta de prepago.

En el sistema GSM de telefonía móvil GSM, en contraste con los sistemas analógicos anteriores, el servicio de fax y datos se envía codificado digitalmente directo al MSC. Estando en el MSC se re-codifica a una señal análoga.

Hay varios nombres diferentes para el MSC en diferentes contextos que refleja su rol complejo en la red, todos estos términos podrían referirse a la misma MSC, pero haciendo cosas diferentes en momentos diferentes.

El MSC *Gateway* (MSC-G) es el MSC que determina en cuál MSC se encuentra localizado el abonado que está siendo llamado. También sirve de interfase con la PSTN. Todas las llamadas de móvil a móvil y de PSTN a móvil son enrutadas a través del MSC-G. Es importante acotar que cualquier MSC puede proporcionar tanto la función de *Gateway* y de Visitado, sin embargo, algunos proveedores diseñan MSC de alta capacidad que no tienen conectadas BSS y los usan sólo para manejar llamadas. A estos MSC se les llama MSC *Gateway* por la cantidad de llamadas que ellos pueden manejar.

El MSC Visitado (MSC –V) es el MSC donde un abonado es localizado actualmente. El VLR asociado con este MSC tendrá la información del abonado.

El registro de localización del visitante es una base de datos temporal de los abonados que han recorrido el área donde se presta el servicio. Cada celda en la red es servida por un solo VLR, así un abonado no puede estar presente en más de un VLR a la vez.

Los datos almacenados en el VLR han sido recibidos del HLR o del MS en la práctica, por razones de desempeño la mayoría de los proveedores integran el VLR con el MSC-V y cuando no lo hacen es unido con el MSC vía una interfase propietaria.

El registro de localización de casa o HLR *(Home Location Register)* es una base de datos central que contiene detalles de cada abonado de telefonía móvil que es autorizado a usar la red de GSM. El HLR almacena los detalles de cada *SIM Card* expendida por el operador celular. Cada módulo de identificación del abonado o SIM *(Subscriber Identification Module)* tiene un identificador único llamado IMSI el cual es la llave primaria de cada registro en el HLR.

3.3. Funcionamiento

La siguiente descripción de una estación móvil haciendo una llamada a otra estación móvil explica mejor la tecnología subyacente en un sistema de red celular.

Una estación móvil inicia una llamada enviando un pedido de inicio de llamada a su estación base más cercana. Este pedido se envía en un canal especial, el canal de control inverso o RCC *(Reverse Control Channel)*. La estación base envía el pedido que contiene el número de teléfono de la parte llamada, al MSC. El MSC valida el pedido y usa el número para hacer una conexión a la parte siendo llamada a través de la PSTN. Primero se conecta a

él mismo al MSC de la parte que realiza la llamada, luego el MSC instruye a las estaciones base y móvil que colocó la llamada para cambiar a los canales de voz. La estación móvil que inició la llamada está entonces conectada con la estación llamada usando canales de voz hacia adelante o FVC *(Forward Voice Channel)* y canal de voz hacia atrás o BVC *(Backward Voice Channel)*.

Los pasos que tienen lugar cuando una estación móvil recibe una llamada entrante son como siguen:

Las estaciones móviles analizan continuamente el canal de control hacia adelante o FCC *(Forward Control Channel)* por señales de búsqueda desde las estaciones base. Cuando un MSC recibe un pedido para una conexión a una estación móvil en su área, envía un mensaje de difusión a todas las estaciones base bajo su control. Este contiene el número de la estación móvil que está siendo llamada. Las estaciones base luego emiten el mensaje en todos los canales de control hacia delante (FCC). La estación móvil correcta reconoce la búsqueda, identificándose en el canal de control inverso (RCC). El MSC recibe el reconocimiento a través de la estación base e instruye a las estaciones base y móvil a cambiar a un canal de voz sin usar. Se transmite entonces un mensaje de datos sobre el FVC que le indica al teléfono móvil que suene.

Los pasos explicados arriba suceden lo suficientemente rápido como para que el usuario no experimente ninguna demora perceptible entre el pedido de inicio de una llamada y su establecimiento.

3.4. Dimensionamiento

El objetivo de dimensionar el hardware, es elegir la cantidad correcta para el cumplimiento del grado de las necesidades de servicio. El sobredimensionamiento es costo-ineficiente para el operador que conduce al

uso ineficiente de los equipos. El dimensionar en menor porcentaje dará lugar a la congestión, los retrasos y deterioro del desempeño del servicio.

La entrada al dimensionamiento son los datos de abonados, el grado de las necesidades de servicio y el desempeño o límites del equipo. Con estos datos es posible calcular la cantidad de hardware necesario.

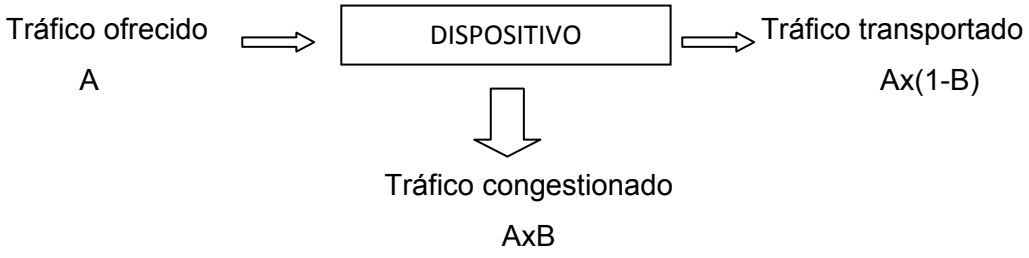
En el MSC existen dos tipos de sistemas: los de pérdida y de demora. Un sistema de pérdida es un sistema en el que se desconecta al usuario si no existe un dispositivo libre que se puede asignar. Un sistema de demora o retardo es un sistema en el que se pone al usuario en cola si no hay un dispositivo libre. Estos dos sistemas requieren fórmulas diferentes para calcular el número requerido de los dispositivos.

3.4.1. Teoría de tráfico telefónico

Erlang es la unidad estándar de tráfico telefónico. Erlang corresponde al uso promedio de un grupo de dispositivos. Si el tráfico de un dispositivo es de 0.5 Erlang, por ejemplo, el uso medio del dispositivo es de 50%.

Para todos los dispositivos que no están libres de la congestión, se acepta que una cierta proporción B de las llamadas son pérdidas. Si ofrecemos un tráfico A (en Erlang) a un dispositivo, BxA será el tráfico que se perdiera. Esto significa que el tráfico transportado, es decir, el tráfico que se sirve por el dispositivo, es (1- B)xA.

Figura 4. Conceptos de tráfico



Fuente: McKeever, Susanne.
MSC hardware dimensioning.
Pág. 14

La notación que se usará es:

λ = Intentos de llamada en la hora pico o BHCA

h = Tiempo promedio de llamada, en segundos

A = Tráfico total hacia un dispositivo, Erlang

B_n = Probalidad de ocupación, carga normal

B_h = Probalidad de ocupación, carga alta

La relación entre tráfico en Erlang y BHCA (expresada en llamadas por hora) es:

$A = \lambda \times h / 3600$

El tráfico total hacia el dispositivo junto con el grado de servicio o GoS *(Grade of Service)* servirá de entrada para el cálculo del número de dispositivos requerido.

3.5. Topología *Stand Alone*

3.5.1. Sistemas de pérdida

Un sistema de pérdida es un sistema donde se rechaza al usuario si no se encuentra un dispositivo disponible.

Para la mayoría de los dispositivos en el MSC, la primera fórmula de Erlang puede ser usada, dando el tráfico (A) como una función de el número de dispositivos (n) y la probabilidad de bloqueo ($E_{1,n}$), donde la probabilidad de bloqueo tiene seis valores constantes entre 0.00001 y 0.01. La serie de valores para el número de dispositivos son limitados a ciertos valores guía, en el rango de 1000 a 6000. Todos los valores intermedios pueden ser determinados con suficiente exactitud por la interpolación lineal:

$$n = n_1 + \frac{A - A_1}{A_2 - A_1}. (n_2 - n_1)$$

Donde:

n = Número de dispositivos para el tráfico A

n_1 = Número de dispositivos para el menor tráfico cercano a A

n_2 = Número de dispositivos para el mayor tráfico cercano a A

A = Tráfico ofrecido al dispositivo

A_1 = El tráfico mayor más cercano en la tabla

A_2 = El tráfico menor más cercano en la tabla.

También en Internet se pueden encontrar calculadores Erlang.

Los requerimientos que se deben llenar para usar la primera fórmula de Erlang son:

1. Sistema de pérdida pura.

2. Completa disponibilidad del grupo, cualquier dispositivo puede ser alcanzado por cualquier llamada.
3. El proceso de llegada es Poisson, es decir el número de llamadas es grande y cada llamada es independiente de las otras.

3.5.2. Sistemas de retardo

Un sistema de demora se caracteriza por el hecho de que haya una cola de espera *(buffer)* donde las llamadas se ponen si ningún dispositivo está disponible. Las llamadas que llegan cuando hay llamadas en cola se dice que encuentra la congestión y se ven obligados a esperar. Contrariamente al sistema de pérdida, estas llamadas sin éxito no se descartan, se retrasan solamente. El tiempo que transcurre entre el instante de llegada de la llamada y el instante en el cual se asigna un llamada a un dispositivo (es decir, el tiempo dedicado esperando en una cola) se conoce como el tiempo de espera. La formación de una cola es la principal característica que distingue a los sistemas de demora de los sistemas de pérdida.

Los supuestos son:

- Plena disponibilidad del grupo; cualquier dispositivo puede ser alcanzado por cualquier llamada.
- El proceso de llegada es de Poisson, es decir, el número de llamadas es grande y las llamadas son independientes entre sí.
- Las llamadas que llegan cuando todos los dispositivos están ocupados forman una cola y esperan en orden la llegada de los dispositivos libres.

Con estos requerimientos completos la segunda fórmula de Erlang o Fórmula C de Erlang o Fórmula de Retardo de Erlang puede ser usada.

$$E_{2,n}(A) = \frac{n.\ E_{1,n}(A)}{n - A\ [\ 1 - E_{1,n}(A)]}$$

$P(w>t) = E_{2,n}(A)\ e^{-(n-A)t/h}$

$P(w>t)$ = Probabilidad que el tiempo de espera w exceda los t segundos

$E_{1,n}(A)$ = Probabilidad de bloqueo

$E_{2,n}(A)$ = Probabilidad de espera

n = Número de dispositivos

A = Tráfico total ofertado

h = Tiempo de llamada promedio (segundos)

3.5.3. Carga normal y alta.

El dimensionamiento se basa en el requerimiento de servicio o grado de servicio requerido, en los valores de intensidad del tráfico a la hora de mayor carga de tráfico y en el valor de pronóstico de la intensidad hasta el siguiente dimensionamiento. La intensidad se mide durante la hora pico del día y como promedio durante un número de días, para evitar valores excepcionales.

En el dimensionamiento de tráfico los términos de carga normal y alta son usados de acuerdo a la recomendación ITU-T E.500. A continuación se presenta la definición para grupos de circuitos:

	Intensidad de tráfico cursado
Carga Normal	El promedio de los 30 días de más alto tráfico durante un período de 12 meses (Tráfico de la hora pico).
Carga Alta	El promedio de los cinco días de más alto tráfico en el mismo período usado en el cálculo de carga normal (Tráfico en la hora pico).

Si el criterio anterior no es aplicable entonces la razón entre carga normal y alta es 1.2 (identificado como Rh) para la intensidad del tráfico de acuerdo a las recomendaciones ITU-T. En la ITU-T E.500 se puede encontrar recomendaciones para diferentes métodos de medición de tráfico.

Si se usa el tráfico de carga alta como entrada, el factor 1.2 no es necesario en los cálculos. El factor es usado solamente si se asume que el valor del tráfico ingresado es el tráfico de carga normal.

En EE.UU. los términos siguientes se pueden utilizar en lugar de los anteriores.

	Definición
Carga HDBH	El día que tiene el tráfico más grande durante la hora pico (basado en la estadística del último año) es designado "El día pico" del año y la hora correspondiente la hora pico del día pico o HDBH (*High Day Busy Hour*). El nivel de tráfico es llamado la carga HDBH.
Factor YYHDCV	La variabilidad de llamadas del día mas alto de un año al otro año o YYHDCV (*Year to Year High Day Call Variability*). Este factor provee protección contra la variabilidad del volumen de llamadas del HDBH de un año a otro.

Si se usa la carga HDBH como entrada, el factor Rh con valor 1.2 no es usado, en lugar de se usa el factor YYHDCV con un valor de 1.04.

Hay un número del requerimiento de grado de servicio, que debe cumplirse. A efectos del dimensionamiento hay dos requisitos de particular interés:

- las probabilidades de bloqueo (es decir la congestión).
- las probabilidades de retrasos que exceden cierto tiempo.

Un ejemplo de lo primero es la probabilidad de congestión cuando se llama a un abonado. De la última podría ser “la demora por conexión”.

3.5.4. Modelo de tráfico

El dimensionamiento de una central de telefonía celular depende en gran medida de las características específicas del tráfico móvil que maneja. También depende de la función actual de la MSC. Un nodo MSC tiene la capacidad de funcionar como un MSC/VLR/GMSC/TSC/SSF/SMS-GMSC. El dimensionamiento de la MSC también depende de si el MSC contiene la funcionalidad MGW o no, ya que tiene un gran impacto en los resultados de dimensionamiento.

El nodo MSC comprende el manejo de tráfico hacia y desde otros MSCs, RNC, BSC, SSP, y la red fija. Además, el tráfico de señalización a HLR, EIR y FNR que ocupará. Específicamente la función del GMSC es la interrogación al HLR y dependiendo de la información recuperada del HLR, el enrutamiento de la llamada a la MSC o la redirección de la llamada al buzón de voz, etc.

La función de MSC / VLR dentro del propio nodo se refiere a menudo a la función como MSC. Específicamente la función de MSC es el establecimiento de llamadas hacia y desde las BSCs y la redirección de llamadas que se hacen cuando, por ejemplo, no hay respuesta o está ocupado. El flujo de tráfico hacia, desde y dentro de un MSC es, pues, un asunto complicado.

Tenga en cuenta que la funcionalidad HLR se puede integrar en el nodo MSC, o puede haber un nodo independiente de HLR en la red. Esto se aplica a SCP también. La SSP o el punto de servicio de conmutación *(Service Switching Point)* no puede ser un nodo independiente, sólo en combinación con un MSC.

3.5.4.1. Parámetros de entrada necesarios para el dimensionamiento

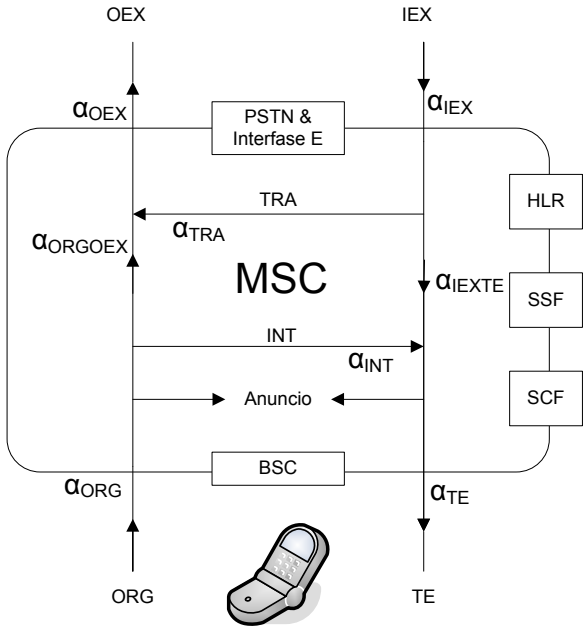
Una cuestión importante para los cálculos de dimensionamiento de tráfico es la disponibilidad de datos de entrada para el usuario. La fórmula más precisa y exacta para el dimensionamiento de los equipos es inútil si el usuario no tiene acceso a los datos de entrada. Los datos utilizados aquí son basados en información que puede estar disponible relativamente fácil a través de las estadísticas de los MSCs.

Un adecuado dimensionamiento necesita una cantidad importante de datos de entrada y es concebible que no se puede tener toda esta información disponible. Para evitar este problema, se han propuesto valores guía para parámetros donde es posible. Estos valores se han obtenido principalmente en datos de campo registrados por varios MSC en Europa Occidental. Es, sin embargo, fuertemente recomendado que siempre que sea posible, los valores reales propios deben ser utilizados en lugar de estos valores orientativos, ya que los perfiles de tráfico pueden variar y se relacionan al dimensionamiento en un grado muy grande.

3.5.4.2. Distribución del tráfico

En la Figura 5 se muestra un diagrama esquemático del flujo del tráfico dentro de la MSC. Esto representa el tráfico de varias interfases. El cuadro punteado representa al MSC. El HLR es puesto al borde del cuadro, ya que puede ser integrado o independiente.

Figura 5. Flujo de tráfico



Fuente: Susanne Mckever**.**
MSC hardware dimensioning.
Pág. 27

La interfase E sirve de unión con la PSTN, otros MSC y el correo de voz.

El tráfico en las interfases principales en el MSC (αORG, αTE, αOEX, αIEX) se presenta en Erlang por abonado. Puesto que los valores pueden diferir sustancialmente entre las partes entrantes y salientes se indican por separado. Los flujos de tráfico interno dentro de la MSC también se indican: αINT representa el tráfico de móvil a móvil en el mismo MSC, αTRA el tráfico de tránsito de entrada externa (IEX) para salida externa (OEX), etc.

Las llamadas se pueden redirigir al GMSC, por ejemplo el desvío de llamadas incondicional y reenvío de llamada de abonados desconectados (si esta información se proporciona en la interrogación del HLR). Algo de este tráfico podría terminar internamente (abonados desconectados) como por

ejemplo un anuncio; el resto del tráfico se ofrecerá de nuevo para el intercambio por el desvío de llamadas. Se asume que el tráfico redireccionado al GMSC, α_{RE1} es un porcentaje del tráfico originario α_{ORG} y el tráfico externo entrante α_{IEX}.

En el MSC, cuando la llamada móvil es desconectada porque el abonado está ocupado o no responde, el tráfico αRE2 se redirige a las máquinas de anuncios, o en caso de desvío de llamadas se ofrece de nuevo al MSC. Aquí se asume que αRE2 terminará en la máquina de anuncios solamente.

3.5.4.3. Datos de entrada necesarios

Los datos de entrada necesarios para el dimensionamiento se enumeran a continuación.

Parámetros de tráfico básicos		Valor Guía
R_h =	Proporción de carga alta de tráfico a carga normal de tráfico	1.200
B_h =	Probabilidad de bloqueo, alta carga	0.001

Datos relacionados con número de abonados

N_{GSM} = Número de abonados de GSM registrados en VLR

Datos del tráfico			Valor Guia
α_{ORG_G}	=	Tráfico originado por abonado en la interfase MSC-BSC (mE)	9.6
α_{TE_G}	=	Tráfico terminante por abonado GSM en la interfase MSC-BSC (mE)	6.4
$\alpha_{INT\_G}^{1}$	=	Tráfico interno por abonado GSM en la interfase	

		MSC-BSC (mE)	0.192
α_{TRA}	=	Tráfico de tránsito de la PSTN por abonado (mE)	6.4
α_{IEX_G}[2]	=	Tráfico externo entrante por abonado GSM en la interfase PSTN (mE)	6.7
α_{OEX_G}[3]	=	El tráfico externo saliente por abonado GSM en la interfase PSTN	9.3
α_{DC_G}	=	Tráfico por abonado GSM, llamadas de datos (mE)	0.5
P_{IEX_PSTN}	=	Proporción del tráfico externo entrante (α_{IEX}) que es tráfico entrante PSTN	0.50
P_{OEX_PSTN}	=	Proporción del tráfico externo saliente (α_{OEX}) que es el tráfico PSTN	0.59
P_{IEX_MSC}	=	Proporción de tráfico externo entrante (α_{IEX}) que es el tráfico entrante de otros MSCs	0.50
P_{OEX_MSC}	=	Proporción del tráfico externo saliente (α_{OEX}) que es el tráfico saliente de otros MSCs	0.41
P_{OEX_DA}	=	Proporción del tráfico externo saliente (α_{OEX}) que es el tráfico de acceso directo	0
P_{RE1}	=	Proporción del tráfico entrante (α_{ORG} + α_{IEXTE}) que es reenviado al GMSC	0.05
P_{RE2}	=	Proporción del tráfico móvil terminante (aprox. 35% del α_{TE}) que es enviado a la MSC (al correo de voz)	0.1
H	=	Promedio de tiempo de una llamada (segundos)	80
h_{ORG}	=	Promedio de tiempo de retención de una llamada originante MSC- BSC (segundos)	75
h_{TE}	=	Promedio de tiempo de una llamada terminada MSC-BSC (segundos)	90
h_{IEX_PSTN}	=	Promedio de tiempo de una llamada entrante MSC-PSTN (segundos)	58

h_{OEX_PSTN} =	Tiempo promedio de una llamada saliente MSC-PSTN (segundos)	78
h_{IEX_MSC} =	Tiempo promedio de una llamada entrante MSC-MSC (segundos)	90
h_{OEX_MSC} =	Tiempo promedio de una llamada saliente MSC-MSC (segundos)	90
h_{VM} =	Tiempo promedio de un mensaje de voz (segundos)	30
h_{DC} =	Tiempo promedio de una llamada de datos (segundos)	600

Nota 1 – El tráfico interno α_{INT} se asume sea del 2% del tráfico originante α_{ORG}.

Nota 2 – El tráfico externo entrante α_{IEX} es la suma del tráfico en tránsito α_{TRA} y el tráfico externo entrante α_{IEXTE}. El valor guía es válido si $\alpha_{TRA} = 0$, de otra manera el α_{TRA} tiene que ser agregado.

Nota 3 – El tráfico externo saliente α_{OEX} es la suma del tráfico en tránsito α_{TRA} y el tráfico originando α_{ORGOEX}. El valor guía es válido si $\alpha_{TRA} = 0$, de otra forma α_{TRA} se tiene que agregar.

Note que el tráfico redireccionado al GMSC y MSC es despreciado en el cálculo de tráfico de las interfases principales descritas anteriormente.

Datos de traspasos

N_{H2} =	Promedio del número traspasos inter-RNC e intra-MSC por llamada	0.10
N_{H3} =	Promedio del número de inter-MSC traspasos por llamada	0.05
N_{H4} =	Promedio del número traspasos intra-MSC e inter-BSC por llamada	0.10

Datos de la actualización de ubicación

$N_{LU,N}$ = Promedio del número de actualizaciones de ubicación inter-MSC (nuevo registro) por abonado durante la hora pico

$N_{LU, A,R}$ = Promedio del número de actualizaciones de ubicación – ligados de IMSI (antes del registrado de abonado) por abonado durante la hora pico

$N_{LU,D}$ = Promedio del número de actualizaciones de lugar. Separación de IMSI por abonado durante la hora pico

$N_{LU,L}$ = Promedio del número de actualizaciones de ubicación intra-MSC (tipo normal, nuevo LAI) por abonado durante la hora pico

$N_{LU,P}$ = Promedio del número de registros periódicos por abonado por hora

N_{LU} = Promedio del número de actualizaciones de ubicación por abonado durante la hora pico

Datos de las características		Valor Guía
N_{SS} =	Promedio del número de llamadas independientes a procedimientos de servicio suplementario por abonado durante la hora pico	0.05
N_{SMST} =	Promedio del número de mensajes de texto terminados en móvil, por abonado durante la hora pico	0.25
N_{SMSO} =	Promedio del número de mensajes de texto originados en móvil, por abonado durante la hora pico	0.05
N_{SP} =	Promedio del número de operaciones de parámetro enviadas, por abonado durante la hora	

	pico	0.14
N_{ST} =	Número de transacciones sucesivas sin chequeo de IMEI	5
N_{SO} =	Número de operaciones sucesivas sin autenticación	5
N_T =	Número de *triplets* / *quintets* buscados a la vez	3
P_{CFU} =	Proporción del tráfico enviado a la GMSC (α_{RE1}) que es incondicionalmente enviado a un número de C	0.67
P_{AST_GMSC} =	Proporción del tráfico enviado a la GMSC (α_{RE1}) que termina con un anuncio	0.33
P_{CFC} =	Proporción del tráfico enviado a la MSC (α_{RE2}) que es enviado condicionalmente a un número de C	0
P_{AST_MSC} =	Proporción del tráfico enviado a la MSC (α_{RE2}) que termina con un anuncio	1

Troncal de Datos

A =	Tráfico promedio por troncal de voz durante la hora pico (Erlang)	0.8

Datos de la Arquitectura de Red

MSC = Número de otros MSCs conectados a la MSC

GMSC = Número de GMSCs conectados a HLR

BSC = Número de BSCs adjuntos a la MSC

También es importante saber si el HLR esta integrado o no al MSC. La otra pieza importante de información es el número de rutas a la diversidad de otros nodos (MSCs, BSCs, PSTN etc.).

3.6. Topología en espera o *Standby*

3.6.1. Características de la topología en espera *(Standby)*

Una solución diseñada para proveer redundancia a nivel del NSS es la topología en espera o *Standby*. La característica de esta topología es que está definida a nivel del hardware necesario para que cada MSC tenga una copia pasiva o en espera, físicamente son dos equipos diferentes que pueden estar en la misma ubicación o en diferente ubicación. Cada BSC en el área de servicio está conectado a un sólo de MSC, en el caso de falla de este MSC, entonces debe existir un proceso manual para cambiar la conexión de la BSC hacia el MSC pasivo, que en ese momento se convierte en activo.

Este es el tipo de configuración que se uso mucho durante la década de los 80´s y 90´s como parte de los planes de recuperación que implementaron las compañías pioneras en este campo.

Si esta topología se implementa incluyendo la redundancia geográfica, es decir que los pares de MSC estén separados al menos 20 Km. entonces presenta un alto nivel de confiabilidad en cuanto a la recuperación en caso de desastres. En contraposición presenta la característica de ser muy ineficiente en cuanto al costo beneficio, porque requiere de tener equipos sin uso en espera de una falla, que eventualmente pueden llegar a ser obsoletos, además que necesita de la implementación de un plan de mantenimiento y pruebas que aseguren que el equipo esté listo para ser usado cuando se necesite, de lo contrario puede presentar la falsa impresión de tener una solución para recuperación que cuando se necesite no esté disponible. Por último en cuanto a costo representa un aumento en la inversión inicial cuando se compra un nuevo MSC, por siempre se debe incluir su pareja, además que los costos de la transmisión aumentan también porque se necesita tener la conexión para ambos MSC desde cada BSC que atienden.

3.6.2. Dimensionamiento del MSC en espera

Para el dimensionamiento de este tipo de topología se usan los mismos conceptos revisados en la sección 3.4 dimensionamiento de este trabajo, porque la solución *Standby* es realmente un duplicado de la *Stand Alone* que se debería ubicar separada geográficamente. El objetivo de dimensionar el hardware, es elegir la cantidad correcta para el cumplimiento del grado de las necesidades de servicio. El sobredimensionamiento es costo-ineficiente para el operador, lo que conduce al uso ineficiente de los equipos. El dimensionar en menor porcentaje dará lugar a la congestión, los retrasos y deterioro del desempeño del servicio.

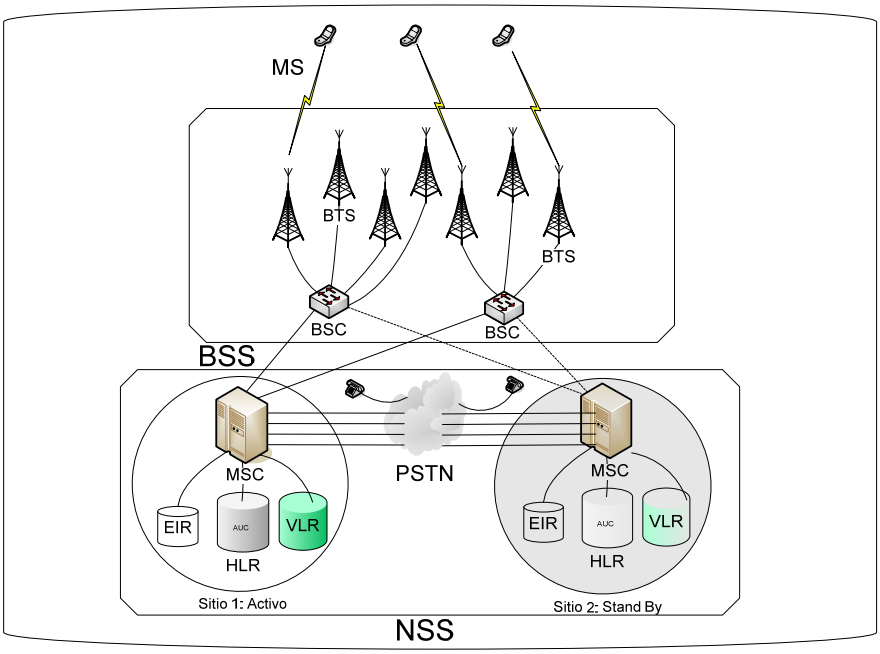
Los datos importantes para definir el dimensionamiento son el número de abonado, el grado de las necesidades de servicio y el desempeño o límites del equipo, además del porcentaje de la capacidad total que se desea respaldar con los MSC en espera, con estos datos es posible calcular la cantidad de hardware necesario utilizando el mismo método expuesto en la sección 3.5.4 de este trabajo.

3.6.3. Configuración de la topología en espera

A continuación en la figura 6 se muestra un diagrama de la topología de MSC en espera, en la cual se puede observar cómo en esta topología se agrega un sitio alterno a nivel del NSS en donde se instala una copia de cada uno de los equipos que se tienen en el sitio inicial, la capacidad de cada uno de estos equipos de los criterios vistos en la sección anterior, sin embargo es necesario instalar al menos un equipo de cada categoría, es decir MSC, EIR, AUC y VLR, para asegurar el funcionamiento de la red en caso de falla en el

nodo inicial. Además la transmisión debe estar instalada previamente para recuperar en el menor tiempo posible.

Figura 6. Topología de MSC en espera



Fuente: Susanne Mckever**.**
MSC hardware dimensioning.
Pág. 27

El cambio del sitio activo al sitio en *Standby* implica configuraciones manuales que deben realizarse en el momento que se necesiten, por ejemplo el cambio de direccionamiento desde las BSC hacia MSC inicial se debe cambiar al MSC alterno. Otro cambio importante es el de la conexión del PSTN que debe cambiarse al MSC alterno desde el original. Se debe tener especial cuidado de que la configuración y parametrización del MSC alterno sea idéntica al MSC original para asegurar la continuidad de la operación. Para reducir el

tiempo de cambio de un sitio activo a un sitio pasivo es fuertemente recomendado realizar secuencias comandos que se actualicen y prueben frecuentemente, este tipo de procedimiento tiene un impacto importante sobre el tiempo de recuperación.

3.7. Topología en grupo o *in Pool*

Una solución diseñada para proveer redundancia geográfica y alta disponibilidad para el NSS es la topología de uso común o en *Pool*. Una topología en *Pool* es una serie de BSCs servido por una serie de MSCs. Cada BSC en el área de servicio está conectado a cada uno de MSC en el *Pool* en una conexión de malla.

Cuando se necesita más capacidad, más nodos MSC se pueden añadir al *Pool* sin la necesidad de cambiar la configuración de red (mover BSC de un MSC a otro) y así evitar un montón de esfuerzo de configuración y las perturbaciones del tráfico. Los nuevos nodos MSC deben ser conectados a todos los BSC respectivamente en una configuración de malla. Los nodos BSC en el área *Pool* son informados para tomar en cuenta el nuevo MSC en su procedimiento de distribución del tráfico.

La característica de MSC en *Pool* es compatible con GSM. El MSC en función del grupo de apoyo de la MSC es compatible con la 3GPP Intra conexión de los nodos de RAN a múltiples nodos de CN (TS 23.236) para GSM/WCDMA. Eso significa que podría trabajar junto a nodos de diferentes proveedores (MSC o BSC) en el *Pool*.

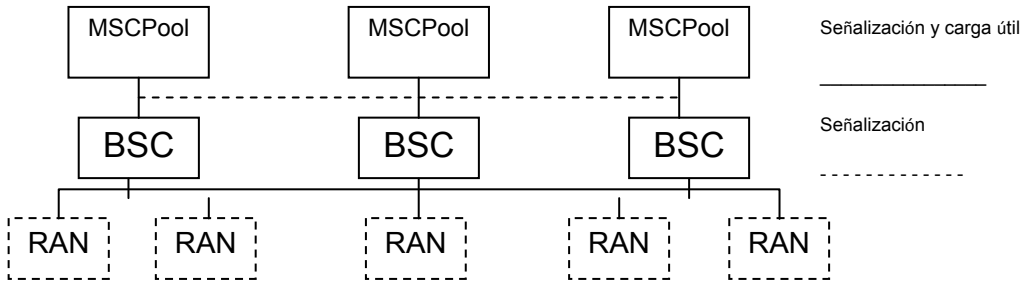
Un área *Pool* es un grupo de nodos MSC compartiendo en paralelo el tráfico generado de una y solamente una área MSC. Un nodo BSC perteneciente a una zona del *Pool* MSC está conectado a todos los nodos de MSC en el *Pool* MSC relacionados.

PRINCIPALES IMPULSORES DE LA TOPOLOGÍA EN *"POOL"*

CONDUCTORES	***POOL***
• Rápido crecimiento de abonados y tráfico	✓ Capacidad de escalamiento ✓ Adición de nodos simplificada
• Mejor utilización de la capacidad	✓ Agrega más del 25% de la capacidad
• Redundancia de la red	✓ Redundancia geográfica ✓ Carga de la red distribuida

El área de servicio en *Pool* se basa en el estándar 3GPP de conexión intra dominio de los nodos BSS a múltiples nodos NSS y es conocida también como A-Flex para GSM.

Figura 7. Arquitectura MSC en *Pool*



Fuente: **MSC *Pool*.**
Pág. 6

3.7.1. Características del servicio en *Pool*

- ✓ *Pool* por área de servicio.
- ✓ Todos los BSC conectados a todos los MSC en el área *Pool*.
- ✓ El MSC que sirve es independiente de la ubicación del abonado.

La reducción de la carga en el servicio *Pool*, se debe a las actualizaciones de ubicación de HLR y las entregas Inter-MSC dentro del *Pool* mostrando que la capacidad estará disponible para el resto del tráfico; no hay ninguna llamada disminuyendo debido a otras entregas MSC; disminución de la carga en HLR, debido a las actualizaciones de localización, todo esto dando como resultado positivo el aumento de capacidad previsto 5 - 10%.

La carga es distribuida equitativamente por BSC entre el MSCs *Pool* basado en la capacidad disponible en la MSC. El tamaño de *Pool* recomendado es de 4-8 MSCs. Dentro de sus beneficios están el uso eficiente de la capacidad disponible de la red. No coinciden las horas pico. Aumenta en 15% la capacidad de utilización de la red, la misma puede ser mayor de acuerdo a las necesidades de ambos BSC y MSCs del cual se obtienen beneficios como la capacidad simplificada de MSC, no es compleja, ni costosa.

Un MSC del *Pool* no tiene conocimiento sobre el comportamiento de los nodos MSC, tanto si pertenecen al mismo grupo de MSC o no. El concepto de MSC *Pool* es aplicable principalmente para la BSC, como el BSC puede ver un *Pool* de nodos de MSC.

Las principales ventajas con la función de MSC *Pool* son las siguientes:

- o Mejora de la escala de la capacidad debido a la carga de compartir, como MSC se puede agregar al servicio *Pool* del área MSC.
- o Aumentar la capacidad de abonados en una red que actúa mediante la adición de un nodo MSC sin mayores repercusiones en el BSC / RNC de reconfiguración (simplificado los proyectos de expansión, la

simplificación de funcionamiento y procedimientos de mantenimiento).

- La principal fuerza impulsora de la introducción de una red de GSM combinados / WCDMA es la mejora de la escalabilidad, ISP, y el costo de propiedad. Debe ser fácil para añadir nuevos MSC en el *Pool* y que debe ser fácil de tomar MSC fuera de servicio, sin impacto en el tráfico.
- Aumentar la disponibilidad del servicio. Si un MSC falla, todos los abonados situados en el MSC se encaminan a otros nodos MSC de servicio de la misma zona del *Pool* por el BSC y RNC de la función de enrutamiento alternativo.
- Reducir la señalización del tráfico en la red principal. De señalización, actualización de la ubicación y entrega / reubicación SNRE entre los nodos MSC con un *Pool* MSC que puede reducirse.
- Funcionamiento simplificado y procedimientos de mantenimiento, como todos los nodos tienen los mismos datos del RAN relacionados.
- Permite el balanceo de carga por la red de acceso de radio.

Limitaciones

- Lista propia de NRI es una estructura de datos en el MSC y tiene un límite de ocho valores.
- Un máximo de 2048 grupos de vecinos MSC se pueden definir en el MSC.
- Un máximo de 16 MSCs puede ser definido en un *Pool* de MSC.

3.7.2. Dimensionamiento del MSC en *Pool*.

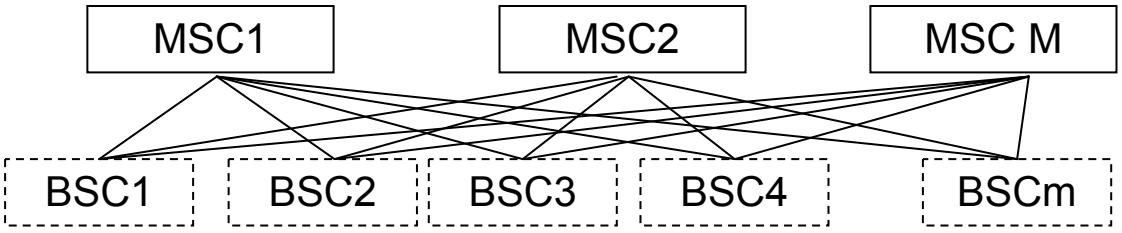
La funcionalidad de MSC en *Pool* permite a los operadores a distribuir el número de abonados de manera más eficiente en la red de tal manera que en un determinado momento una MSC que está muy cargado y otros MSC que no están tan cargados se pueden redistribuir los abonados entre los diferentes MSC automáticamente, esto se realiza de acuerdo a un parámetro de BSC (PAC). Otra ventaja de esta característica es que el operador puede optar por tener redundancia de MSC en caso de fallo de un MSC. En la siguiente sección se considera que un máximo de un MSC podría fallar y que otra MSC del grupo soportará a los abonados de la fallida MSC, lo que les permite continuar con el servicio.

3.7.3. Configuración

El dimensionamiento del hardware para MSC que pertenece a un *Pool* definido es muy similar a los presentados previamente. Sin embargo, hay algunas cosas que deben tomarse en consideración:

1. Todas las BSC del *Pool* deben ser conectadas a todas las MSC del mismo *Pool*, en una estructura de malla. Esto requerirá de más definición de rutas en los MSCs.
2. En caso se desee redundancia para la falla de una sola MSC, entonces las otras MSCs que están disponibles deberían tener capacidad de tomar todo el tráfico perdido sin presentar congestión.
3. La frecuencia de unos pocos casos de tráfico se reducirá (inter MSC *handover*, actualización de localización), mientras otros casos incrementarán su frecuencia (actualización de localización intra MSC, intra MSC *handover*).

Figura 8. Arquitectura MSC en *Pool*



Fuente: McKeever, Susanne.
MSC hardware dimensioning.
Pág. 145

Se asume que se conoce el tráfico entre cada BSC y cada MSC, y que se desea la redundancia de una sola MSC en caso de falla. Dividiendo este tráfico entre el promedio de uso por abonado, se obtiene el número de abonados de cada BSC que están registrados en cada MSC.

$Nj_{BSCi} = A_{BSCi\text{-}MSCj} / (\alpha_{ORG} + \alpha_{TE})$

Entrada:

Nj_{BSCi} = Número de abonados del BSCi registrados en el VLRj

M = Número de MSCs definidas en el *Pool*

Intermedio:

$N_{MSChigh,BSCi}$ = Número de abonados del BSCi registrados en la MSC con los números más altos de abonados

$N_{MSC2ndhigh,BSCi}$ = Número de abonados del BSCi registrados en la MSC con los segundos números más altos de abonados

$N_{MSCj,BSCi,red}$ = El número adicional de abonados del BSCi que pudieran registrarse en MSCj en caso de una falla en el MSC.

Resultado:

$N_{tot,\ MSCj,\ BSCi,red}$ = Número dimensionado de abonados del BSCi que podrían ser registrados en MSCj, en caso de falla redundante en el MSC

$N_{tot,\ MSCj,\ red}$ = Número dimensionado de abonados que podrían ser registrados en MSCj, en caso de falla redundante del MSC

Procedimiento:

1. Calcular el número de abonados adicionales de cada BSC que deben ser manejados por cada MSC pertenecientes al *Pool*

$$N_{MSCj,BSCi,red} = \frac{N_{MSChigh,BSCi}}{M} \cdot N_{MSCj,\ BSCI} \quad \text{if } MSCj \neq MSChigh$$

2. Calcular el número dimensionado de abonados del BSCi registrados en MSCj: Un 10% de margen del número total de abonados para manejar temporalmente el tráfico desbalanceado en el *Pool* MSC es recomendado e incluido en la siguiente fórmula:

$$N_{tot,\ MSCj,\ BSCi,\ red} = N_{MSCj,\ BSCi} + 0.1 \times N_{MSCj,\ BSCi} + N_{MSCj,\ BSCi,\ red}$$

Nota:

En caso que la redundancia MSC no se requiera, la fórmula será así:

$$N_{tot,\ MSCj,\ BSCi} = N_{MSCj,\ BSCi} + 0.1 \times N_{MSCj,\ BSCi}$$

Nota:

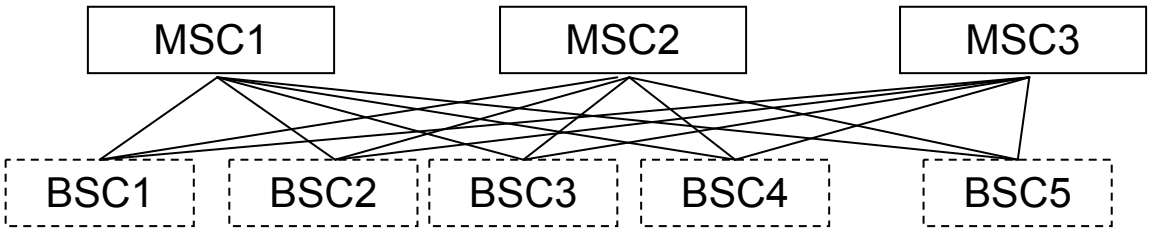
El valor guía para el número de inter-MSC e intra-MSC por traspasos de llamadas y de número de actualizaciones de localización por abonado en las horas ocupadas se modificará debido a la MSC en la *Pool*. El valor dependerá en gran medida de la configuración de la red y el tráfico de usuarios registrados.

Se pueden usar valores guía:

N_{H3pool} =	Número de traspasos del inter-MSC por llamada	0.01
N_{H4pool} =	Número de traspasos intra-MSC, entre BSC por llamada	0.14
$N_{LU,Npool}$ =	Número promedio de lugares actualizados de inter-MSC (nuevo registro) por abonado durante la hora pico	0.06
$N_{LUC,Lpool}$ =	Número total de lugares entre MSC actualizados por abonados durante la hora pico	0.52

A continuación se presenta un ejemplo tomando en consideración un conjunto de 3 de MSC, que ha conectado 5 de BSC.

Figura 9. Ejemplo de arquitectura MSC en *Pool*



Fuente: McKeever, Susanne.
MSC hardware dimensioning.
Pág. 145

En este capítulo se asume el número de abonados para cada BSC que están registrados en cada MSC y la redundancia para cada MSC es deseada.

Entrada

$N1_{BSC1}$ = Número de abonados del BSC1 registrados en el VLR1 = 100,000

$N1_{BSC2}$ = Número de abonados del BSC2 registrados en el VLR1 = 120,000

$N1_{BSC3}$ = Número de abonados del BSC3 registrados en el VLR1 = 80,000

$N1_{BSC4}$ = Número de abonados del BSC4 registrados en el VLR1 = 90,000

$N1_{BSC5}$ = Número de abonados del BSC5 registrados en el VLR1 = 140,000

N1 = Número de abonados registrados en el VLR1 = 530,000

N2BSC1 = Número de abonados del BSC1 registrados en el VLR2 = 100,000

N2BSC2 = Número de abonados del BSC2 registrados en el VLR2 = 200,000

N2BSC3 = Número de abonados del BSC3 registrados en el VLR2 = 50,000

N2BSC4 = Número de abonados del BSC4 registrados en el VLR2 = 70,000

N2BSC5 = Número de abonados del BSC5 registrados en el VLR2 = 60,000

N2 = Número de abonados registrados en el VLR2 = 480,000

N3BSC1 = Número de abonados del BSC1 registrados en el VLR3 = 130,000

N3BSC2 = Número de abonados del BSC2 registrados en el VLR3 = 140,000

N3BSC3 = Número de abonados del BSC3 registrados en el VLR3 = 170,000

N3BSC4 = Número de abonados del BSC4 registrados en el VLR3 = 50,000

N3BSC5 = Número de abonados del BSC5 registrados en el VLR3 = 60,000

N3 = Número de abonados registrados en el VLR3 = 550,000

Intermedio

$N_{MSCj,BSCi,red}$ = Número adicional de abonados del BSC_i que serian registrados en MSC_j en caso de la falla de un MSC

Salida

$N_{tot,MSCj,BSCi,red}$ = Número dimensionado de abonados del BSC_i que serían registrados en MSC_j en caso de falla de la redundancia de una MSC

$N_{tot,MSCj,red}$ = Número dimensionado de abonados que serian registrados en MSC_j en caso de falla de la redundancia de una MSC

Procedimiento

1. Calcule el número adicional de abonados de cada BSC que debe ser manejado por cada MSC en el *Pool*

MSC_3 tiene el número mayor de abonados (550,000)

MSC_1 tiene el segundo número mayor de abonados (530,000)

$N_{MSCHigh,BSCi}$= Número de abonados del BSC_i registrados en el MSC_3

$N_{MSC2ndHigh,BSCi}$= Número de abonados del BSC_i registrados en el MSC_1

$$N_{MSC1,BSC1,red} = \frac{130,000}{(330,000-130,000)*100,000} = 65,000$$

$$N_{MSC1,BSC2,red} = \frac{140,000}{(460,000-140,000)*120,000} = 53,500$$

$$N_{MSC1,BSC3,red} = \frac{170,000}{(300,000-170,000)*80,000} = 104,615$$

$$N_{MSC1,BSC4,red} = \frac{50,000}{(210,000-50,000)*90,000} = 28,125$$

$$N_{MSC1,BSC5,red} = \frac{60,000}{(260,000-60,000)*140,000} = 42,000$$

$$N_{MSC2,BSC1,red} = \frac{130,000}{(330,000-130,000)*100,000} = 65,000$$

$$N_{MSC2,BSC2,red} = \frac{140,000}{(460,000-140,000)*200,000} = 87,500$$

$$N_{MSC2,BSC3,red} = \frac{170,000}{(300,000-170,000)*50,000} = 65,385$$

$$N_{MSC2,BSC4,red} = \frac{50,000}{(210,000-50,000)*70,000} = 21,875$$

$$N_{MSC2,BSC5,red} = \frac{60,000}{(260,000-60,000)*60,000} = 18,000$$

$$N_{MSC3,BSC1,red} = \frac{100,000}{(330,000-100,000)*130,000} = 56,522$$

$$N_{MSC3,BSC2,red} = \frac{120,000}{(460,000-120,000)*140,000} = 49,412$$

$$N_{MSC3,BSC3,red} = \frac{80,000}{(300,000-80,000)*170,000} = 61,818$$

$$N_{MSC3,BSC4,red} = \frac{90,000}{(210,000-90,000)*50,000} = 37,500$$

$$N_{MSC3,BSC5,red} = \frac{140,000}{(260,000-140,000)*60,000} = 70,000$$

2. Calcule el número dimensionado de abonados de BSCi registrado en el MSCj considerando redundancia de MSC:

$N_{tot,MSC1,BSC1,red}$ = 100,000 + 0.1x100,000 + 65,000 = 175,000

$N_{tot,MSC1,BSC2,red}$ = 120,000 + 0.1x120,000 + 52,500 = 184,500

$N_{tot,MSC1,BSC3,red}$ = 80,000 + 0.1x80,000 + 104,615 = 192,615

$N_{tot,MSC1,BSC4,red}$ = 90,000 + 0.1x90,000 + 28,125 = 127,125

$N_{tot,MSC1,BSC5,red}$ = 140,000 + 0.1x140,000 + 42,000 = 196,000

$N_{tot,MSC2,BSC1,red}$ = 100,000 + 0.1x100,000 + 65,000 = 175,000

$N_{tot,MSC2,BSC2,red}$ = 200,000 + 0.1x200,000 + 87,500 = 307,500

$N_{tot,MSC2,BSC3,red}$ = 50,000 + 0.1x50,000 + 65,385 = 120,385

$N_{tot,MSC2,BSC4,red}$ = 70,000 + 0.1x70,000 + 21,875 = 98,875

$N_{tot,MSC2,BSC5,red}$ = 60,000 + 0.1x60,000 + 18,000 = 84,000

$N_{tot,MSC3,BSC1,red}$ = 130,000 + 0.1x130,000 + 56,522 = 199,522

$N_{tot,MSC3,BSC2,red}$ = 140,000 + 0.1x140,000 + 49,412 = 203,412

$N_{tot,MSC3,BSC3,red}$ = 170,000 + 0.1x170,000 + 61,818 = 248,818

$N_{tot,MSC3,BSC4,red}$ = 50,000 + 0.1x50,000 + 37,500 = 92,500

$N_{tot,MSC3,BSC5,red}$ = 60,000 + 0.1x60,000 + 70,000 = 136,000

4. DEFINICIÓN DE POSIBLES ESTRATEGIAS DE RECUPERACIÓN

Un programa de Continuidad de Negocios tiene como objetivo proteger a su personal, información, operaciones y a la empresa y además de suma importancia para la protección de vidas humanas, reducir la confusión y permitir decisiones efectivas en tiempos de crisis, reducir la dependencia de personal específico, reducir la pérdida de datos, utilidades, clientes, etc., facilitar la recuperación oportuna de las funciones del negocio y mantener la imagen pública y la reputación.

Según lo que sugiere la norma BS 25999 para la definición de las posibles estrategias de recuperación se debe realizar primero un estudio previo de la organización que consiste en un análisis del impacto al negocio y una evaluación de riesgos de los servicios y procesos que son críticos. Como resultado de este análisis la organización estará en posición para escoger las estrategias de continuidad apropiadas que le permita cumplir sus objetivos.

El enfoque de la organización para determinar las estrategias de BCM debe ser:

a) Implementar las medidas apropiadas para reducir la probabilidad que ocurran incidentes y/o reducir los potenciales efectos de estos incidentes.
b) Tomar en cuenta debidamente la capacidad de recuperación y medidas de mitigación.
c) Proveer continuidad para las actividades críticas durante y después de un incidente.
d) Tener en cuenta aquellas actividades que no han sido identificadas como críticas.

La organización debería considerar las distintas opciones estratégicas para sus actividades críticas y los recursos que cada actividad requerirá en su reanudación. La estrategia o estrategias más apropiadas dependerán de un rango de factores como:

- El período máximo tolerable de una caída de una actividad crítica, esto es conocido como RTO (*Recovery Time Objetive*).
- Los costos de implementación de una estrategia o estrategias.
- Las consecuencias de una inacción.

Las estrategias deben cubrir los siguientes recursos de la organización:

- Personal.
- Localidades.
- Tecnología.
- Información.

En cada caso, la organización debe minimizar la probabilidad de implementar una solución de Continuidad del Negocio que pueda ser afectada por el mismo incidente que causa la interrupción del negocio.

4.1. Personal

La organización debe identificar las estrategias apropiadas para mantener las habilidades y el conocimiento clave. Este análisis se debe extender más allá de los empleados a los contratistas y otras partes interesadas quienes posean amplias habilidades especializadas y conocimiento. Las estrategias para proteger o proveer esas habilidades pueden incluir:

a) Documentación de la forma en la cual las actividades criticas son ejecutadas.
b) Entrenamiento multidisciplinario.

c) Separación de las habilidades críticas para reducir la concentración del riesgo, esto supondría la separación física del personal con conocimientos clave o garantizar que más de una persona tiene las habilidades clave necesarias.
d) Uso de terceros.
e) Planes de sucesión.
f) Retención y administración del conocimiento.

Las personas son las que hacen la planificación y ejecución de un plan de Continuidad del Negocio y de Desastre, pero hay muchos aspectos de las personas que a menudo son pasados por alto durante el proceso de planificación. Las personas son responsables del diseño, ejecución y supervisión de los procesos destinados a salvaguardar los datos. Algunas personas, especialmente aquellas con una formación de preparación para emergencias comenzarán a tomar acciones efectivas a través de roles de liderazgo. Otros estarán completamente abrumados y serán incapaces de actuar con eficacia.

La organización identificaría las estrategias apropiadas para mantener las habilidades y conocimientos clave. Este análisis debe ir más allá de los empleados, a los contratistas, a los interesados quienes poseen un amplio conocimiento y habilidades especializadas. Las estrategias para proteger o proveer esas habilidades incluyen:

4.1.1. Documentación de actividades críticas

El definir las actividades críticas de una empresa es un paso importante dentro de la metodología de la Continuidad del Negocio, sirve desde el análisis

de impacto al negocio, evaluación de riesgos y la documentación de los mismos como estrategia para la recuperación desde la perspectiva del personal.

Para la documentación de las actividades críticas en una empresa de telecomunicaciones se puede usar como referencia el marco de trabajo para la industria de telecomunicaciones o eTOM *(Enhanced Telecomunication Operations Map)*.

El marco de referencia posee información fundamental para el mundo de las telecomunicaciones y pretende dar estructura coherente a los procesos de la empresa, para lo cual abarca 3 grandes áreas:

- Gestión de la empresa o EM *(Enterprise Management).*
- Estrategia, infraestructura y producto o SIP *(Strategy, Infraestructure and Product).*
- Operaciones o OPS *(Operations).*

A partir de estas tres grandes áreas deriva hasta tres niveles de procesos, aportando todas las actividades relacionadas a las mejores prácticas de las empresas del sector. Su uso permite comprender mejor los procesos de la empresa para luego identificar cuáles son los procesos críticos.

4.1.2. Entrenamiento multidisciplinario

El entrenamiento multidisciplinario asegura que una persona pueda llevar a cabo varias actividades en el momento de la recuperación, esto se utiliza para minimizar el riesgo de la falta de personal en el momento de una recuperación. El entrenamiento se debe realizar al personal propio y solicitar que se haga con los contratistas también.

Para realizar este entrenamiento multidisciplinario se propone un modelo de seis fases:

4.1.2.1. Fase de análisis

Se realiza un análisis de las tareas por puesto de trabajo dentro de la organización para identificar las habilidades necesarias y especificar las tareas desempeñadas para soportar las operaciones. Esto se realiza a través de una gira por la oficina haciendo entrevistas de una encuesta previamente definida, luego la revisión de los datos de desempeño y por último la preparación del informe del análisis de las tareas por puesto.

El definir las actividades críticas de una empresa es un paso importante dentro de la metodología de la Continuidad del Negocio, sirve desde el análisis de impacto del negocio, evaluación de riesgos y la documentación de los mismos como estrategia para la recuperación desde la perspectiva del personal.

4.1.2.2. Fase de evaluación

Por último, se realizan exámenes periódicos y evaluaciones finales para cada módulo. Se completa el perfil de estudiante, se evalúan los resultados exhaustivamente, se analizan los resultados de las evaluaciones para determinar el nivel de éxito del programa de entrenamiento.

4.1.2.3. Fase de diseño

Se establecen las directrices para el entrenamiento incluyendo las metas y objetivos, la identificación de componentes especiales y materiales requeridos, el desarrollo de un plan efectivo para realizar el entrenamiento, determinar los métodos de evaluación, explorar las oportunidades de entrenamiento en

actualizaciones y por último la determinación y priorización de los programas de entrenamiento a desarrollar.

4.1.2.4. Fase de desarrollo

Se desarrollan los módulos de entrenamiento usando los datos reunidos durante el análisis y las directrices realizadas en la fase de diseño. Asignar maestros especialistas en cada área del currículo desarrollado. Explorar el material de referencia. Determinar el formato del currículo de entrenamiento. Desarrollo de los segmentos de entrenamiento práctico.

4.1.2.5. Fase de implementación

Se seleccionan los instructores calificados, se determinan los locales a utilizar y se monitorea continuamente el progreso de las clases incluyendo la instrucción, los resultados de las pruebas, contacto con el instructor y la retroalimentación del estudiante.

4.1.2.6. Fase de revisión

Por último, se realizan exámenes periódicos y evaluaciones finales para cada módulo. Se completa el perfil del estudiante y se evalúan los resultados exhaustivamente, se analizan los resultados de las evaluaciones para determinar el nivel de éxito del programa de entrenamiento.

4.1.3. Separación de habilidades clave

Para reducir la concentración del riesgo se recomienda la separación física del personal con conocimientos clave o garantizar que más de una persona tiene las habilidades clave necesarias. El primer paso para esto es la formulación de una política que se distribuya a nivel de toda la organización donde se especifica esta estrategia de continuidad. Esta estrategia puede ser implementada con un procedimiento parecido al del entrenamiento multidisciplinario.

Se realiza un análisis de las tareas por puesto de trabajo dentro de la organización para identificar las habilidades clave y las personas que los poseen. Esto se realiza por medio de una gira por la oficina haciendo entrevistas de una encuesta previamente definida, luego la revisión de los datos de indicadores clave de desempeño KPI *(Key performance indicators)* y por último la preparación del informe del análisis de las tareas por puesto.

Se desarrollan y aplican evaluaciones escritas o prácticas de los individuos identificados para recibir el entrenamiento de las habilidades clave. Todas las evaluaciones son basadas en las habilidades y las tareas realizadas en el trabajo.

Se establecen las directrices para la separación del personal con las habilidades clave, incluyendo el lugar y horarios de trabajo, la identificación de componentes especiales y materiales requeridos.

Por último se completa el perfil de las personas con las habilidades clave y se mantiene control periódico para asegurar que se cumple con la política.

4.1.4. Uso de terceros

Para implementar esta estrategia se debe realizar primero un análisis de qué procesos del negocio pueden ser desempeñados por una empresa externa que tiene como área de experiencia profesional el o los procesos identificados. Nuevamente se puede ver lo importante que es tener definidos los procesos críticos del negocio con su priorización.

Es importante observar que esta estrategia no significa la tercerización del proceso, sino el uso de un tercero en caso de desastre. Esto implica que se debe firmar un contrato previo con la empresa externa para asegurar que se brindará el servicio en caso de desastre.

Un factor importante a evaluar es que esta empresa no debe estar dentro de la misma área geográfica porque en este caso el riesgo que ambas empresas sean afectadas en caso de un desastre natural es muy grande, la organización debe minimizar la probabilidad de implementar una solución de Continuidad del Negocio que pueda ser afectada por el mismo incidente que causa la interrupción del negocio.

4.1.5. Plan de sucesión

En primer lugar se debe tener detectados los posibles candidatos que reemplacen a las personas que ocupan en la actualidad puestos claves y vitales para el desarrollo del negocio, esto en las grandes empresas incumbe a los puestos directivos, pero si pensamos en empresas de menor tamaño, veremos que en posiciones de mandos intermedios encontramos personas que poseen las claves del funcionamiento operativo de la empresa y dejar esto en manos de una persona, es una estrategia equivocada, que en primer lugar pone en riesgo el negocio y segundo crea una sobrecarga de responsabilidad en la persona

que lo posee, negándole incluso en ocasiones el derecho a ausentarse en caso de estar enfermo.

Se recomienda que cuando una persona tiene potencial de desarrollar funciones de mayor responsabilidad, tenga como requisito de promoción, la detección y formación de una persona para su reemplazo, en esto además de garantizar una continuidad con personas que ya conocen la organización y cuya carrera profesional se ha seguido de cerca, permite observar las capacidades del futuro, mando como formador y persona capaz de generar equipo, competencias claves en cualquier directivo o mando, de lo contrario podemos darnos cuenta que hay veces que un excelente profesional, no tiene porque ser un buen jefe.

Un punto fundamental dentro de este proceso, es seleccionar los puestos que serán objeto de este plan y posteriormente identificar las competencias requeridas para ejercerlo de manera idónea, por lo que se deja de lado a la persona que lo ocupa actualmente y se centra en los aspectos objetivos, no se trata de buscar un clon del actual ocupante, sino es incluso la oportunidad de mejorar la actual gestión, en ocasiones debemos sentirnos orgullosos si alguna persona que hemos seleccionado, lo hace mejor que nosotros, ya que esto quiere decir que hemos hecho bien nuestro trabajo y en definitiva implica un grado de madurez y sabiduría que nos posiciona en un nivel superior.

Al identificar las personas que tengan el potencial necesario, se debe seleccionar quienes pueden promocionar a corto, medio y largo plazo, ya que esto permite que el sistema se enriquezca y siga sin tener que depender de un solo candidato, siempre se está a tiempo de acudir a una segunda o tercera línea para darle continuidad al programa. Las técnicas empleadas para estos fines son diversas, desde la recomendación, pasando por un centro de evaluación y retroalimentación de 360º, entrevistas, etc.

Luego de este paso, se entra en los aspectos que implican la formación y adiestramiento de los candidatos, es importante encontrar un equilibrio entre la

formación teórica y el adiestramiento en las nuevas funciones, podemos definir este último como un proceso de entrenamiento asistido.

Es importante destacar que en definitiva esta política garantiza la Continuidad del Negocio, pero sobre todo genera una cultura donde las personas son un recurso valioso, que interactúan de manera generosa, compartiendo su experiencia y conocimiento, enriqueciéndose mutuamente y velando por el futuro y crecimiento de su propia carrera profesional.

4.1.6. Gestión y retención del conocimiento

La gestión del conocimiento es un nuevo enfoque gerencial que se basa en el reconocimiento y la utilización del valor más importante de las organizaciones: los recursos humanos, su conocimiento y su disposición a colocarlos a su servicio en este caso para la Continuidad del Negocio.

Con frecuencia, se afirma que estamos en una “era basada en los intangibles”, un concepto que se aplica a los resultados de las actividades que se basan y se derivan del conocimiento o de la inteligencia puesta en acción. La gestión del conocimiento se soporta en un sistema que permite administrar la recopilación, organización, refinamiento, análisis y diseminación del conocimiento en una organización.

Sus principales objetivos son contribuir a comprender cómo conseguir organizaciones más competitivas y adaptables, así como crear procesos y mecanismos de gestión que aceleren los procesos de aprendizaje, la creación, adaptación y difusión del conocimiento, tanto dentro de la empresa como entre la organización y su entorno.

En la gestión del conocimiento, se administran los activos no materiales de la organización; se genera, busca, almacena y transfiere el conocimiento con el propósito de aumentar la productividad y competitividad de las organizaciones.

Las ventajas competitivas que produce una adecuada gestión del conocimiento no dependen de la cantidad de conocimiento que se consiga reunir y almacenar sino del uso que se haga de ellos; por ello, y como parte de ella, es necesario adoptar una cultura corporativa que fomente el intercambio y la colaboración entre los miembros de una organización.

La gestión del conocimiento fomenta la creación y difusión de una cultura organizacional y un entorno de colaboración que favorezca dichas acciones mediante la presencia de un liderazgo, la cooperación mutua y las comunidades de práctica. Asimismo, posibilita la implementación de políticas en la organización, que estimula la capacitación, el aprendizaje y la motivación de cada miembro de la organización, según sus necesidades, además de crear las condiciones necesarias para que la información fluya en forma idónea sobre la base de un soporte tecnológico que facilite y agilice el flujo de la información y el conocimiento. Así, se facilita la toma de decisiones en función del cumplimiento de la misión, visión, metas y objetivos de la organización.

Las organizaciones generan nuevos conocimientos a partir de la experiencia, las aptitudes y actitudes en el desarrollo de una cultura propia; ellas deben crear un ambiente que estimule el conocimiento en el que converjan la calidad de los recursos humanos, la capacidad de gestionar la información y la presencia de un modelo organizativo capaz de implementar e integrar las herramientas, técnicas y métodos adecuados para involucrarse completamente en el proceso de creación del conocimiento.

En este contexto, es imprescindible destacar la inevitable relación entre la gestión del conocimiento, la gestión de la información, la gestión de la tecnología, la cultura organizacional y la gestión de los recursos humanos como elementos fundamentales para que el proceso resulte eficiente.

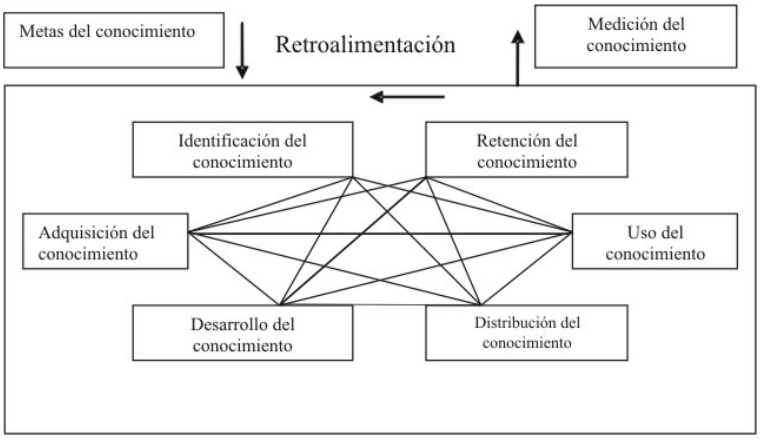
La gestión del conocimiento requiere de una eficiente gestión de la información. Por tanto, el éxito de la gestión del conocimiento está invariablemente condicionado a cómo se realice dicha gestión en la

organización así como por la calidad de los resultados que este proceso sea capaz de alcanzar. Otros elementos indispensables para lograr una adecuada gestión del conocimiento son la utilización de las tecnologías como herramientas fundamentales para la rápida y adecuada transmisión, generación y difusión del conocimiento; así como el desarrollo de los recursos humanos y de una cultura organizacional que actúe como elemento globalizador en las organizaciones, que exige de un compromiso a todos los niveles, depende en gran medida de su dimensión humana y busca incrementar el aprendizaje organizacional.

4.1.6.1. Procesos estratégicos de la gestión del conocimiento

La gestión del conocimiento está compuesta por un grupo de procesos estratégicos que se producen en forma cíclica ver figura 10.

Figura 10. Procesos estratégicos de la gestión del conocimiento.



Fuente: Probst G, Raub y Romhardt K.
Administre el conocimiento.

4.1.6.1.1. Identificación del conocimiento

El proceso de identificar el conocimiento en las organizaciones adquiere cada vez mayor importancia. Han surgido alternativas para solucionar los aspectos relativos a la transparencia del conocimiento organizacional. Se eliminan jerarquías y desarrollan estilos horizontales. Los superiores dejan de ser barreras en lo que a la transmisión del conocimiento se refiere y los expertos se comunican entre ellos. Las organizaciones se orientan hacia las redes internas a partir del empleo de determinadas técnicas y herramientas que facilitan estas acciones.

Los miembros de las organizaciones poseen conocimientos, habilidades, experiencias e intuición; sin embargo, ella sólo controla una parte mínima de estos. Por ello, es necesario desarrollar estrategias para lograr que los empleados tengan claros sus conocimientos para que se conviertan en información y que ésta se registre en documentos. La actuación de las personas en la organización es indispensable para una adecuada interrelación entre la gestión documental, la gestión de la información y finalmente, la gestión del conocimiento.

La gestión del conocimiento posee diversas herramientas para identificar el conocimiento: los directorios y las páginas amarillas de expertos, los mapas de conocimiento, las topografías del conocimiento, los mapas de activos del conocimiento, los mapas de fuentes del conocimiento, que se utilizan indistintamente en función de los objetivos propuestos, pero todos con resultados probados en diversos contextos.

Una vez identificado el conocimiento, las organizaciones deben trazar estrategias que permitan “anclarlo” a estas y se posibilite su uso.

4.1.6.1.2. Adquisición del conocimiento

Una vez identificado el conocimiento en la organización, este crece y se multiplica en la medida en que se utiliza. Esto exige a las organizaciones que se encuentran en constante proceso de transformación, a trabajar intensamente para renovar su conocimiento. Es precisamente por eso, que la gestión del conocimiento no puede considerarse como un proceso aislado en la organización sino alineado con sus estrategias.

Igualmente y tomando en cuenta que el conocimiento se expresa por medio de la información y que ésta debe registrarse en documentos que respalden el accionar de la organización, se apunta que todo sistema que gestiona conocimiento debe disponer para el desarrollo del proceso de adquisición efectiva de los sistemas de información y de gestión documental.

En caso de que la organización carezca de un conocimiento específico necesario, debe buscarlo en su entorno para adquirirlo o simplemente desarrollarlo en su interior.

4.1.6.1.3. Desarrollo del conocimiento

Como se refirió en el proceso de identificación del conocimiento, cuando la organización no posee un determinado conocimiento ésta debe crear condiciones e invertir para su desarrollo en la propia organización. Este proceso de creación o desarrollo del conocimiento no es más que un proceso de desarrollo de las competencias y habilidades de los individuos que pertenecen a la organización, es un proceso donde se propicia el establecimiento de un ambiente que favorezca el surgimiento de nuevas ideas para fomentar la innovación y de esta forma, generar soluciones que contribuyan al progreso de la sociedad en general.

4.1.6.1.4. Distribución del conocimiento

El conocimiento organizacional puede proceder de fuentes internas propias de la organización o externas cuando se adquiere de otras. Si se encuentran localizados e identificados los activos del conocimiento en la organización, entonces es posible compartir y distribuir el conocimiento.

Las organizaciones enfrentan problemas para distribuir y colocar a disposición de sus miembros el conocimiento que ellos necesitan. Es preciso considerar que el conocimiento se transfiere mediante acciones personales y por tanto, este proceso puede realizarse desde un centro de distribución del conocimiento hacia uno o varios grupos específicos de individuos, entre y dentro de los grupos y equipos de trabajo de la organización o entre individuos. Para esto, se soportan en herramientas tecnológicas, crean determinadas plataformas, software que facilitan compartir y distribuir el conocimiento, aunque ello no significa que éste último se utilice igualmente por todos los individuos en la organización. Se trata de proporcionar el conocimiento que necesita cada individuo para la realización de sus tareas específicas.

El conocimiento puede difundirse mediante su reproducción, es decir, por medio de la capacitación. Tanto ésta como el desarrollo profesional forman parte de la reproducción del conocimiento que se cumple mediante la realización de actividades como son los eventos, los foro-debate, etcétera. Estas técnicas también favorecen a la conservación del conocimiento organizacional, porque al compartirse se evita que la ausencia de un individuo, por una u otra razón, prive a la organización de un conocimiento que necesita.

4.1.6.1.5. Uso del conocimiento

En el ciclo de los procesos estratégicos de la gestión del conocimiento, el uso del mismo se ubica casi al final; sin embargo, esta ubicación es relativa,

debido a que los procesos de identificación, adquisición, desarrollo y distribución del conocimiento siempre se encuentran en consonancia con las necesidades de los usuarios por eso es necesario considerar un sistema de gestión de información que facilite información actualizada sobre las necesidades de los usuarios con vistas a lograr una eficiente gestión del conocimiento.

Para obtener una gestión efectiva del conocimiento, se deben crear plataformas de conocimientos, intranets, portales, escenarios, entre otras herramientas, con el objetivo de incentivar a los individuos a consumir información e incrementar su conocimiento.

Existen determinados elementos como los estilos de dirección, las políticas y la cultura de la organización que inciden en el uso del nuevo conocimiento. Estos elementos deben manejarse con el objetivo de potenciar el proceso de gestión del conocimiento. Es necesaria una actitud proactiva ante los retos que impone un entorno organizacional cada día más complejo y cambiante. También deben aceptarse los retos y fomentar el aprendizaje. El conocimiento en la organización constituye un recurso cuyo uso proporcionará relevantes beneficios.

4.1.6.1.6. Retención del conocimiento

La retención del conocimiento constituye un proceso esencial en la gestión del conocimiento. Si no es posible retener los conocimientos en la organización, se perderán los esfuerzos realizados en los procesos anteriores. Este proceso es de especial interés para la Continuidad del Negocio porque muchas de las interrupciones del mismo provienen por fallas de factor humano es decir por falta de conocimiento.

La retención del conocimiento significa conservar la información y los conocimientos utilizados por medio de un sistema de gestión documental que respalde la acción de la organización y que facilite su consulta en el momento necesario. Con ello, se escribe la historia de la organización, su evolución, como una manera más de enfrentar los nuevos cambios y desafíos, que renovada y de manera constante, impone la sociedad moderna a sus instituciones.

El nuevo conocimiento organizacional sólo puede desarrollarse sobre la base del conocimiento previo. Ni los individuos ni las organizaciones borran sus experiencias anteriores con las nuevas. Ellas se apartan y no se utilizan en las circunstancias actuales, no obstante, permanecen como una opción.

Para la retención del conocimiento, existen tres subprocesos fundamentales:

- Seleccionar, a partir de los múltiples sucesos que vive la organización, las personas y procesos que por su valor deben retenerse.
- Guardar la experiencia en forma apropiada.
- Garantizar que la memoria organizacional se actualice constantemente.

En todos ellos, el especialista en información tiene un lugar y una función muy importante, estos constituyen gran parte de su responsabilidad.

4.1.6.1.7. Guardar la experiencia en forma apropiada

Es garantizar que la memoria organizacional se actualice constantemente.

El especialista en información tiene un lugar y una función muy importante, estos constituyen gran parte de su responsabilidad.

Una alternativa para retener el conocimiento puede ser la creación de grupos de trabajo integrados por miembros de la organización, con independencia de su nivel de experiencia y con el objetivo de generar una transferencia del conocimiento de los más experimentados a los más jóvenes. Así, es posible minimizar los riesgos de la organización ante cualquier eventualidad con los individuos más calificados y experimentados que ella posee.

4.1.6.1.8. Medición del conocimiento

Medir el conocimiento no significa calcular su valor monetario, sino evaluar en qué medida se cumplen o no los propósitos del conocimiento en la organización. Para esto, se aplican diferentes técnicas. El proceso de evaluación y medición del conocimiento puede dividirse en dos fases:

1. Se observan los cambios en la base del conocimiento organizacional.
2. Se interpretan estos cambios en relación con los objetivos de dicho conocimiento.

El problema fundamental para medir el conocimiento radica en las características que poseen los sistemas de contabilidad tradicionales, los cuales deben transformarse para poder contabilizar las operaciones con los activos intangibles; ellos sólo posibilitan otorgarle un valor financiero tangible al conocimiento una vez que este se haya incorporado a los bienes comercializables.

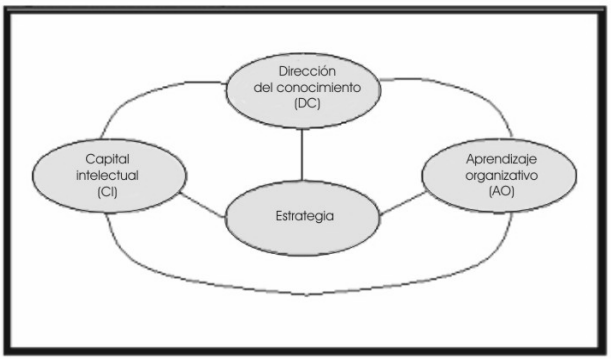
La idea de que el conocimiento puede medirse induce a esperar objetividad donde sólo puede haber aproximación. Por tanto, en este sentido, los sistemas de medición pueden sólo ofrecer aproximaciones sobre el comportamiento de este activo (el conocimiento) en la organización, debido a su propia naturaleza intangible.

Cada uno de estos procesos estratégicos, que interactúan en la gestión del conocimiento, son susceptibles de medirse por medio de diversos indicadores con el objetivo de determinar en qué medida se cumplen o no con eficiencia y tomar medidas correctivas en caso necesario. Esto, sin duda, permite potenciar una adecuada gestión del conocimiento que contribuye directamente al incremento del capital intelectual en las organizaciones.

El conocimiento inicia al admitir, conocer su variabilidad y sus causas, estas son imposibles de conocer sin medición. Conocer esto es precisamente la clave para administrar el proceso para conquistar los objetivos de excelencia que se plantea una entidad particular.

En la denominada tríada conceptual, en la que, en forma estratégica, se relacionan los tres conceptos claves, derivados de las tres palabras protagonistas de la sociedad del conocimiento (información, conocimiento y aprendizaje), se evidencia que la gestión del conocimiento es un enfoque holístico donde se relacionan elementos como el aprendizaje organizacional y la gestión del capital intelectual, además de la gestión del conocimiento propiamente dicho, ver figura 11.

Figura 11. La información, el conocimiento y el aprendizaje: una triada conceptual.



Fuente: Bueno E.
Enfoques principales y tendencias en dirección del conocimiento: Gestión del conocimiento desarrollos teóricos y aplicaciones.

4.1.6.2. Aprendizaje organizacional

El aprendizaje organizacional es el resultado de un proceso continuo de creación de valores e intangibles. A partir del aprendizaje individual y de los procesos de captación, estructuración y transmisión de conocimiento, puede llegarse a hablar de aprendizaje organizacional. Mediante un uso adecuado de las habilidades del personal; la creación de un ambiente competitivo, que incentive a las personas a que aprendan cada vez más; la generación de un ambiente favorable para compartir y distribuir la información entre todos los miembros de la organización para que ellos puedan utilizarla y convertirla en conocimiento individual y posteriormente en conocimiento organizativo; se desarrollan las capacidades de la organización para enfrentar problemas cada vez más complejos.

En las organizaciones, cuando las personas comienzan a trabajar en grupos, al principio suelen producirse problemas de coordinación, sin embargo, en la medida que transcurre el tiempo, los procesos se perfeccionan cada vez más y las tareas se realizan en forma integrada. Por tanto, puede afirmarse que el aprendizaje organizacional quiere decir, sin dudas, “aprender juntos a resolver problemas con efectividad”.

El aprendizaje es la clave para que las personas y la organización sean cada vez más inteligentes, a partir de la memorización y transformación de la información en conocimiento. El aprendizaje organizacional, muy ligado a los conceptos de “organizaciones inteligentes” y de “organizaciones que aprenden” defienden que: “Una organización inteligente es una organización que aprende y que tiene las habilidades necesarias para crear, adquirir y transferir conocimiento, así como para modificar su comportamiento para reflejar el nuevo conocimiento”.

Por tanto, el aprendizaje comienza con un nuevo conocimiento, que puede generarse internamente o proceder del exterior y que debe aplicarse

correctamente para modificar las metas organizacionales y los comportamientos. El aprendizaje organizacional ocurre cuando sus miembros responden a los cambios que se producen en el ambiente interno y externo, mediante la modificación de las estrategias y normas existentes con el objetivo de ajustar propósitos a la realidad de la organización.

La gestión del conocimiento es una nueva forma de administrar los procesos organizacionales. Su objetivo fundamental es identificar, capturar, desarrollar, distribuir y retener el conocimiento organizacional, tiene su origen y reside en las personas que componen la organización. Permite obtener ventajas competitivas para sobrevivir en el caso de un desastre.

La gestión del conocimiento comprende la gestión de los activos intangibles que generan valor para la organización. Dichos intangibles abarcan recursos que pertenecen a la organización pero que no se registran y valoran desde el punto de vista contable.

Los activos intangibles son también las capacidades que se generan en la organización cuando sus miembros comienzan a trabajar en grupo. La mayoría de estos intangibles se relacionan con los procesos de captación, estructuración y transmisión de los conocimientos. Es precisamente en este punto, donde se refleja la relación de la gestión del conocimiento con el aprendizaje organizacional y por ello, se afirma que la gestión del conocimiento tiene en el aprendizaje organizacional su principal herramienta.

Una adecuada gestión del conocimiento, soportada en el aprendizaje organizacional, contribuye a elevar y desarrollar el capital intelectual de una organización y sirve de base como estrategia para la recuperación en caso de desastres.

4.2. Localidades

Un recurso importante de las estrategias de recuperación son las localidades donde se planea continuar con el negocio en caso de desastre, para esto existen varias opciones que incluyen el uso de sitios alternos, acuerdos de cooperación, uso de compañías externas que pueden prestar este servicio y trabajo remoto o desde casa, a continuación se desarrolla cada una de estas posibles estrategias de recuperación. Se analizarán estas posibles estrategias en el caso de centros técnicos que es donde se instalan las centrales de telefonía móvil.

Las estrategias del lugar de trabajo pueden variar significativamente y existe un rango importante de opciones. Los diferentes tipos de incidentes o amenazas pueden requerir la implementación de diferentes o múltiples opciones de lugares de trabajo. Las estrategias correctas serán en parte determinadas por el tamaño de la organización, el sector al que pertenece y la extensión de las actividades, por las partes interesadas y por la situación geográfica. Por ejemplo, según el país las operadoras de telefonía móvil por ley necesitaran mantener un servicio continuo en sus comunidades a pesar de los desastres.

La organización debe elaborar una estrategia para reducir el impacto de la falta de disponibilidad de su sitio o sitios de trabajo normal. Esta puede incluir una o más de las siguientes:

4.2.1. Sitios alternos propios

Los centros técnicos, en donde se instalan las centrales telefónicas rara vez son cuidadosamente planificados desde el punto de vista de Continuidad del Negocio, es decir ubicados en un sitio que tiene el menor riesgo posible de

desastres naturales o artificiales. Se encuentran normalmente cerca de la sede de la empresa o de otro importante centro de operaciones que están a menudo en los grandes centros urbanos que pueden ser objeto de atentados de origen humano lo que puede producir desastres e interrupciones.

Muchas veces las operadoras celulares no tienen identificado a uno de los actuales centros técnicos para usarlo como sitios de recuperación interna. Las empresas a menudo tienen múltiples centros técnicos a nivel regional e internacional, pero, rara vez se dan a la tarea de identificar un centro técnico de la empresa como un sitio de recuperación y mantener el control de la recuperación de desastres.

No hay que olvidar que esta estrategia implica el traslado del personal a los centros técnicos alternos, estos locales deben estar lo suficientemente cerca para que el personal esté dispuesto y sea capaz de viajar a ellos, tomando en cuenta las posibles dificultades que pueden ser causadas por el incidente. Sin embargo, los sitios alternos no deben estar tan cerca para que no sean afectados por el mismo incidente. Para un operador de telefonía móvil es recomendable contar con al menos dos centros técnicos separados al menos 20 Km. para distribuir el riesgo de un desastre natural o provocado por el hombre.

4.2.2. Acuerdos de cooperación

Los acuerdos de cooperación o acuerdos recíprocos son los servicios utilizados cuando una operación celular puede aceptar el trabajo de otra operación celular temporalmente fuera de servicio, para que sean efectivos estos acuerdos es necesario que las operaciones involucradas pertenezcan al mismo grupo corporativo, la misma industria, además utilizan equipos de proveedores similares y ejecutan procesos similares. Incluso existe el riesgo

que si una de las partes de un acuerdo recíproco es víctima de un desastre, la otra parte puede sufrir el impacto de dicho desastre.

Es difícil hacer acuerdos recíprocos que sean totalmente confiables. Los cambios en cualquiera de los equipos y sistemas pueden provocar que se invalide el acuerdo. Además, los cambios en la Dirección pueden invalidar los acuerdos sin previo aviso y pueden dejar sin acuerdos de respaldo a la empresa.

4.2.3. Sitios de terceros

Este tipo de estrategia de recuperación es muy común en el mundo de IT, en donde la empresa tiene una localidad alterna con la infraestructura, los servicios de telecomunicaciones que puedan ser usados por la empresa contratante para recuperar los sistemas de información o funciones críticas del negocio. Los *hot sites* son instalaciones completamente operacionales mantenidas por proveedores independientes que normalmente son contratados por una tarifa mensual para la disponibilidad, espacio, equipo y servicios que ofrecen. Es una estrategia costosa pero proporciona un marco de tiempo de recuperación más corto. Para la tecnología de telecomunicaciones no existen este tipo de hot sites.

Este tipo de estrategia debe tomar en cuenta que el uso de lugares alternos deben estar bien soportado por un contrato claro en cuanto a si los *hot sites* son para uso exclusivo de la empresa. Si los *hot sites* son compartidos con otras empresas, debe haber un plan desarrollado y documentado de mitigación en el caso de que no esté disponible cuando se necesite.

4.2.4. Trabajo desde casa o remoto

En el caso de desastre y ante la imposibilidad de trabajar en los locales de la empresa una alternativa es trabajar desde casa.

Se configura una oficina en la residencia de los empleados o en algún lugar remoto con internet, una computadora portable con las aplicaciones necesarias para realizar el trabajo, y el acceso a la red de área local de la oficina vía una red privada virtualo VPN *(Virtual Private Network).* Este tipo de estrategia es válido también para los técnicos que realizan soporte y mantenimiento de las centrales de telefonía móvil.

Además puede ser apropiado mover la carga de trabajo en lugar de mover al personal por ejemplo, la carga de trabajo del centro de llamadas sustituye a la maquila de teléfonos.

4.3. Tecnología

Para realizar las estrategias de recuperación desde el punto de vista de la tecnología en el caso de operadores de telefonía celular se deben diferenciar en dos grandes categorías, la tecnología que soporta los procesos del negocio que es responsabilidad del área de tecnologías de la información (IT) y la tecnología que soporta la operación de la red de telefonía móvil que es responsabilidad del área de operaciones técnicas (OT), en general las estrategias de tecnología dependerán de la naturaleza de la tecnología empleada y su relación con las actividades críticas, pero será una combinación de las siguientes.

- Disposiciones adoptadas por la organización.
- Servicios prestados a la organización.
- Servicios prestados externamente por terceras partes

Las estrategias pueden incluir:

- La distribución geográfica de la tecnología por ejemplo tener la misma tecnología en diferentes ubicaciones que no serán afectadas por la mismo desastre del negocio.
- Mantener equipo viejo para ser usado como repuesto en caso de emergencia.
- Mitigar el riesgo de tener equipo sin redundancia o en su defecto largos tiempos de entrega del equipo.

Para las tecnologías de la información (IT) los servicios frecuentemente necesitan estrategias de continuidad complejas. En donde dichas estrategias son requeridas, se debe cumplir lo siguiente:

- Los tiempos de recuperación objetivo (RTOs) para sistemas y aplicaciones que soportan las actividades clave identificadas por el BIA.
- Localidades y la distancia entre estos sitios donde está la tecnología.
- Número de sitios tecnológicos.
- Acceso remoto.
- Uso de centros de datos sin personal como complemento de los centros de datos con personal.
- Conectividad de telecomunicaciones y su redundancia.
- La naturaleza del conmutación por falla entre los centros de datos, cuando se necesita intervención manual para activar la conmutación de sistemas, o cuando debe ocurrir automáticamente.
- Conectividad a terceros y los enlaces externos.

Si se escoge la estrategia de conmutación en caso de falla de un sitio a otro, la ruta de la red de datos entre los dos sitios tiene que ser considerada cuidadosamente, así como la distancia entre los centros de datos, porque pueden tener impacto negativo en la forma en la cual los sistemas de IT operan.

En el caso que la organización de IT tenga más de un centro de datos, puede haber una estrategia de recuperación de IT mutua, esto es que los sistemas, la red y el almacenamiento en cada sitio son dimensionados para hacer frente al tráfico combinado y al trabajo de ambos sitios.

Otra solución a relocalizar al personal en sitios alternos es proveer al personal con acceso remoto a los sistemas vía acceso telefónico o a través de internet usando una red privada virtual o alguna tecnología similar.

La recuperación de tecnología puede incluir tanto estrategias de servicios centrales como de las unidades de negocios. Si se pierde información electrónica clave, puede ser crucial para una unidad de negocios tener acceso a archivos importantes en forma manual.

Mayores directrices en continuidad de IT y hardware de telecomunicaciones pueden ser encontradas en documentos como PAS 77, BS ISO / IEC 27001 y BS ISO / IEC 2000.

Para las tecnologías de la red celular (OT) se necesita desarrollar estrategias en dos capas, la del subsistema de estación base y la del subsistema de conmutación de red o red central. Por su misma naturaleza, el subsistema de estaciones base es distribuido, lo que hace que las estrategias de esta capa estén enfocadas a tener una redundancia a nivel de la red de transmisión y manejar una estrategia a nivel de BSC similar a lo que se hace con las MSC del subsistema de conmutación de red como se discutió con profundidad en el capítulo 3.

Para las estrategias a nivel de NSS, se debe tomar en cuenta lo siguiente:

- Los tiempos de recuperación objetivo (RTOs) para los componentes del NSS soportan las actividades clave identificadas por el BIA.
- Centros técnicos y la distancia entre estos sitios.
- Número de centros técnicos.
- Acceso remoto.

- Red de transmisión entre centros técnicos y su redundancia.
- Topología del subsistema de conmutación de la red (NSS).
- Hardware y equipo que forma el NSS.
- Versiones de software de los equipos del NSS.
- La naturaleza de la conmutación por falla entre los centros técnicos, cuando se necesita intervención manual para activar la conmutación de sistemas o cuando debe ocurrir automáticamente, esto está muy relacionado con el tipo de topología que se utiliza.
- Conectividad a PSTN y otros operadores.
- Procedimientos para restaurar datos y sistemas críticos.

La estrategia de respaldo de información debe incluir la información de las bases de datos del NSS, como HLR y VLR, además de las configuraciones de los MSC para que en caso de emergencia puedan ser recuperados en el menor tiempo posible.

La coordinación de las estrategias de tecnología de red de los servicios clave debe basarse en los requerimientos del negocios tal y como se definió en el BIA. El grupo de OT trabajará sobre estos requerimientos y desarrollará una estrategia inicial basada en la complejidad técnica, los sistemas críticos, los tiempos de recuperación, los parámetros de pérdida de información y los costos. Es normal que esta estrategia sea modificada una vez que se conoce el costo real.

4.3.1. Internos

Las estrategias de tecnología con solución interna implican la compra, la instalación y la configuración de equipos por parte del operador. Se diferencian tres tipos de soluciones la distribución de las operaciones, la implementación de equipo en espera y el uso de equipo viejo como respuesta.

Cuando se considera el uso de recursos internos se debe poner especial atención a los costos, con frecuencia puede ser una opción costosa comparada con el uso de recursos externos.

A continuación se detallará cada una de las soluciones:

4.3.1.1. Distribución de las operaciones

Las estrategias de tecnología pueden incluir la distribución geográfica de tecnología, por ejemplo mantenimiento de la misma tecnología en diferentes localidades que no serán afectadas por la misma interrupción de negocios, la aplicación para NSS es el MSC en *Pool* que se discutió en detalle en el capítulo 3 de este trabajo.

Esta solución presenta las ventajas que el equipo puede presentar la configuración optima para la Continuidad del Negocio, las pruebas se pueden hacer a conveniencia de la empresa, los controles de seguridad se pueden instalar con base en el estándar corporativo, los sistemas están disponibles siempre que así se requiera, es la estrategia mas confiable pero también la más costosa.

4.3.1.2. Equipo en espera o *Standby*

Como alternativa para la recuperación de la tecnología se puede tener una solución con equipo en espera o *Standby*. Este equipo debe estar instalado, configurado y listo para ser utilizado en caso de desastre, debe estar ubicado en un lugar diferente a donde se encuentra el equipo al que respalda, lo suficientemente lejos para evitar que un desastre afecte a ambos equipos a la vez, debe existir un procedimiento manual de conmutación en caso de falla.

Más detalles sobre esta solución se presentan en el capítulo relacionado a los temas de topología en espera o *Standby*.

Esta solución presenta las ventajas que se puede contar con el equipo para recuperar en el corto plazo en caso de desastre, las pruebas se pueden hacer a conveniencia de la empresa, los controles de seguridad se pueden instalar con base en el estándar corporativo, los sistemas están disponibles siempre que así se requiera, como desventaja presenta un procedimiento manual de conmutación en caso de falla, que implica una interrupción del servicio durante el tiempo que se realizar la conmutación de los sistemas, es una estrategia con un costo similar a la estrategia de distribución de operaciones pero con mayor tiempo de respuesta.

4.3.1.3. Equipo viejo

Mantener equipo viejo como reemplazo de emergencia o de piezas de repuesto y mitigación de repuesto adicional para equipo único o de entrega de largo plazo es otra estrategia para la recuperación de la tecnología en el momento de un desastre. Este equipo debe estar almacenado en un lugar externo a los sitios técnicos, lo suficientemente lejos para evitar que un desastre afecte más de una localidad a la vez.

Esta solución presenta las ventajas que es la de menor costo de implementación, se puede contar con el equipo para recuperar en el corto plazo en caso de desastre como desventajas presenta una degradación del servicio al momento de operar después del desastre porque el equipo viejo puede tener una menor capacidad que el equipo nuevo, procedimiento manual para el cambio del equipo lo que implica una interrupción del servicio durante este tiempo, es la estrategia que menor grado de confianza presenta al momento de un desastre porque puede ser incierto el desempeño del equipo de reemplazo.

4.3.2. Soluciones externas

Los servicios comerciales de recuperación de centrales telefónicas en caso de desastre se limitan a la firma de acuerdos de entrega rápida con los proveedores del equipo de la red celular. En este caso la estrategia implica la compra de equipo en el momento del desastre los acuerdos preestablecidos con los proveedores que pueden enviar rápidamente hardware permite restablecer más rápida y eficientemente los sistemas de misión crítica y deben tomarse en cuenta los componentes específicos de hardware especializado del NSS.

Dichos acuerdos incluyen:

- Acuerdo de revendedor/distribuidor: Este contrato le otorga a los abonados el compromiso del proveedor del mejor esfuerzo para acelerar la venta de hardware si este está disponible al momento del desastre.
- Acuerdo de renta pre concertado: En este contrato se le asegura a los abonados que el hardware estará disponible para envío rápido y que puede ser utilizado/rentado para el período de recuperación.
- Acuerdo de almacenamiento/envío dedicado: Con este contrato se les garantiza a los abonados tener hardware almacenado exclusivamente para su uso, que será enviado inmediatamente a una localidad alterna en caso de un desastre.

4.4. Información

Las estrategias de recuperación de la información deben asegurar que la información vital para la operación de la empresa está protegida y sea recuperable de acuerdo a los tiempos definidos en el BIA.

Para mayor información se puede buscar en el BS ISO/IEC 27001. El almacenamiento y la recuperación de la información tienen que cumplir con las legislaciones que le atañen.

En general, la información es un elemento crítico para asegurar la Continuidad del Negocio, en una empresa de telecomunicaciones la información es parte crítica para asegurar el servicio, como ejemplo se tiene la información de los servicios de los abonados, el registro de las llamadas realizadas que sirve de base para el cobro y la información para el cobro y facturación de los mismos.

Las leyes existentes de seguridad de la información, en la mayoría de los países, ofrecen pocas directrices en lo que las compañías deben cumplir, por lo que las compañías deben buscar primariamente en las normas y mejores prácticas que viene de la industria de seguridad de datos.

Como mínimo, las compañías deben mantener un inventario de la información que poseen, implementar programas de seguridad, políticas y auditorías sobre estas y actualización de la seguridad de los sistemas regularmente.

Las estrategias de información deberían ser tal que garanticen que la información vital de la operación de la organización es protegida y recuperable de acuerdo a los plazos descritos en la BIA.

Toda la información necesaria para permitir la realización de las actividades críticas de la organización debería disponer de:

- Confidencialidad.
- Confiabilidad.
- Integridad.
- Disponibilidad.

Las estrategias de información deben ser documentadas para la recuperación de la información que aún no ha sido copiada o guardada en un lugar seguro.

En todos los casos, la información necesita ser recuperada a un determinado punto en el tiempo que es conocido y aceptado por la alta gerencia. Existen varios métodos de copia que pueden ser usados, como cintas de respaldo, microfichas, fotocopias, creación de doble copia al momento de la producción. Este punto de recuperación es frecuentemente referido como el Punto de Recuperación Objetivo o RPO *(Recovery Point Objetive).*

4.4.1. Formato físico o copia impresa

Para la información que se encuentra en forma impresa como registros o contratos se debe almacenar afuera del sitio de operación para permitir la recuperación de datos después de un incidente, el sitio en donde se almacenan debe presentar mejores condiciones de seguridad que los sitios operativos.

Dentro de las copias de registros o copia impresa se debe considerar:

- Preparativos, planes y procedimientos de unidad de negocios.
- Copia de los registros como inventarios, registros de fórmulas y productos.
- Contratos o papelería legal.

4.4.2. Formato electrónico

El almacenamiento de la información en formato electrónico continua evolucionando en términos de capacidades, también tiende a ser menos caro conforme pasa el tiempo, a continuación se presentan algunas soluciones disponibles hasta el día de hoy.

4.4.2.1. RAID

El arreglo redundante de discos económicoso o RAID *(Redundant Arrays of inexpensive Disks)* viene en varias formas. La capacidad de cambiar los discos cuando se encuentran en operación *(hot-swap)* dentro del arreglo puede ser un atributo importante de la estrategia de recuperación de los discos. Existen varias configuraciones posibles del RAID incluyendo RAID 1+0, RAID 1+1, RAID n+1, RAID 5+0 que lo implican es el nivel de redundancia que maneja el arreglo. Debe evaluarse detenidamente cuales son los argumentos a favor y en contra de cada una de estas configuraciones para tomar una decisión sobre la estrategia de redundancia.

4.4.2.2. Diario remoto

El diario remoto o *Remote Journaling* es un método por el cual cada operación de escritura y actualización a nivel de base de datos es replicada en otro dispositivo. Esto es parte de una solución de recuperación de información que debe ser complementada con el proceso de restauración de esta información a los sistemas de redundancia en caso de desastre. Puede ser útil en caso de intrusión de red o corrupción de la información. El diario hecho en tiempo real crea una copia espejo de las transacciones. Esta información de las transacciones del diario puede ser transmitida sobre un enlace de comunicaciones permitiendo la rápida recuperación en el caso de una corrupción de información, violación de la seguridad u otro tipo de falla en la información.

4.4.2.3. Replicación

La replicación de los discos involucra la copia de los datos en un servidor primario y uno secundario. Existen dos métodos para realizar la replicación el sombreado *(Shadowing)* y agrupamiento *(Clustering).* El sombreado se ejecuta asincrónicamente, esto significa que los cambios son colectados y aplicados en el servidor secundario de forma periódica. El sombreado puede ser parte de una estrategia para mitigar un riesgo, pero hay que mantener en mente que cualquier corrupción o error en el servidor primario podría ser replicado en el servidor secundario también. El agrupamiento es una solución mas avanzada que el sombreado y provee alta disponibilidad. El agrupamiento de servidores trabaja de manera similar al RAID de discos duros. Con el agrupamiento, varios servidores están atados juntos y periódicamente se sincronizan con los otros. Si un servidor se cae, la carga de trabajo se traslada a los servidores restantes. Este proceso es transparente para los usuarios que están conectados a las aplicaciones y no tienen idea de cual servidor les provee de la información. El agrupamiento de servidores provee un balance de la carga de los usuarios y esta funcionalidad también provee un nivel de mitigación del riesgo.

4.4.2.4. Bóveda electrónica

Bóveda electrónica es el proceso que transmite las copias de seguridad de los datos de los sistemas a una localidad remota. Los respaldos o copias de seguridad no necesitan ser transportados o almacenados en un sitio afuera y en el caso de una interrupción del negocio; pueden ser más fácilmente accesados que cintas almacenadas en la bóveda de un banco u otro sitio seguro afuera de las instalaciones. La bóveda electrónica puede reducir dramáticamente el

tiempo de recuperación, especialmente si es usado en conjunto con el diario remoto.

4.4.2.5. Sistemas operativos en espera

Como es bien conocido, el sistema operativo con sus parches y actualizaciones es un aspecto crítico para poder tener las aplicaciones nuevamente en línea. El tener discos duros en espera con sistemas operativos preconfigurados disponibles puede reducir los riesgos y tiempos de recuperación. Cada vez que se actualice el sistema en producción se debe actualizar los sistemas en espera, así el sistema operativo está listo para usarse en el caso de una falla o interrupción.

4.4.2.6. Almacenamiento adjunto a la red o NAS

El NAS *(Network Attached Storage)* es un dispositivo de almacenamiento con una interfase para la red puede ser adjunto a la misma en cualquier ubicación que provee conectividad de red. Así, una unidad de almacenamiento que puede ser contenida en una bóveda, un cuarto de servidores o en el medio de un área de trabajo. Este tipo de dispositivos de almacenamiento son fáciles de instalar y mantener.

4.4.2.7. La red de área de almacenamientoo SAN

La SAN *(Storage Area Network)* es una red de alta velocidad dedicada al almacenamiento de datos. El almacenamiento es independiente de los servidores y es guardado a través de la red de almacenamiento. En la mayoría de las organizaciones, mucho del tráfico de la LAN es dedicado a las copias

respaldo, la replicación y actividades de recuperación de desastres. Con una SAN, estas actividades son restringidas a la red de almacenamiento y el ancho de banda en la LAN es liberado para otras necesidades de los usuarios.

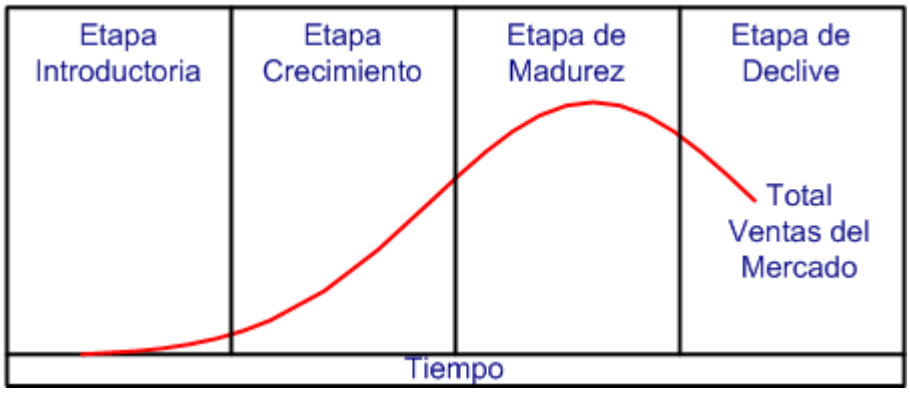
5. CRITERIOS DE SELECCIÓN DE ESTRATEGIAS

Luego de haber realizado la definición de las posibles estrategias a seguir tomando en cuenta al personal, las localidades, la tecnologia y la información se deben evaluar la combinación de las estrategias de recuperación bajo el análisis de criterios que se han identificado como claves para cumplir con los objetivos de recuperación definidos por la organización. Los tres principales criterios para seleccionar la estrategia son la fase actual dentro del ciclo de vida en la que se encuentra el negocio a recuperar, el análisis costo beneficio de las diferentes estrategias y la factibilidad técnica. A continuación se presentará en detalle cada uno de los criterios.

5.1 Ciclo de vida del negocio

Para el análisis del ciclo de vida utilizaremos el modelo de las cuatro etapas o fases: la primera es la introductoria, la segunda es de crecimiento, la tercera de madurez y por último la fase de declive. Ver figura 12.

Figura 12. Ciclo de vida del negocio



Fuente: **Plantillas de Microsoft Visio.**

El ciclo de vida tiene que ver con la vida de un producto en el mercado con respecto de sus costos y ventas comerciales por lo que podemos concluir que las ganancias suben y bajan en las diferentes etapas del ciclo de vida y los negocios requieren diferentes estrategias de continuidad en cada etapa del ciclo de vida debido a esta razón.

En la primera etapa, los costos son altos, hay bajos volúmenes de ventas, no hay mucha competencia, la demanda se debe crear, se le pide a los clientes que prueben el producto, generalmente no se generan ganancias en esta etapa. Debido a las caracteristicas anteriores, la estrategia recomendada a nivel de personal es tener documentación de la forma en la cual las actividades críticas son realizadas y entrenado al personal en múltiples hábilidades. Como en esta etapa existe poco personal, deben ser generalistas y conocer muy bien la operación.

A nivel de localidades, normalmente en esta etapa se cuenta con un sólo centro técnico por lo que la estrategia implica recuperar en este mismo sitio, o buscar un lugar alternativo proveido por terceros, quizás esta sea la mayor de las desventajas porque de acuerdo a la magnitud del desastre esto puede tomar semanas o incluso meses.

A nivel de tecnología normalmente en esta etapa se cuenta con el hardware necesario para operar pero no se cuenta con redundancia geográfica lo cual compromete mucho la recuperación. La estrategia más recomendada a nivel de tecnología en esta etapa es negociar acuerdos de despacho rápido para la compra de tecnología necesaria para seguir operando en el momento del desastre, lo cual sin este tipo de acuerdo previo puede implicar semanas o meses de espera, esto reducirá el tiempo de espera y minimiza la inversión necesaria para la Continuidad del Negocio. Para la implementación de esta estrategia es muy probable que se necesite contratar personal del proveedor del hardware para instalarlo.

Por último, en cuanto a la información se recomienda revisar la legislación del país para verificar cuáles son los requerimientos oficiales al respecto. Pero si no hay un requerimiento específico la estrategia más común en esta etapa es guardar copias de seguridad, tanto de los datos como las configuraciones de las centrales, en un lugar fuera del centro técnico, se recomienda que este proceso se realice diariamente.

En resumen, durante la etapa introductoria las estrategias recomendadas son a nivel de procesos con la mínima inversión posible y la negociación de un acuerdo de despacho rápido para la compra del hardware necesario para recuperar en el momento del desastre. Esta estrategia está en concordancia con la poca generación de ganancias de esta etapa por lo cual es dificil conseguir un presupuesto alto para la Continuidad del Negocio cuando está en etapa introductoria y el éxito del mismo no está asegurado.

En la segunda etapa o de crecimiento, los costos se reducen debido a economías de escala, el volumen de ventas se incrementa significativamente, las ganacias empiezan a crecer, la conciencia pública sobre la compañía se incrementa, nuevos competidores se empiezan a establecer en el mercado, el incremento de la competencia provoca la reducción de los precios.

Basados en las anteriores caraceristicas la estrategia recomendada a nivel de personal es igual a la etapa anterior, tener documentación de la forma en la cual las actividades críticas son realizadas y entrenar al personal en múltiples habilidades para tener al menos dos personas capacitadas para realizar la misma tarea; el cambio más significativo es que muy probablemente se incluya la separación geográfica de las habilidades principales para reducir la concentración del riesgo, en esta etapa empiezan los especialistas que conocen muy bien una área de la operación, para ellos es importante generar personas alternas que puedan suplirlos en caso de ausencia esto se hace con la implementación de planes de sucesión.

A nivel de localidades, debido al crecimiento del negocio se recomienda implementar un nuevo centro técnico cuando se necesite crecer en el centro técnico existente, esto nos permite tener redundancia geográfica, la distancia mínima entre ambos centros debería ser de 20 kilómetros. Al implementar este nuevo centro técnico se permite realizar estrategias de recuperación en sitio alterno, la ventaja de esta estrategia es que cuando se necesita realizar el tiempo de implementación es de días, una reducción importante comparado en la etapa anterior.

A nivel de tecnología, al poder contar con un segundo centro técnico es necesario contar con capacidad extra en cada uno de los centros técnicos lo cual permite la recuperación en caso de desastre. Esta estrategia implica la definición del nivel de operación en caso de desastre, una medida porcentual de la capacidad normal de operación. El tiempo de respuesta de esta estrategia es de días, una mejora importante sobre el tiempo de respuesta de la etapa anterior. Por último, en cuanto a información, se recomienda realizar copias de seguridad en línea, guardar las copias de seguridad tanto de los datos como las configuraciones de las centrales en el otro centro técnico, se recomienda que este proceso se realice diariamente en horas de poco tráfico celular.

En resumen, durante la etapa de crecimiento se vuelve viable financieramente el implementar la estrategia de recuperación de redundancia geográfica con la construcción de otro centro técnico, esto es posible debido al crecimiento en las ganancias y que se vuelve importante proteger la imagen pública de una compañía celular por ser un servicio importante en caso de desastres naturales.

En la tercera etapa o de madurez, los costos se reducen como resultado del incremento de la producción en volumen, las ventas llegan a su máximo y se alcanza la saturación del mercado, se empiezan a consolidar los competidores en el mercado, los precios tienden a bajar debido al incremento en el tamaño de los competidores. Se enfatiza en la diferenciación y

diversificación para mantener o incrementar la participación de mercado, las ganancias en la industria empiezan a bajar.

En esta etapa la empresa puede empezar a capitalizar la creación de toda una arquitectura de Continuidad del Negocio realizada en la etapa de crecimiento, al llegar a esta etapa si se implementaron las estrategias anteriores se puede utilizar la preparación de la Continuidad del Negocio como un diferenciador importante para la compañía dificil de imitar por los competidores que no implementaron similares estrategias en las etapas previas.

La estrategia recomendada a nivel del personal para esta etapa se basa en las estrategias desarrolladas en etapas anteriores, el tener documentadas todas las actividades críticas, el entrenamiento de múltiples habilidades para el personal, la separación de las habilidades clave para la reducción de la concentración del riesgo esto puede ser a través de separación física o asegurando que más de una persona cuenta con las habilidades clave requeridas y la implemetación de planes de sucesión para este personal clave. Además de las anteriores, se recomienda la implementación del uso de proveedores y aplicar políticas de retención del conocimiento.

A nivel de localidades, en esta etapa de acuerdo al crecimiento del negocio se pudieron implementar uno o varios centros técnicos adicionales, lo que permite tener redundancia geográfica, la distancia mínima entre centros técnicos debería ser de 20 kilómetros, esto permite que el personal pueda viajar, durante el incidente, al centro alterno o los centros alternos tomando en cuenta las posibles dificultades causadas por el incidente, sin embargo, está lo suficientemente separado para que sea poco probable que se vea afectado por el mismo incidente. Otra estrategia que se puede implementar, es la de trabajar desde casa o en forma remota para las actividades que asi lo permitan.

A nivel de tecnología, al poder contar con uno o varios centros técnicos es posible implementar una topología de centrales en grupo lo cual permite el trasladar el tráfico del sitio afectado a los otros sitios en forma automática.

Entre más centros técnicos se implementen menor es la inversión en capacidad extra disponible que se tiene que realizar para implementar esta estrategia de recuperación, lo que además facilita enormemente la recuperación en caso de desastre y reduce la concentración del riesgo. El tiempo de respuesta de esta estrategia es casi inmediato, no requiere la intervención humana, una mejora importante sobre el tiempo de respuesta de la etapa anterior que puede permitir tener una ventaja competitiva importante.

Por último, en cuanto a información se recomienda realizar copias de seguridad en línea, guardar las copias de seguridad tanto de los datos como las configuraciones de las centrales en el otro centro técnico; se recomienda que este sea un proceso automático que se realice diariamente en horas de poco tráfico celular. En todos los casos, la información necesita ser recuperada en un punto en el tiempo que es conocido y aprobado por la alta gerencia.

En resumen, durante la etapa de madurez la estrategia de recuperación en caso de desastres se vuelve estratégica, se capitaliza la implementación de estrategias realizada en las etapas previas y se utiliza como ventaja competitiva difícil de emular por los competidores que no realizaron las inversiones en Continuidad del Negocio en las etapas previas. El enfoque es en la recuperación en el menor tiempo posible con las mejores tecnologías y prácticas.

En la última etapa o declive, los costos se convierten en óptimos, el volumen de ventas declina o se estabiliza, los participantes en el mercado están consolidados, los precios y las ganancias disminuyen. Las ganancias se generan más por la eficiencia operativa que por el incremento de ventas. En esta etapa la empresa ya no está más interesada en invertir en arquitectura de Continuidad del Negocio sino más enfocada en optimizar la inversión realizada en las etapas anteriores.

La estrategia recomendada a nivel personal para esta etapa basada en las estrategias desarrolladas en etapas anteriores, el tener documentados todas las

actividades críticas, el entrenamiento de múltiples habilidades para el personal, la separación de las habilidades claves para la reducción de la concentración del riesgo esto puede ser a través de separación física o asegurando que más de una persona cuenta con las habilidades clave requeridas y la implemetación de planes de sucesión para este personal clave. Además de la implementación del uso de proveedores y aplicar políticas de retención del conocimiento. Esta estrategia es de suma importancia para maximizar la inversión realizada en continuidad durante las etapas anteriores.

A nivel de localidades, en esta etapa de acuerdo a la reducción del tráfico se plantea la consolidación y reducción de centros técnicos, al punto de tener el mínimo necesario que son dos, si el tamaño del negocio lo permite se pueden seguir con los centros técnicos desarrollados previamente, sino lo recomendable es consolidar al mínimo necesario. Se recomienda mantener la redundancia geográfica, con el criterio de la distancia mínima entre centros técnicos de 20 kilómetros.

A nivel de tecnología se recomienda mantener la topología de centrales en grupo, conforme se reduce el tráfico se puede mantener la capacidad necesaria en los centros técnicos para trasladar en forma automática el tráfico perdido de un centro a los otros o el otro según sea el caso. En esta etapa el foco está en la eficiencia de los recursos, lo que debe aplicarse también a las estrategias de recuperación de las centrales. El tiempo de respuesta de esta estrategia deberia ser casi inmediato, sin la intervención humana, como lo era en la etapa anterior.

Por último, en cuanto a información se recomienda realizar copias de seguridad en línea, guardar las copias de seguridad tanto de los datos como las configuraciones de las centrales en el otro centro técnico, se recomienda que éste sea un proceso automático que se realice diariamente en horas de poco tráfico celular.

En resumen, durante la etapa de declive la estrategia de recuperación en caso de desastres debe estar alineada con la eficiencia operativa, se optimiza la implementación de estrategias realizada en las etapas previas. El enfoque es en la recuperación con la mejor eficiencia posible de acuerdo a las tecnologías y prácticas implementadas en las etapas anteriores.

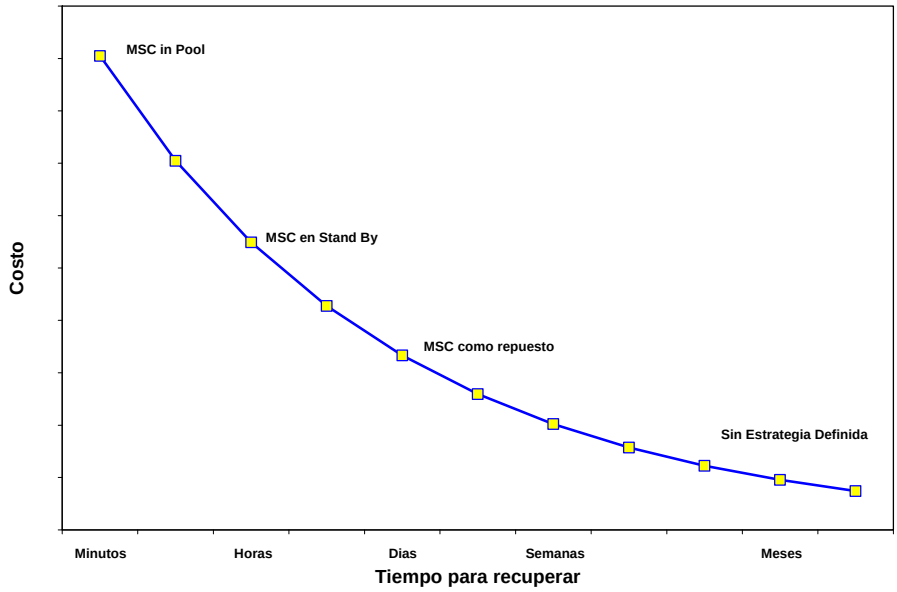
5.2 Análisis de costo beneficio

El análisis de costo beneficio es el siguiente criterio importante para seleccionar cuál es la mejor estrategia de recuperación, asimismo, podemos definir cuál es la estrategia que entrega más valor económico a la organización.

Para este análisis de costo beneficio necesitamos construir dos gráficas la de costo de la disponibilidad y el impacto financiero por lo que es importante tomar el tiempo para entender y evaluar las posibles alternativas. Una decisión precipitada cuando se trata de Continuidad del Negocio siempre es una decisión que se lamentará.

Para la gráfica de costo de disponibilidad, definimos los costos de disponibilidad de cada una de las estrategias propuestas, luego la gráfica de costo de disponibilidad se construye al trazar sobre una línea los costos de cada una de las estrategias analizadas como se muestra en la figura 13.

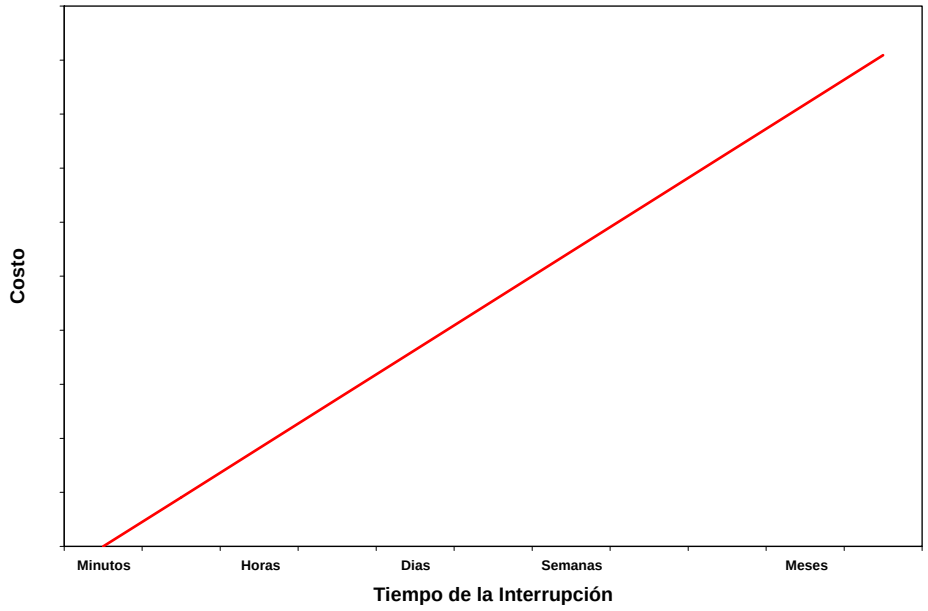
Figura 13. Gráfica de costo de disponibilidad



Fuente: Instituto Internacional para la Recuperación de Desastres. **Curso de administración de continuidad de negocios para profesionales avanzados**. Pág. 4.45

La gráfica de impacto financiero se construye al trazar sobre una línea las pérdidas de acuerdo al tiempo de interrupción del servicio, esto puede hacerse basado en los datos históricos de la empresa como se muestra en la gráfica a continuación. Para construir la gráfica de impacto financiero necesitamos saber cuáles son los ingresos de la compañía durante el último año y de allí definir el costo que tendría una interrupción durante una hora, por ejemplo. Hacemos una ecuación lineal con estos datos para definir el costo financiero de la interrupción en los períodos de tiempo a evaluar por simplicidad se realiza con una línea recta.

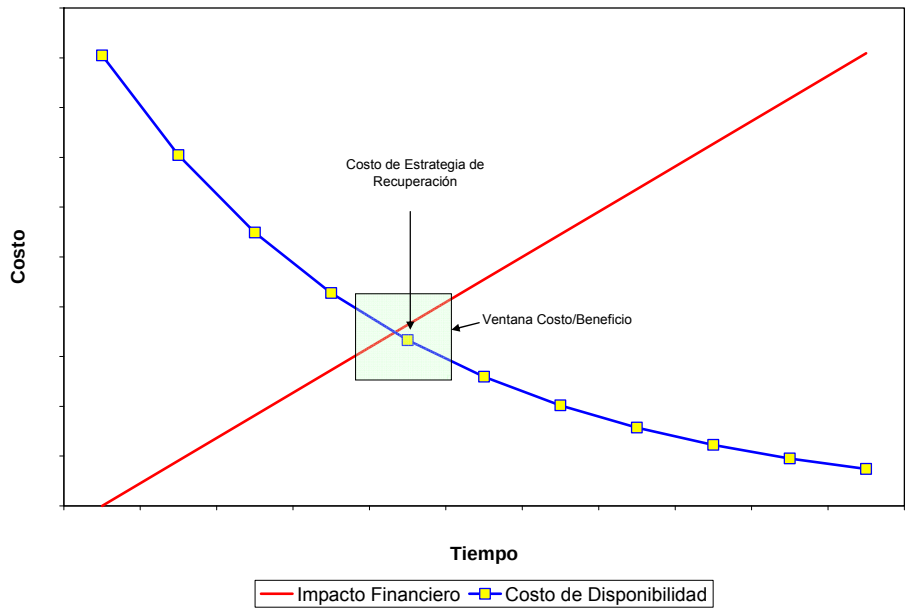
Figura 14. Gráfica de impacto financiero



Fuente: Instituto Internacional para la Recuperación de Desastres. **Curso de administración de continuidad de negocios para profesionales avanzados**. Pág. 4.45

Luego de haber construido las dos gráficas anteriores, las unimos en la figura 15 Análisis de Costo-Beneficio que se muestra a continuación, de esta forma se define la ventana costo-beneficio alrededor de la intersección de ambas gráficas en donde se espera encontrar la estrategia más acertada en cuanto al costo y el beneficio que implica la protección de la pérdida esperada.

Figura 15. Gráfica de análisis de costo-beneficio



Fuente: Instituto Internacional para la Recuperación de Desastres.
Curso de administración de continuidad de negocios para profesionales avanzados.
Pág. 4.47

Con la gráfica Costo-Beneficio se realizan varios análisis, por ejemplo en el lado izquierdo tenemos la línea de costo financiero en un valor bajo, cercano a cero, mientras la línea de costo de disponibilidad en un valor alto, esto debido a que las soluciones que tienen un tiempo de recuperación bajo son caras, entre más cercano a cero más cara será la solución de recuperación. Por el lado izquierdo de la gráfica tenemos la línea de pérdida financiera con un valor alto, lo que implica que entre más tiempo pase la interrupción mayores serán las pérdidas para el negocio, además, podemos ver que la línea de costo de disponibilidad tiene unos valores bajos, esto debido a que entre mayor sea el tiempo de recuperación más baratas son las soluciones, como por ejemplo el no

invertir nada y esperar el momento del desastre para salir a comprar los equipos necesarios para recuperar.

El dibujar una ventana de costo-beneficio alrededor de la intersección de ambas líneas, la de impacto financiero y costo de disponibilidad, asegura que lo que se invierta en la solución para recuperar está en la relación directa con lo que perderá el negocio por una interrupción. Esta es el área en donde se espera poder operar, es la ventana de costo-beneficio tal como se muestra en la figura 15.

Como podemos observar este es un método directo para poder escoger la estrategia que mas le conviene implementar a la empresa basado en el costo y beneficio que podrá recibir por ella al implementar esta estrategia.

5.3 Factibilidad técnica

Para las estrategias de recuperación de centrales de telefonía celular podemos identificar varias clases: MSC en grupo, MSC en espera, MSC única. El análisis de factibilidad técnica está orientado al desarrollo de la solución interna o al de servicios comerciales que cumpla con la estrategia seleccionada.

Los proveedores frecuentemente comercializarán su tecnología "patentada", utilizarán conceptos no conocidos para las personas de la empresa. Cuando se realiza el proceso de comparación de proveedores o verificación de la solución se utilizará el principio de mantener todo simple y evitar usar terminología propia del proveedor. Si resulta confuso asegurarse de comprender todo lo que se está ofertando, esto es muy útil para comparar soluciones de distintos proveedores. Requerir del proveedor pruebas de concepto para asegurar que la solución realmente funciona validando contra el tiempo objetivo de recuperación o RTO *(Recovery Time Objetive)* definido en el análisis de impacto del negocio o BIA *(Business Impact Analisys).*

En cada una de las estrategias propuestas es importante analizar el riesgo de la misma en cuanto a procesos del negocio, tecnología y personal que la ejecutará. En el caso de la tecnología muchos de estos riesgos son minimizados al implementar un modelo de "Prueba y Compra" *(Try & Buy),* esto debe ser solicitado al proveedor como parte del proceso de selección de la estrategia, si la solución es desarrollada internamente por la empresa también es importante hacer pruebas periódicas de la misma para asegurar el correcto funcionamiento de la misma sea invocada en caso de desastre.

Si en la implementación de la estrategia es necesario ejecutar procesos manuales, se recomienda automatizar estos procesos con la creación de secuencias de comandos o *Scripts* para reducir el tiempo de ejecución y asegurar la ejecución correcta en el momento que se necesite. Además de la implementación de un plan de pruebas frecuente para asegurar que la solución funciona adecuadamente y mejorar la capacidad de ejecución del personal en caso que se necesite.

CONCLUSIONES

1. Debido a los desastres naturales y provocados por el hombre que han afectado a varios países alrededor del mundo, la norma BS 25999 se ha difundido grandemente convirtiéndose en una de las normas más aceptadas para el desarrollo de planes de Continuidad del Negocio a nivel gobierno y empresas privadas.

2. Para tener una mayor probabilidad de supervivencia de las empresas de telefonía celular durante y después de un desastre es importante tener un plan de Continuidad del Negocio que se enfoque en las personas, las localidades, la tecnología y la información necesaria para las mismas.

3. A nivel mundial la tecnología celular más utilizada es GSM, en Guatemala los tres operadores celulares tienen esta tecnología. Las topologías disponibles para utilizar en la estrategia de las centrales telefónicas son *Stand Alone*, *Standby* y en *Pool* para determinar la mejor se debe evaluar la etapa del ciclo de vida en la que se encuentra el negocio, y hacer un análisis costo beneficio.

4. Para el diseño de las estrategias para las centrales de telefonía celular el análisis de la tecnología se debe dividir en dos: tecnologías de la información (sistemas administrativos y de gestión) y tecnologías de la operación del negocio o red celular.

5. Antes de hacer estrategias de recuperación para centrales de telefonía celular ante desastres, se debe hacer un análisis de impacto al negocio y una evaluación de riesgos de los servicios, productos y procesos, para generar estrategias con base a los requerimientos identificados.

6. Para diseñar las estrategias de Continuidad del Negocio para centrales de telefonía celular se divide el análisis en las siguientes cuatro áreas vitales: personal, localidades, tecnología e información. Para cada una de estas áreas existen varias alternativas de respuesta y la combinación de las alternativas seleccionadas es la estrategia óptima de recuperación del negocio.

7. Este trabajo de graduación puede ser utilizado por cualquier tipo de empresa privada o gubernamental para generar sus estrategias para la recuperación en caso de desastres.

RECOMENDACIONES

1. Es importarte contar con un plan de Continuidad del Negocio como factor fundamental para la sobrevivencia de las empresas durante y después de un desastre, sin importar el tamaño, tipo y ubicación de las mismas.

2. Se debe utilizar una metodología de clase mundial, como la norma BSI 25999, para el diseño de las estrategias de recuperación de las centrales de telefonía celular.

3. Se debe hacer un análisis de costo beneficio y determinar en qué fase del ciclo de vida se encuentra la empresa antes de implementar cualquier estrategia de recuperación de las centrales de telefonía celular.

4. Las compañías de telecomunicaciones deben poner especial importancia en las estrategias de recuperación de la tecnología, porque es el componente fundamental de su negocio.

5. Los profesionales de Ingeniería deben buscar la certificación en Continuidad del Negocio para tener mayores posibilidades en el campo profesional.

BIBLIOGRAFÍA

1. Balaouras, Stephanie and Schreck, Galen. **Maximizing data center investments for disaster recovery and business resilience by for IT infrastructure & operations professionals**. October 5, 2007

2. British standard, BSI 25999, business continuity management – Part 1: Code of practice. UK: BSI, 2006.

3. Bueno, E. **Enfoques principales y tendencias en dirección del conocimiento: gestión del conocimiento, desarrollos teóricos y aplicaciones**. Cáceres. Ediciones La Coria, 2002.

4. **Continuity insights staff special report: risk & continuity - How they relate and integrate**. Issue archive: may/june 2009

5. Ericsson MSC *Pool*. **Presentación**. Septiembre 2009

6. Millicom Guatemala. **Mobile softswitch solution. New Generation and Swap. Proposal**. Septiembre 2009

7. Okolita Kelley. **Issue archive: november/december 2009 final thoughts – A little practical advice.**

8. Probst G, Raub y Rombahardt, K. **Administre el conocimiento**. México, D.F. Pearson Educación. 2001.

9. Snedaker, Susan. **Continuity & disaster recovery for IT professionals.** EEUU: syngress publishing, Inc., 2007.

10. Wallace, Michael y Webber, Lawrence. **The disaster recovery handbook. EEUU: Amacom** , 2004.