DECANATO DE ESTUDIOS DE POSTGRADO E INVESTIGACIONES
ESPECIALIZACION EN GERENCIA Y TECNOLOGIA DE LAS TELECOMUNICACIONES
PROFESOR: Ing. Vincenzo Mendillo

Prevención y Recuperación de Desastres - Caso de estudio: Centro de Operaciones de Telefonía Celular.

Ing. Carlos Enrique Atencio Figuera
Carnet No.3181230
Caracas, Octubre del 2005.

DERECHO DE AUTOR

Cedo a la Universidad Metropolitana el derecho de reproducir y difundir el presente trabajo, con las únicas limitaciones que establece la legislación vigente en materia de derecho de autor.

En la ciudad de Caracas, a los 03 días del mes de Octubre de 2005.

_____

Ing. Carlos Enrique Atencio Figuera

APROBACIÓN

Considero que el Trabajo de Grado titulado

Prevención y Recuperación de Desastres - Caso de estudio: Centro de Operaciones de Telefonía Celular.

Elaborada por el ciudadano:

_____

Ing. Carlos Enrique Atencio Figuera

para optar por el título de

Especialista en Gerencia y Tecnología de las Telecomunicaciones

Reúne los requisitos exigidos por la Escuela de Ingeniería Eléctrica de la Universidad Metropolitana, y tiene méritos suficientes como para ser sometido a la presentación y evaluación exhaustiva por parte del jurado examinador que se designe.

En la ciudad de Caracas, a los 02 días del mes de Octubre de 2005.

_____

Ing. Vincenzo Mendillo

RESUMEN

Prevención y Recuperación de Desastres - Caso de estudio: Centro de Operaciones de Telefonía Celular.

Autor:

Ing. Carlos Enrique Atencio Figuera

Tutor: Ing. Vincenzo Mendillo Caracas.

El siguiente trabajo se desarrolla con la finalidad de establecer un método estructurado en forma general y especifica para desarrollar un plan de contingencia de un centro de operaciones de una empresa de telecomunicaciones.

Se toma en cuenta tanto la seguridad del personal, las instalaciones, el respaldo de la información, el mantenimiento y recuperación de los procesos informáticos e internos para asegurar la continuidad de las operaciones en el tiempo. Se plantea la posibilidad de establecer un sitio alterno en caso de desastres y se establecen pautas para realizar su ubicación y equipamiento.

Índice

LISTA DE TABLAS Y FIGURAS

Tablas

Figuras

Introducción

En la actualidad las telecomunicaciones en Venezuela se considera como la actividad económica de mayor crecimiento a nivel nacional en sus distintos sectores como son la telefonía fija, celular y transmisión de datos.

Las compañías que ofrecen servicios de telefonía deben garantizar el buen funcionamiento del servicio las 24 hrs. los 365 días al año.

A medida que las empresas se han vuelto cada vez más dependientes de telecomunicaciones para manejar sus actividades, la disponibilidad de los sistemas informáticos se ha vuelto crucial. Actualmente, la mayoría de las empresas necesitan un alto nivel de disponibilidad y algunas requieren incluso un nivel continuo para sus operaciones, ya que les resultaría extremadamente difícil funcionar sin las telecomunicaciones.

En caso de un desastre, la interrupción prolongada de las telecomunicaciones puede llevar a pérdidas financieras significativas y la credibilidad del público o los clientes y como consecuencia, la empresa puede terminar en un fracaso total.

Por lo tanto, la capacidad para recuperarse exitosamente de los efectos de un desastre dentro de un periodo predeterminado debe ser un elemento crucial en un plan estratégico de seguridad para una organización.

Imagínese una situación que interrumpa las operaciones de las computadoras durante una semana o un mes y la pérdida de todos los datos de la empresa, todas las unidades de respaldo del sitio y la destrucción de equipos vitales del sistema ¿Cómo se manejaría semejante catástrofe? Si Ud. se ve en

esta situación y lo único que puede hacer es preguntarse ¿Y ahora qué ? ¡ ya es demasiado tarde ! La única manera efectiva de afrontar un desastre es tener una solución completa y totalmente probada para recuperarse de los efectos del mismo.

Objetivos

Descripción del trabajo:

Elaborar un plan de contingencia para un centro de operaciones de telefonía celular.

Objetivos a desarrollar:

- Analizar aquellos aspectos de la empresa que necesitan ser mejorados en caso de riesgos imprevistos y plantear mejoras a nivel de medios de comunicación, conexión del centro de operaciones con el sistema celular y redundancia de los sistemas informáticos de monitoreo y control.
- Organizar un plan de entrenamiento teórico - práctico para el personal que labora en el centro de operaciones en caso de contingencia.
- Realizar un estudio de los requerimientos necesarios para un nuevo centro de operaciones, a nivel de infraestructura, equipos y personal calificado.
- Diseñar un plan de transición en las operaciones de la compañía basadas en un solo centro de operaciones a dos centros de operaciones funcionando en paralelo.

¿Qué es un desastre?

Según el diccionario Larousse :

Desastre “Desgracia grande, suceso infeliz y lamentable.”

Se pueden conseguir varias definiciones de desastres: “Termino empleado para definir un acontecimiento repentino que interrumpe el normal desenvolvimiento de la población, física o emocionalmente.”

En el contexto de este trabajo utilizaremos la siguiente definición:

“Interrupción prolongada de los servicios de telecomunicaciones o informáticos prestados por una organización, que no pueden corregirse dentro de un periodo de tiempo aceptable y es necesario la utilización de un sitio o equipo alterno para su recuperación.”

Causas obvias son los grandes incendios, las inundaciones, los terremotos, las explosiones, los actos de sabotaje, etcétera.

Tipos de desastres

Aunque es imposible proporcionar una lista completa de todos los tipos de desastres, pueden identificarse varias categorías:

Los desastres locales son eventos limitados a un área, cuarto o lugar específicos de un edificio (por ejemplo, la sala de computación). Este tipo de desastre puede ser resultado de:

- Incendio
- Inundación
- Falla irreparable del equipo

- Sabotaje
- Falla en el suministro de energía eléctrica

Los desastres en el sitio afectan a todo el edificio y pueden ser causados por eventos como:

- Inundaciones
- Bombas
- Explosiones de gas
- Incendios
- Daño de trasformadores de electricidad

Los desastres de área por lo general afectan la zona donde se localiza el edificio. Esta zona puede cubrir un radio de varios kilómetros y pueden ser causados por:

- Terremotos
- Erupciones volcánicas
- Huracanes y tornados
- Caídas de aviones
- Bombas
- Ataques terroristas
- Motines y saqueos
- Contaminación química o nuclear
- Epidemias

En algunas de las situaciones anteriores, puede ser que el equipo de procesamiento de datos siga intacto aún y que sea utilizable, pero que resulte sencillamente inaccesible. Con una planeación previa, se podrá dirigir el centro de datos desde una ubicación remota por un corto periodo.

Estadísticas recientes sobre los tipos más comunes de desastres a nivel mundial muestran que el terrorismo y los incendios son las causas más comunes.

Tabla 1. Frecuencia de desastres por tipo en el mundo.
Fuente: Contingency Planning Research Inc. Estos datos están basados en 57 incidentes de desastres desde 1988.

Terrorismo	17.5 %
Incendio	17.5 %
Huracanes y tornados	14.0 %
Terremotos	10.5 %
Interrupción de suministro de energía eléctrica	9.5 %
Errores en hardware	5.3 %
Interrupción de servicio en la red	3.5 %
Rotura de tuberías	3.5 %
Otros	2.9 %

Venezuela ante los desastres

La segunda quincena de diciembre de 1999, Venezuela sufrió una de las mayores catástrofes de su historia. Durante ese mes, en la franja costera del país, se registraron precipitaciones extraordinarias, siendo el Estado Vargas, ubicado en la parte norte del país, uno de los mas afectados y en menor dimensión y no menos grave por las afectaciones: el Distrito Federal de Caracas, los estados de Miranda, Carabobo, Yaracuy, Falcón y, más al occidente, Zulia y Táchira.

El desastre causó la muerte de miles de personas, y las cifras (aún no conocidas con exactitud), oscilan entre los 10.000 y 20.000 muertos y más de 5.000 desaparecidos, 100.000 personas fueron afectadas directa o indirectamente por el desastre. Los daños y pérdidas materiales se estimaron en más de 3.000 millones de dólares[1] y puso en evidencia la significativa vulnerabilidad de la población frente a las situaciones de amenaza y, por ende, su limitada reacción para responder o manejar adecuadamente ante la ocurrencia de fenómenos naturales peligrosos. El desastre de diciembre de 1999 puso en evidencia una serie de vulnerabilidades, problemas y carencias, muchas de ellas asociadas a formas y modos de subsistencia, a actitudes y formas de convivencia con el entorno natural y socio institucional; a fragilidades de las instituciones en cuanto a aplicar mecanismos de control, normar y planificar el territorio; en cuanto a generar

[1] Fuente CEPAL según datos de CONAVI y OCEI.

información hidrometeorológica en tiempo real y de utilidad para movilizar poblaciones; al no uso o inexistencia de instrumentos y herramientas que permitan manejar situaciones de preparativos y emergencias ante desastres, etc. Ejemplos que ilustran la carencia de políticas orientadas a la gestión y reducción de riesgos y a manejar adecuadamente esos momentos de la emergencia, lo señalamos con los planes de ordenación territorial que recién en estos últimos años se les incorporan la variable de riesgo; o simplemente con el hecho de la falta de planificación urbana o de habilitación de barrios u ocupación descontrolada de cauces y quebradas[2]. También podemos mencionar como ejemplo que, en pleno proceso del periodo de ocurrencia del desastre, era clara la existencia de estructuras organizativas y administrativas orientadas fundamentalmente a la atención y respuesta, pero con limitada capacidad operativa (tanto de recursos humanos como de materiales y equipos tecnológicos).

Es en estos últimos años, coincidentemente con lo ocurrido por los desastres en Venezuela, se viene notando un gran interés y preocupación por el tema de la reducción de los riesgos, entendiéndolo en su dimensión integral. Sin embargo, pesar de estos importantes avances y desarrollos institucionales, no se puede afirmar de que exista aún una cultura de Gestión de Riesgo en el conjunto o totalidad de la sociedad venezolana, en sus instituciones, en sus políticas y en sus poblaciones en general. Es usual escuchar en autoridades y estudiosos del tema, el sostener que fue el desastre y específicamente el- desastre de Vargas- lo que marcó un hito en Venezuela. Es el punto de referencia que sirvió de impulso para

[2] Según el censo de población de 1990 el 44% de la población del área de Caracas viven en 144 barrios localizados en distintas jurisdicciones municipales, representando más de 1 200,000 personas. El 75% de estos barrios están localizados en los municipios del Libertador y Sucre.

que algunos sectores, organismos públicos y privados evalúen el que hacer en cuanto a desastres y emergencias a la fecha, y en estrategias y formas de intervención que con lleven a revertir las situaciones de vulnerabilidad y riesgo que precedieron al desastre de diciembre del año 1999.

Venezuela es un país que presenta alto nivel de riesgo, como resultado de gran número de población asentada en zonas expuestas a un conjunto de amenazas. Algunas características generales de riesgo en Venezuela[3] muestran lo siguiente:

- Poblaciones, equipamientos e infraestructuras de servicios, ciudades y comunidades y, en general, un país que presenta un alto grado de vulnerabilidad cuya tendencia es, lamentablemente, de constante incremento.

- Áreas y territorios en donde las inundaciones, los deslizamientos, los incendios, los sismos, las tormentas tropicales, contaminación, etc. son elementos innatos de su naturaleza e historia; es decir un territorio en donde estas amenazas han existido, existen y seguirán progresivamente manifestándose;

[3] Fuente: Tomado del documento Estrategia de rehabilitación y reconstrucción de Venezuela preparado por una Misión del expertas del PNUD –ERD (BCPR).Abril 2001.

- Un territorio donde los desastres son hechos recurrentes, forman parte de la historia de sus poblaciones y de manera determinante se relacionan con los procesos de desarrollo de sus comunidades y ciudades;

- Sociedades que, de una u otra manera, se han organizado y han desarrollado una serie de prácticas para enfrentar y responder a los desastres y que tienen que ver con qué y cómo hacer en las etapas del antes, durante y después. No obstante, pese a los esfuerzos invertidos en estos años, hechos como los sucedidos en diciembre de 1999 y en febrero del 2005 (Lo sucedido con la llamada “lluvias de carnaval” en sólo 5 día, del 7 al 12 de Febrero de 2005, en pleno lunes de carnaval se produce una las más fuertes vaguadas que se registrara en los últimos años, sin llegar a la magnitud de afectaciones como lo ocurrido en diciembre de 1999, pero que pone en evidencia la alta vulnerabilidad de gran parte del país. Esta vaguada afecto el Estado Falcón quién fue la primera entidad afectada por su paso, para luego propagarse hacia toda la región norte costera de Venezuela pasando por los estados centrales de Aragua y Carabobo, y afectando fuertemente al Distrito Capital, al estado Vargas y la Región Andina específicamente el Estado de Mérida.), evidencian que lo realizado no es suficiente cuando se trata de reducir el riesgo a desastres, ya que ésta es una gestión que demanda acciones planificadas y concertadas, con una perspectiva de corto, mediano y largo plazo.

A esta realidad debemos sumarle la presencia de las siguientes amenazas[4]:

- Alta sismicidad: presencia de un sistema de fallas sobre el cual se encuentran asentados los estados intervenidos, situación que les dan una predisposición sísmica importante. El área de intervención pertenece a una región sísmico- tectónica activa que constituye la zona de contacto y desplazamiento de las placas del Caribe y América del Sur.

- Alta propensión a la ocurrencia de fuertes precipitaciones, vientos, mares de fondo y oleajes: el área de intervención reviste una alta probabilidad de ser afectada por la persistencia de lluvias extraordinarias de gran intensidad.

- Elevado potencial de generación de movimientos de masa: la persistencia de lluvias extraordinarias de gran intensidad, bajo ciertas condiciones físicas genera movimientos en masa (deslizamientos o derrumbes).

- Alta probabilidad de producción de sedimentos y de ocurrencia de inundaciones: la persistencia de lluvias intensas activa los procesos de infiltración en las cuencas, desarrollándose procesos de erosión y arrastre de sedimentos, rocas y materiales. Todas las cuencas evidencian condiciones naturales (pendiente, topografía, rugosidad, lechos

[4] Fuente: Plan Operativo Global 2004 del Programa PREDERES “Prevención de Desastres y Reconstrucción Social en Vargas”, cofinanciado por la Comunidad Europea y el Gobierno Bolivariano de Venezuela

encajonados) que les asignan un alto potencial de producción de sedimentos e inundaciones.

- La inestabilidad de sus laderas y las características hidráulicas de sus áreas ubicadas en cauces de quebradas y conos de deyección: que la hacen susceptible de verse afectada por derrumbes, crecidas o por la ocurrencia de flujos torrenciales.

La alta gerencia tiene que decidir el periodo predeterminado que lleva una interrupción de servicio de la situación de "problema" a la de "desastre". La mayoría de las organizaciones logran esto llevando a cabo un análisis de impacto en el negocio para determinar el máximo tiempo de interrupción permisible en funciones vitales de sus actividades.

La reanudación de las actividades ante una calamidad puede ser una de las situaciones más difíciles con las que una organización deba enfrentarse. Tras un desastre, es probable que no haya posibilidades de regresar al lugar de trabajo o que no se disponga de ninguna de los recursos acostumbrados. Incluso, es posible que no se pueda contar con todo el personal. La preparación es la clave del éxito para enfrentar los problemas.

No existe ninguna manera para protegerse completamente contra todo tipo de riesgos, particularmente amenazas naturales a gran escala que pueden arrasar zonas extensas. Como consecuencia, siempre se tiene que tolerar algún riesgo residual. La decisión sobre el alcance del desastre para el que habrá de prepararse debe tomarse en los más altos niveles de la empresa. Por ejemplo, la

mayor parte de las empresas implementan una estrategia que proteja contra desastres locales, pero pocas cubren desastres a nivel nacional o incluso internacional. Asimismo, las organizaciones que cuentan dos o más sitios, pueden tener una estrategia de recuperación que funcione en caso de que un sitio sea destruido o dañado, pero no si varios sitios son destruidos o dañados al mismo tiempo.

Un plan de contingencia es el proceso de determinar qué hacer si una catástrofe se abate sobre la empresa y es necesario recuperar la red y los sistemas.

Desdichadamente, un plan de contingencia es como el ejercicio y la dieta: más fácil pensar en ello que hacerlo. Por lo general tiende a dejarse para una ocasión posterior. Uno de los problemas asociados al plan de contingencia es saber por dónde empezar.

Metodología para un plan de contingencia

Antes de realizar un plan de contingencia para recuperación de desastres, se debe tener un cuenta que no es una tarea fácil y se deben hacer las siguientes consideraciones:

1. Debe ser diseñado y elaborado según sean las necesidades de la empresa.
2. Puede requerir la construcción o adaptación de un sitio alterno.
3. Requerirá del desarrollo de nuevos procedimientos que deben ser compatibles con los existentes y debe participar personal de todas las áreas de la compañía que sean claves para su funcionamiento.

4. Es un compromiso entre costo, tiempo de recuperación y alcance de la solución y desastres cubiertos.

Un forma de empezar a realizar un plan de contingencia en seguir un método organizado donde se tomen en cuenta todos los aspectos. A continuación se enumeran las principales actividades requeridas para el desarrollo:

1. Identificación y evaluación de riesgos
2. Asignar prioridades y establecer los requerimientos de recuperación
3. Elaborar de la documentación
4. Verificar la implementación del plan, distribución y mantenimiento del plan.

Identificación y evaluación de riesgos

La primera fase del plan de contingencia es el análisis de riesgos. En esta fase, la preocupación está relacionada con tres simples preguntas: ¿qué está bajo riesgo?, ¿qué puede ir mal? y ¿cuál es la probabilidad de que suceda?. La evaluación de riesgo implica la cuantificación de los costos implicados a una interrupción de las actividades por un desastre.

La mayoría de las compañías de telefonía celular instalan un centro único de operaciones de la red, donde se ejecutan los procesos de monitoreo y atención de fallas de la red celular y sus elementos de valor agregado manteniendo el control y la operatividad. También allí se resuelven y canalizan la resolución de problemas reportados por los clientes tanto internos como externos, a fin de dar una respuesta eficiente y garantizar la pronta solución de las deficiencias que afectan el servicio.

Situaciones anormales como los desastres naturales o eventos causados por el hombre (como disturbios callejeros y actos vandálicos) a puntos claves de la infraestructura de la red, pueden ocasionar la perdida total o parcial de la gestión y atención de las fallas por personal calificado. De igual forma la integridad física de los empleados se ve comprometida, al no estar preparados para afrontar esta clase de eventualidades.

La carencia de planes estratégicos genera los siguientes problemas y consecuencias:

Tabla 2. Problemas y Consecuencias
Fuente: Elaboración Propia

Problema	Consecuencia
➢ Falta de planes de desalojo en caso de situaciones como Incendios, terremotos, inundaciones etc.	➢ Perdida de vidas al no desalojar en tiempo y de forma adecuada las instalaciones.
➢ Falta de planes de acción en caso de situaciones de protestas civiles y disturbios callejeros.	➢ Personas atrapadas en su sitio de trabajo por falta de seguridad a su integridad física.
➢ Falta de conocimiento en la utilización del sistema de extinción de incendios por parte del personal que labora en las instalaciones del centro de operaciones de la red.	➢ Perdidas humanas en caso de incendios ➢ Perdida de la infraestructura y equipos dedicados al monitoreo de la red celular. ➢ Descarga accidental de sistema de extinción de incendios.
➢ Falta de redundancia los sistemas de monitoreo, servidores, aplicaciones etc.	➢ Perdida total del conocimiento de las alarmas ocurridas en la red, afectación del servicio celular en

	diversas zonas del país.
➢ Falta de redundancia y respaldo de los sistemas de comunicación con otros puntos y personas clave de la organización.	➢ Sin comunicación con las regiones del país, centrales, personal técnico y proveedores de servicios, etc.,

Como se ha mencionado anteriormente, el realizar un plan de recuperación contra desastres que cubra todos los riesgos posibles es prácticamente imposible, por esto necesario responder a la pregunta ¿cuál es la probabilidad de que suceda?. Si se contara con una cantidad de recursos ilimitados, esto carecería de sentido ya que, por ejemplo, se podría intentar proteger los sistemas e infraestructura contra un ataque nuclear o la caída de un meteorito, lo que es algo improbable que suceda.

En relación a los costos asociados ocasionados por un desastre, nos basaremos en las fallas operativas que no puedan ser atendidas y gestionadas por el centro de operaciones y que hayan sido identificadas como las actividades principales generadoras de ingresos de la compañía, por ejemplo como lo señala los indicadores de CONATEL la mayoría de los clientes son aquellos que tienen la modalidad de pago “prepago” que consiste en cancelar el costo de la llamadas antes de realizarlas.

Esto quiere decir que la falla operativa mas importante es que uno de los servidores que procesan las llamadas de los clientes que están en prepago quede fuera de servicio por una falla que afecte la realización de las llamadas.

Tabla 3: Telefonía móvil suscriptores según modalidad de pago
año 1997 - 2004
Fuente: Observatorio Estadístico. Conatel
(*): Cifras preliminares basadas en la Encuesta Agregada de los Principales Indicadores del Sector. Conatel.

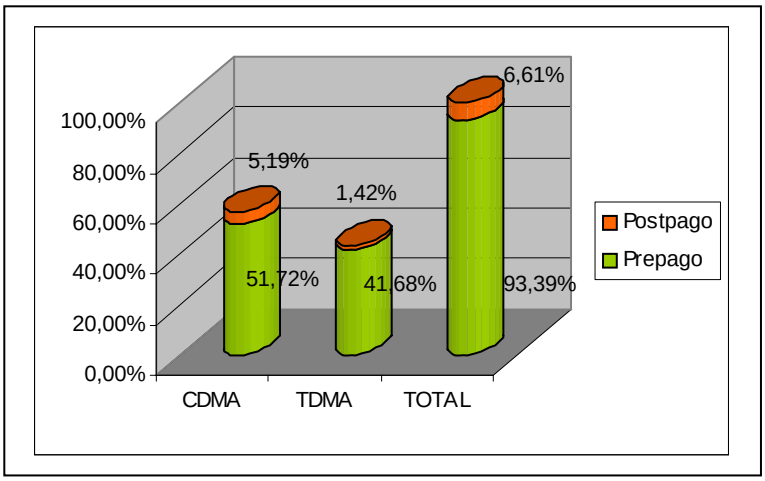
Año	Postpago	Prepago	Total Suscriptores
1997	698.183	404.765	1.102.948
1998	843.053	1.166.704	2.009.757
1999	641.706	3.143.029	3.784.735
2000	592.209	4.854.963	5.447.172
2001	542.519	5.930.065	6.472.584
2002	534.836	6.007.058	6.541.894
2003	496.209	6.518.912	7.015.121
2004(*)	560.960	7.860.020	8.420.980

Tabla 4: Distribución de los clientes según modalidad de pago Telecomunicaciones Movilnet al 31 de julio de 2005.
Fuente: Indicadores internos Telecomunicaciones Movilnet C.A.

Tecnología utilizada	**Prepago**	**Postpago**
CDMA	1.928.307	193.480
TDMA	1.553.853	52.792
TOTAL	**3.482.160**	**246.272**
	Prepago	**Postpago**
CDMA	51,72%	5,19%
TDMA	41,68%	1,42%
TOTAL	**93,39%**	**6,61%**

PREPAGO	3.482.160	93,39%
POSTPAGO	246.272	6,61%
TOTAL CLIENTES	**3.728.432**	**100,00%**

Figura 1. Distribución de los clientes según modalidad de pago Telecomunicaciones Movilnet al 31 de julio de 2005.
Fuente: Indicadores Internos Movilnet

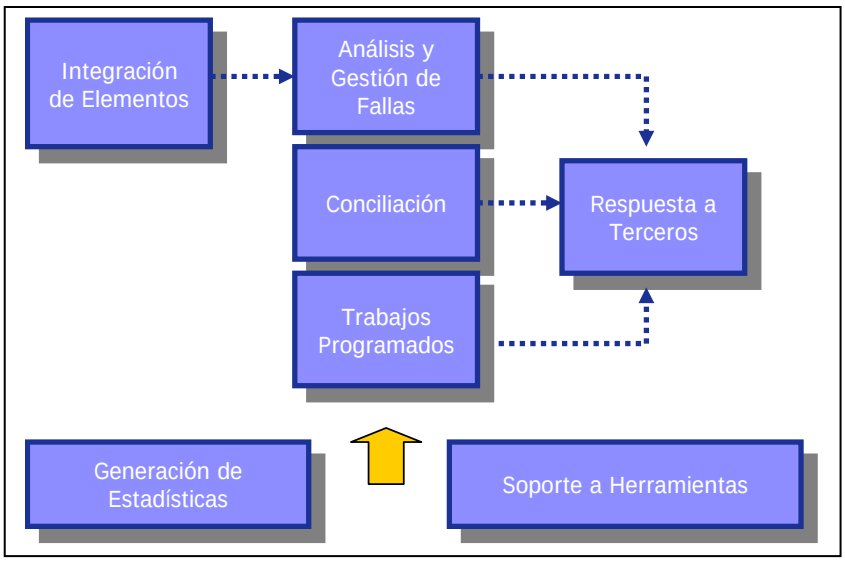


Asignar prioridades y establecer los requerimientos de recuperación

En esta fase se debe establecer el alcance del plan de contingencia en relación a qué desastres o acontecimientos anormales se puede actuar y tener una respuesta eficaz. Se deben implantar niveles de jerarquía entre los procesos y aplicaciones mas importantes y necesarios para recuperar lo antes posible el normal funcionamiento de las actividades.

En el caso de un centro de operaciones de telefonía celular, se deben identificar cuales son los procesos mas importante y cuales tienen un efecto mayor en la red celular.

Figura 2. Procesos Claves Centro de Operaciones Telecomunicaciones Movilnet c.a.
Fuente: Indicadores Internos Telecomunicaciones Movilnet c.a.



Como se puede apreciar en la Figura 4, un ejemplo es el caso de Telecomunicaciones Movilnet C.A.. El centro de operaciones tiene distintos procesos los cuales dependen entre si y trabajan en conjunto para realizar el trabajo final, que es velar por el buen funcionamiento del sistema celular.

Estos procesos están encargados de las siguientes labores:

- *Integración de elementos:* se ocupa de poner en funcionamiento nuevos componentes del sistema celular, como estaciones base y servicios de valor agregado.
- *Generación de estadísticas*: realiza la función de generar reportes detallados sobre los elementos que fallan en el sistema celular.
- *Soporte a Herramientas:* su función es cuidar por el buen funcionamiento de los programas informáticos utilizados por el centro de operaciones.
- *Conciliación*: proceso mediante cual se llega a acuerdos con otras operadoras como CANTV, Movistar, Digitel etc. en la duración de fallas donde varias operadoras intervienen para solucionar la falla.
- *Análisis y Gestión de Fallas*: es el proceso mas importante dentro del centro de operaciones ya que es el encargado de diagnosticar, atender las fallas del sistema celular en primera instancia. En caso de no poder resolverse en forma remota, se involucra a personal especializado, sea de la compañía o entes externos.

- *Trabajos programados:* en este proceso se controlan y se aprueban los cambios a realizar en el sistema celular ocasionados por una falla o una mejora a la red celular y que impliquen o no afectación de servicio.
- *Respuesta a terceros*: este es el segundo proceso mas importante dentro del centro de operaciones, ya que mediante él, se notifican y se escalan las fallas en el sistema celular al personal calificado.

Debido a esto y las causas expuestas anteriormente sobre la situación ante desastres en la que se encuentra Venezuela y en especial Caracas, sólo se analizarán los desastres mas comunes que puede ocurrir localmente, dándole prioridad a la seguridad del personal y a los procesos mas importantes dentro de un centro de operaciones, como es la atención de fallas y notificación al personal calificado.

Una forma tentativa de estructurar los alcances del plan de recuperación para el centro de operaciones es la siguiente:

- Fallas operativas: son aquellas que comprometen la funcionalidad de los sistemas informáticos dentro del centro de operaciones y los cuales son necesarios para realizar su labor. Entre ellas podemos encontrar las siguientes:
    - Falla en la red de computadores que integran el centro de operaciones.
    - Fallas en los medios de comunicación.
    - Falla en el suministro eléctrico.

- Desastres naturales: son eventos causados por la naturaleza de intensidad no controlable por el hombre y que en ocasiones sus consecuencias son irrecuperables. Para esta clase de eventos se deben tomar la mayor cantidad de medidas de protección de acuerdo al prepuesto disponible. Entre estos contamos los siguientes:
    - Incendios.
    - Inundaciones.
    - Terremotos.

- Desastres causados por el hombre: se refiere a toda clase de sucesos que puedan alterar en normal desenvolvimiento de las actividades de las compañía. Entre ellas tener a los sabotajes, motines y disturbios.

Campos de Acción

Para asegurar el monitoreo, la gestión el control de fallas y la seguridad del personal, se debe tener en cuenta los siguiente:

- Medios de comunicación
- Conexión del centro de operaciones con el sistema celular.
- Redundancia de los sistemas de monitoreo.
- Centro de operaciones redundante o alterno.
- Cultura de seguridad.

Medios de Comunicación

Los sistemas de comunicación mas utilizados en un centro de operaciones son la telefonía celular y la telefonía fija. Cuando ocurren situaciones de contingencia, los sistemas de comunicaciones tradicionales como la telefonía fija y los sistemas celulares colapsan ya que no están diseñados para atender a todos los usuarios en un mismo instante de tiempo, sumándole a esto tenemos que los equipos principales como los servidores que procesan las llamadas de los usuarios no garantizan un funcionamiento óptimo a toda su capacidad, lo cual tiene como consecuencia la dificultad al tratar de comunicarse con el personal necesario para la atención y resolución de fallas, ya que se congestiona el sistema celular.

Para evitar esta clase de inconvenientes, se recomienda utilizar medios de comunicación alternos como teléfonos celulares de proveedores diferentes, telefonía satelital y sistemas radio de dos vias.

Para utilizar un medio de comunicación alterno se debe tener en cuenta los siguiente:

- Ventajas y desventajas de cada uno
- Inversión de los equipos a instalar.
- Permisología especial en caso de ser necesaria.
- Costo
- Manejo del equipo

Se podrían considerar tres propuestas como medios de comunicación alternos:

- Radios de Onda Corta.
- Telefonía Satelital.
- Teléfonos celulares de otras operadoras.

Radios de Onda Corta

Esta clase de equipos son muy comunes hoy en día aunque con el avance de la tecnología la tendencia es que sean utilizados por grupos de personas o empresas para sus comunicaciones internas, sin la necesidad de intermediarios.

Instalar un sistema de radios de onda corta requiere de una permisología adicional. Para este caso el ente regulatorio de las telecomunicaciones debe asignar al usuario frecuencias en una parte del espectro radio eléctrico para su uso exclusivo, y se deben cancelar los impuestos que esto amerita. Para tener una cobertura igual a la red celular instalada o como mínimo poder tener una comunicación sin intermediarios (es decir sin el uso de repetidores), es necesario utilizar una gran potencia de transmisión a frecuencias bajas en la banda de 80 mts. o 40 mts. El gran tamaño de las antenas y su infraestructura son de difícil manejo lo cual incrementa los costos operativos en el orden de 10 veces más de un equipo celular tradicional.

Telefonía Satelital

Este medio de comunicación, a diferencia de los demás, funciona en forma similar a un sistema celular, pero con la particularidad que su radio base o estación repetidora es un satélite. Para su utilización no es necesario ninguna clase de permisología adicional. Este teléfono es similar a teléfono celular normal

pero que por las altas frecuencias que estos utilizan, la antena de transmisión debe tener una posición especial.

El Inconveniente que este sistema presenta es en la interconexión con las otras operadoras. Se realiza por uno o dos enlaces E1 utilizando la red de telefonía convencional. Esto quiere decir que al ocurrir eventos que impliquen la saturación del sistema de telefonía tradicional, la comunicación se verá afectada. La única posibilidad de impedir esto es que se realice la comunicación entre dos teléfonos satelitales, en donde no se vea involucrada la red de telefonía convencional.

Celulares de otras operadoras:

El uso de equipos celulares convencionales de otras operadoras, no garantiza la comunicación en caso de contingencia, pero si se toma en cuenta que al momento de un desastre natural no todos los sistemas son afectados en una misma magnitud y que estos son independientes entre si, tendremos una comunicación redundante a un costo asequible a cualquier empresa.

Tabla 5: tabla de porcentajes medios de comunicación alterno
Fuente: Elaboración Propia

Sistema a Implementar				
Radios de onda corta	A			
Telefonia Satelital	B			
Celulares de otras operadoras	C			
Consideraciones	Peso	Puntajes		
		A	B	C
Cobertura a nivel nacional	60%	0,5	1	1
Sin necesidad de intermediarios	15%	1	0,5	0,1
Sin Permisologia Especial	5%	0,3	1	1
Costo	10%	0,2	0,4	1
Facil Manejo	10%	0,2	0,7	1
Total	100%	50,50%	83,50%	***87%***

Tabla 6: Comparación de costos entre medios de comunicación alternos.
Fuente: Elaboración propia.

<table>
<tr><th colspan="2"><u>Sistema de radio de onda corta.</u>[5]</th><th colspan="2"><u>Telefonía satelital</u>[6]</th><th><u>Celulares comunes</u>[7]</th></tr>
<tr><td rowspan="3">Componentes basicos</td><td><u>Equipo de mano</u>
 
Fabricante: ICOM
Modelo : IC-W32A
Rango : 2M/440 HT
Precio $289.9</td><td colspan="2"><u>Teléfono satelital</u>
  </td><td rowspan="3"> 
  </td></tr>
<tr><td><u>Estación base</u>
Fabricante: ICOM
Modelo: IC-756PROIII
Rango: HF+6M
Precio $2999.99</td><td colspan="2"><u>Fabricante: Globalstar</u>
<u>Modelo: SAT-550</u>
<u>Precio: $ 550</u>
<u>Renta Básica: $ 24</u></td></tr>
<tr><td>  </td><td colspan="2">Estación base
Modelo:FAU 200 - Fixed Phone
Precio: $625.00
Renta Basica: $ 22
  </td></tr>
</table>

Una vez identificados los procesos claves del centro de operaciones, se deben establecer prioridades de recuperación y tiempos máximos, tolerables para cada falla así como acciones a tomar en cada caso. Como se menciono anteriormente, el proceso fundamental sobre el cual están basadas las actividades de un centro de operaciones son la gestión y atención de fallas operativas del sistema celular; para esto se debe asegurar la conexión con la red celular. De

[5] Fuente: http://www.hamradio.com/
[6] Fuente: http://www.globalstar.com.ve/
[7] Fuente: http://www.movistar.com.ve/

igual manera se debe realizar un inventario de las aplicaciones necesarias para realizar dicha labor, estableciendo las relaciones y prioridades entre ellas y su tiempo de recuperación.

Para elaborar el diseño de la solución de recuperación es necesario determinar los siguientes requerimientos para cada aplicación y para todos los datos:

1. El máximo tiempo aceptable de “caída” para cada aplicación (pérdida de servicio)

2. La máxima cantidad tolerable de pérdida de datos en un desastre (pérdida de datos)

3. La actualidad que los datos deberán tener cuando se reanude el servicio. La actualidad de los datos se define como una medida de la aproximación del nivel de los datos restaurados con el nivel de datos en el momento del desastre. Por lo general, los datos pueden restaurarse al nivel del respaldo más reciente, o al de los registros acumulados de las transacciones. Este nivel tal vez sea diferente del que exista en el momento del desastre.

4. Requerimientos de la capacidad del hardware en el sitio alternativo como:

- Capacidad del procesador (poder de procesamiento, almacenamiento, canales)
- Capacidad de disco, en gigabytes, por modelo y tipos - Número de unidades de cinta, por modelo y tipos.

- Requerimientos de impresión como capacidad, número de unidades y destino
- Otro equipo específico, como scanners (o digitalizadores) y lectores de documentos

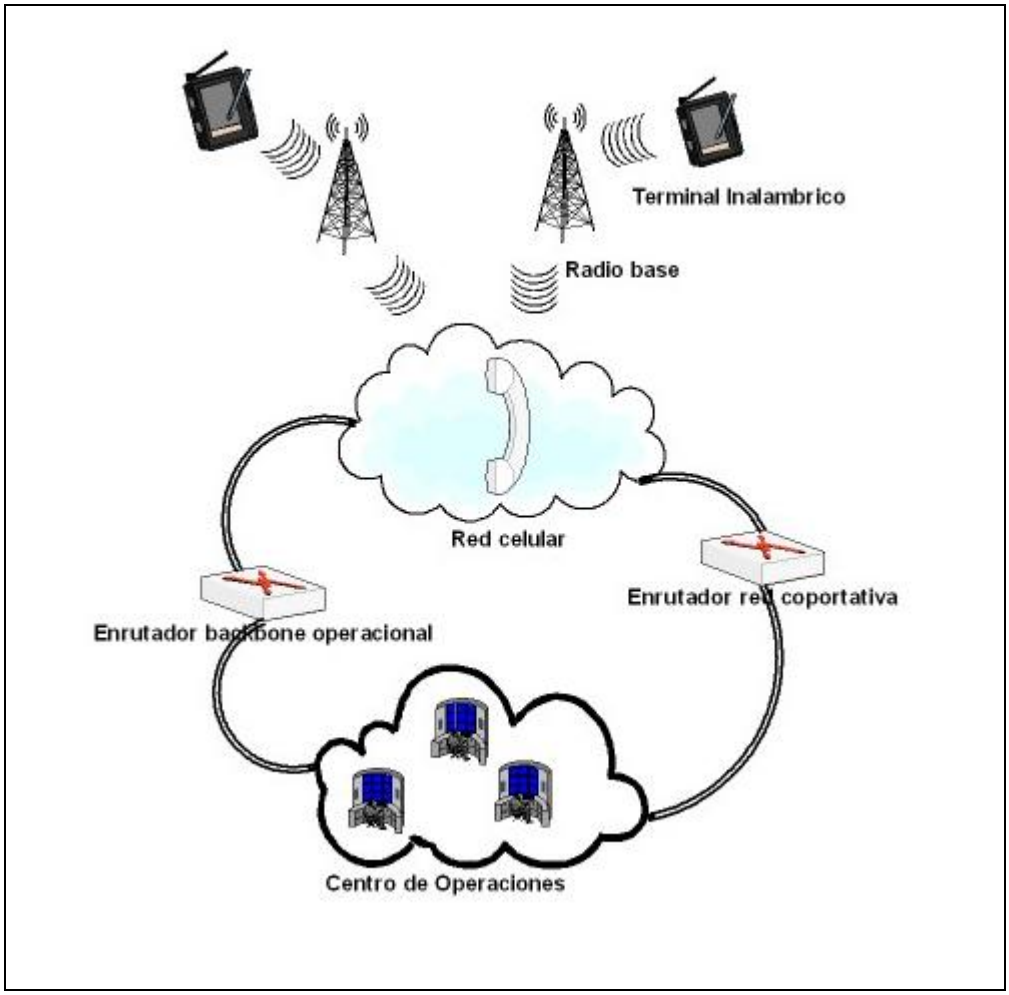
5. Requerimientos de red que se relacionan con:
   - Topología del respaldo
   - Máximo tiempo tolerable de la caída
   - Ancho de banda de la transmisión
   - Cuáles departamentos estarán conectados en modo de recuperación de desastres
   - Los niveles de servicio que se habrá de mantener después del desastre.

Para asegurar la conexión con la red celular en todo momento, se debe asegurar por diferentes medios. Por ejemplo, distintas redes de acceso a los equipos, una red alámbrica y una inalámbrica como la proporcionada por los distintos operadores de telefonía celular, son las redes celulares con capacidad de transmisión de datos a alta velocidad. Por ejemplo Telecomunicaciones Movilnet dispone de una red CDMA (Code Division Multiplexing Access) con celdas EVDO (Evolution Data Only) la cual permite un acceso inalámbrico a Internet a velocidades de transmisión y recepción de datos entre 500 kbps y 2400 kbps.

Un modelo de conexión viable incorporaría a los computadores dedicados al monitoreo a dos segmentos de red distintos, pero con capacidad para poder acceder a los mismos equipos finales, como por ejemplo: radios bases o celdas, centrales de conmutación, STP, HLR etc., esta se puede realizar utilizando una

red de área local de uso común por todos los usuarios de la compañía. También se debe considerar el uso de una red de uso dedicado para el acceso a los elementos claves del sistema celular y en la medida que sea posible, se debe implementar el uso de un sistema de monitoreo inalámbrico y que pueda gestionar los equipos primordiales desde cualquier sitio donde halla cobertura celular. En el caso de Telecomunicaciones Movilnet se utilizan las tres vías de conexión como lo muestra la Figura 5.

Figura 3.Esquema de conexión del centro de operaciones Movilnet.
Fuente: Elaboración propia



Programas o gestores de monitoreo.

Una vez que se ha determinado los requerimientos de recuperación de las aplicaciones y que se ha evaluado la interdependencia entre ellas y sus datos, el resultado es un inventario de aplicación, como se ilustra en la tabla 11.

Tabla 7: Modelos de tabla de inventario de aplicaciones.
Fuente: Elaboración propia.

	NIVEL CRÍTICO	DURACIÓN DE LA INTERRUPCIÓN DEL SERVICIO	MÁXIMA PÉRDIDA DE DATOS	DATOS A LOS QUE SE TIENE ACCESO	INTERRELACIÓN CON OTRAS APLICACIONES
Aplicación 1	medio	18 horas	últimas 3 horas	depósito 1 de base de datos	aplicación n, DB2
Aplicación 2	bajo	36 horas	últimas 500 transacciones	depósito de procesamiento por lotes	flujo de procesasamiento por lotes XYZ
Aplicación 3	alto	10 minutos	Ninguna	depósito 2 de base de datos	Ninguna
....					
Aplicación n					

	UNIDADES DE RENDIMIENTO DEL PROCESADOR	ALMACENAMIENTO DEL PROCESADOR (MEGABYTES)	ALMACENAMIENTO DEL DISCO (GIGABYTES)	CARGA DE RED (BIT/SEG)	VOLUMEN DE IMPRESIÓN (PÁGINAS/DÍA)
Aplicación 1	7.0	7	1.1	2x9600	10,000
Aplicación 2	6.1	12.8	3.6	2x64k	40,000
Aplicación 3	1.4	6.2	0.4	1x4800	5,000
Aplicación n	. . .	. . .	. . .	. . .	. . .
Total	32.0	96 MB	70 GB		160,000

La gestión de los equipos que forman la red celular se realiza con herramientas que son suministradas por el fabricante. Esto tiene la ventaja de contar con el soporte técnico especializado en caso de falla las 24 hrs.. La desventaja es el tiempo de respuesta que requiere el equipo de soporte técnico

del fabricante para solventar un problema en un equipo o en uno de los programas que administra. Para disminuir el tiempo de atención de fallas, se debe contar con programas desarrollados de acuerdo a las necesidades de la empresa, alternos a los desarrollados por el fabricante y que puedan gestionar a los equipos involucrados e irse adaptando a las necesidades del tiempo. De esta forma se disminuyen los costos adicionales por soporte técnico externo.

Centro de Operaciones Alterno

El tiempo entre un desastre y el principio del trabajo del segundo sitio debe ser corto. Es posible una rápida recuperación, si el segundo sitio está listo en todo momento, con el hardware requerido completo e instalado y todos los datos a un nivel actual.

Para desarrollar un segundo centro de operaciones que funcione en paralelo con el actual, se debe tener en cuenta lo siguiente:

a. Plan de transición en las operaciones entre los dos centros de operaciones y posteriormente dividir las zonas de atención.
b. Selección de la ubicación geográfica idónea para su construcción e instalación, en donde se aprovechen al máximo los recursos instalados de la empresa.
c. Requerimientos del centro de operaciones: realizar una lista a nivel de equipos, espacio y personal necesarios para su instalación.

a . Plan de transición en las operaciones

Un centro de operaciones alterno puede funcionar en conjunto o únicamente en situaciones de contingencia con el principal. Su utilización será decisión de la alta gerencia de la compañía y como periodo de transición en las operaciones del Monitoreo a dos centros de operaciones se pueden tomar como ejemplo los siguientes planes:

PLAN A: Centro de operaciones primario con 100 % de la carga y alterno en stand by.

- ✓ Ventajas:
  - ❖ - Todo centralizado en un mismo lugar.
  - ❖ - Fallas masivas a nivel nacional gestionadas desde un mismo sitio.
- ✓ Desventajas:
  - ✓ No se aprovechan los recursos instalados en el centro de operaciones redundante constantemente.
  - ✓ Solo es utilizado en casos de emergencia.

PLAN B: Centro de operaciones primario y alterno con 50 % de la carga.

- ✓ Ventajas:
  - ✓ Se hace uso de los recursos asignados al centro de operaciones alterno.
  - ✓ Se centraliza la atención y gestión de fallas por zonas y regiones, disminuyendo su tiempo de resolución.

- ✓ Asegura el monitoreo y atención de la red en todo momento.

- ✓ Desventajas:
  - ✓ Reubicación o contratación de personal extra para su puesta en marcha y funcionamiento.

Plan para monitoreo en paralelo:

<u>Puntos Preliminares</u>

- Determinar la cantidad de personas necesarias para poner en funcionamiento el centro de operaciones redundante, con la mitad de la carga de trabajo.
- Realizar una encuesta entre las personas que trabajan en el principal y estarían dispuestas a trasladarse a la ubicación del centro de operaciones redundante, antes de que empiece a funcionar en su totalidad.

<u>Plan de Puesta en marcha:</u>

Monitorear en forma paralela en ambos centros de operaciones con 100 % de carga por un período de tiempo donde el centro de operaciones primario lidere la gestión y atención de fallas. Luego se distribuiría las regiones entre ambos centros de operaciones.

<u>b. Selección de la ubicación geográfica.</u>

Para realizar la elección correcta se deben tomar en cuenta lo siguiente:

- ➢ Sismicidad: es la cantidad de movimientos telúricos que ocurren en un lugar en un periodo de tiempo y se mide por la intensidad y magnitud,

(definiciones estas completamente diferentes, que en muchas ocasiones se confunden).

- **Intensidad sísmica:** Los efectos producidos por los terremotos en las estructuras y en las personas, se mide por medio de la Intensidad sísmica, describiendo de una manera subjetiva el potencial destructivo de los sismos. La Intensidad sísmica depende de los siguientes factores:

- Distancia del sitio al epicentro. Mientras más lejos se encuentre del epicentro, menor será la intensidad y los efectos.

- Tipo de suelo en que se encuentran las edificaciones; se conoce que los suelos blandos pueden amplificar las ondas sísmicas causando más daño.

- De la topografía del lugar. Por ejemplo, si una construcción se encuentra al borde de una ladera, tendrá mayor probabilidad de daño que una que se encuentre en un terreno completamente plano.

- Depende de la resistencia de las estructuras. Una edificación que es sismo resistente presentará menos daño que una que no lo es.

- Depende también del grado de preparación de la gente, en el sentido de saber tomar precauciones para evitar accidentes.

- **Magnitud sísmica:** Los sismógrafos son equipos que miden la amplitud del movimiento de la tierra y el registro en papel se llama sismograma. En base a estos registros se determina la magnitud de un sismo. La magnitud de un evento sísmico mide la energía liberada en el hipocentro. Este concepto se fundamenta en el hecho de que la amplitud de las ondas sísmicas es una medida de la energía liberada en el foco o hipocentro.

Actualmente Venezuela se encuentra divida en zonas según el grado de aceleración del suelo. Esto representa la magnitud y la intensidad con la que pueden ocurrir en dicha zona geográfica los movimientos telúricos, sin que este sea el grado de aceleración (aumento de velocidad) máximo del suelo. Es un patrón definido con fines de ingeniería para la construcción de edificaciones sismo resistentes en Venezuela según la norma Covenin 1756-2001.

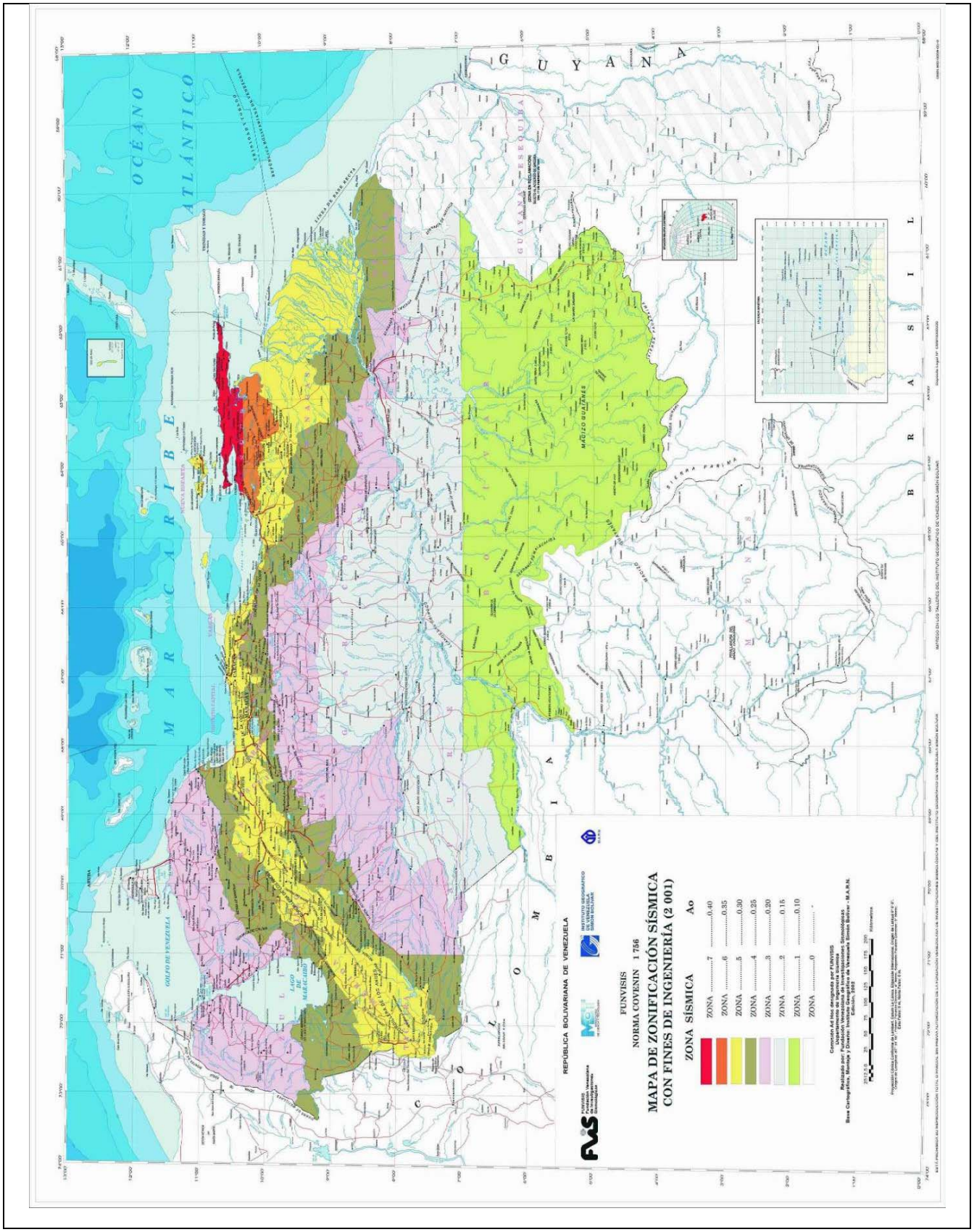


Figura 4. Mapa de Zonificación Sísmica
Fuente: http: //www.funvisis.gob.ve

Tabla 8. Intensidad y Magnitud sísmica vs. Aceleración del Suelo
Fuente: Elaboración Propia

Intensidad (MERCALLI)	**Magnitud** (RICHTER)	**Tipo**	**Efectos**	**Aceleración del Suelo (g)**	**Zona**
I	Hasta 2.5	Muy Suave	No se siente.	0.1	**1**
II	2.6 - 3.1	Suave	Percibido solo por algunas personas en reposo.	0.15	**2**
III	3.1 - 3.7	Ligero	Percibido por una parte pequeña de la población.	0.20	**3**
IV	3.7 - 4.3	Moderado	Sentido por personas en movimiento, algunas personas dormidas se despiertan.		
V	4.3 - 4.9	Algo Fuerte	Se despiertan las personas.	0.25	**4**
VI	4.9 - 5.5	Fuerte	Percibido por todos, caminar inestable, árboles y materiales se agitan por el efecto del sismo.	0.30	**5**
VII	5.5 - 6.1	Muy Fuerte	Dificultad para mantenerse en pie. objetos colgantes se caen, se pueden producir pequeños derrumbes y deslizamientos.	0.35	**6**

VIII	6.1 - 6.7	Destructivo	Colapso parcial de estructuras, daños considerables en edificios.		
IX	6.7 - 7.3	Ruinoso	Daños considerables en estructuras, especialmente construidas; colapso de edificios y casas; daños generales en bases, presas y diques.	Superiores a 0.40	**7**
X	7.3 - 7.9	Desastroso	Destrucción de la mayoria de las edificaciones, derrumbe de puentes, daños serios en presas y muelles.		
XI	7.9 - 8.4	Muy Desastroso	Pocas estructuras quedan en pie. Fisuras grandes en el terreno.		
XII	Mayor a 8.4	Catastrófico	Destrucción total, grandes masas rocosas desplazadas, objetos lanzados al aire.		

Se debe tener en cuenta la configuración de la red de telefonía instalada y los principales elementos que la conforman y donde se encuentran ubicados para

aprovechar al máximo los recursos de la red y disminuir los costos de infraestructura e ingeniería.

Una forma de presentar los resultados del estudio realizado para escoger la ubicación idónea es la siguiente:

Consideraciones	**Peso**	**Ubicaciones geográficas posibles**		
Equipos instalados		A	B	C
Vías de acceso				
Zona de peligrosidad sísmica				
Sismicidad histórica				
Total				

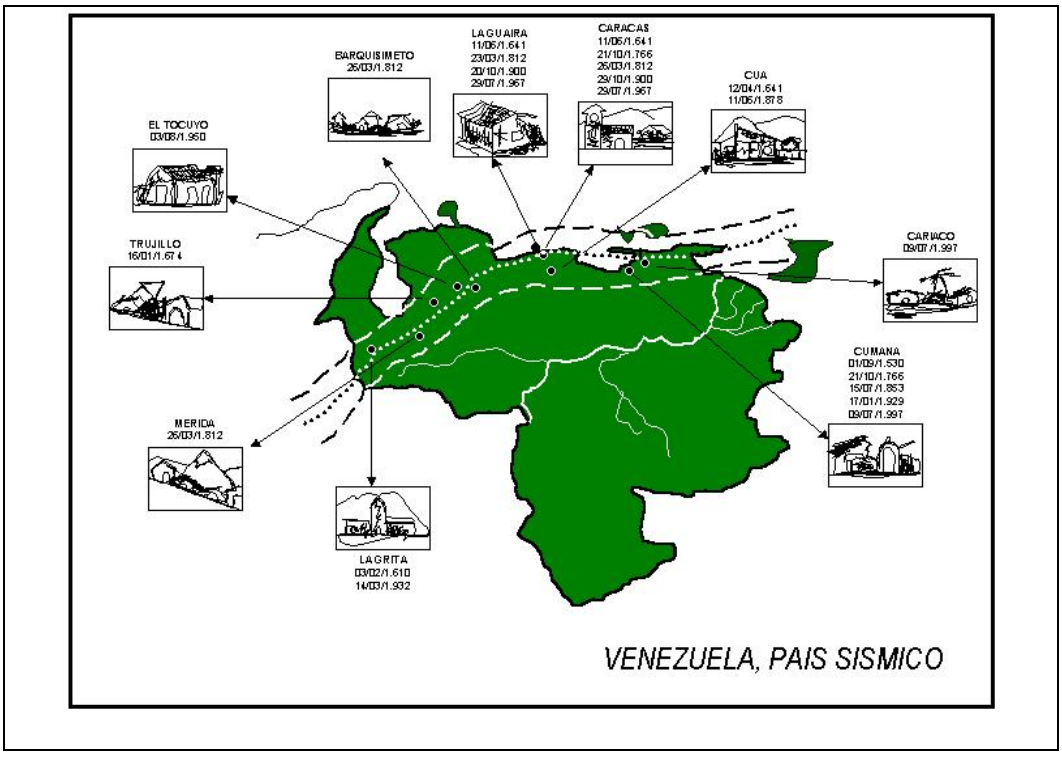
Consideraciones: son los aspectos más relevantes a evaluar según el criterio de la compañía y estos pueden variar dependiendo de sus prioridades. Entre los aspectos que recomienda tomar en cuenta están los siguientes:

- **Equipos instalados:** se refiere a la infraestructura de la compañía, la cantidad, distribución y la importancia de los mismos para la red celular.
- **Vías de acceso:** hace reseña a la facilidad de acceso a la localidad o región donde será instalado el sitio alterno.
- **Zona de peligrosidad sísmica:** según la norma Covenin para, el caso especifico de Venezuela, esta es una forma de dividir el país según el grado de aceleración del suelo, es decir, la velocidad a la cual pudiese llegar el suelo en caso de un sismo o terremoto.

Mientras mayor sea el grado de aceleración mayor será la intensidad y lo daños que éste pudiese causar.

- **Sismicida histórica:** hace referencia a la frecuencia con la que se han presentado movimientos telúricos en la zona geográfica a escoger. De esta información se puede sacar un estudio estadístico de que zona seria la mas adecuada para la instalación de un sitio alterno. En el caso especifico de Venezuela, Funvisis (Federación Venezolana de Investigaciones Sismologicas) puede facilitar esta información.
- **Total:** en este renglón se sumarán las puntuaciones obtenidas en cada renglón y la que tenga mayor puntuación será la locación más adecuada para la instalación del sitio alterno.

Figura 5. Sismicidad Historia en Venezuela
Fuente:http://www.funvisis.gob.ve



c. Requerimientos de un centro de operaciones redundante.

Si se quiere igualar la capacidad del centro de operaciones primario, se debe proceder en primera instancia a realizar un levantamiento de la información del centro de operaciones primario y duplicar los elementos de mayor importancia. Esta información se debe juntar a el inventario de las aplicaciones necesarias para la información sea la indicada al momento de su instalación.

La información puede ser presentada de esta forma en donde se engloba los requerimientos de personal, computadores y espacio de infraestructura necesarios.

Tabla 9. Requerimientos centro de operaciones redundante Telecomunicaciones Movilnet c.a.
Fuente: Dirección del Centro de Operaciones de Telecomunicaciones Movilnet c.a.

Requerimientos Centro de Operaciones Redundante		
Espacio Total 460 mts.^{2}	Sala de monitoreo y control	120 mts.^{2}
	Sala de conferencias	25 mts.^{2}
	Sala de descanso	25 mts.^{2}
	Baños	18 mts.^{2}
	Cocina	20 mts.^{2}
	Oficinas y áreas de uso común	252 mts.^{2}
Conexiones	Red Operacional	5 conexiones E1
	Intranet Corporativa	5 conexiones E1
Consumo de Energía Promedio	10 KVA	
Cantidad de puestos de trabajo en la sala de Monitoreo y Control	Monitoreo y Control	1 Gerente
		1 Coordinador
		5 Analistas
	Soporte a Usuarios	1 Gerente
		1 Coordinador
		7 Analistas

Cantidad de Computadores Necesarios	Analistas de Monitoreo y Control	13 Computadores personales
	Analistas de Soporte a Usuario	8 Computadores personales
	Coordinadores	3 Computadores personales
	Gerentes	6 Computadores personales
	Total	30 Computadores personales

Sistema de Extinción de Incendios	Sistema de extinción de incendios con agente químico FM-200

Pantallas de retro proyección	Dos pantallas de un tamaño de 2 x 2 mts.	Retro proyectores con capacidad de doble lámpara de proyección para mayor durabilidad

Cultura de Seguridad

Para implantar un plan de contingencia, no solo requiere de recursos económicos, también es necesario crear una cultura de seguridad en el personal que se desempeña dentro de las instalaciones.

Se debe instruir a los trabajadores sobre como actuar en la forma correcta ante situaciones de contingencia. Pudiese ser con la implantación de un programa de entrenamiento en conjunto con personal calificado como lo son bomberos y defensa civil. Por ejemplo, en caso de CANTV, este programa de entrenamiento se denomina; Brigada Industrial.

Estos constituyen un órgano con un rol clave en materia de seguridad, está integrado por trabajadores de las distintas áreas de la compañía, cuya función es actuar de acuerdo a una orientación preventiva de la seguridad en las áreas de trabajo, y en última instancia proporcionar asistencia en los casos de accidentes o contingencias en la empresa.

Como una primera Instancia para realizar una preparación ante eventos inesperados, se debe instruir al personal que está presente 24 hrs. en el centro de operaciones a través de un curso iniciación con los siguientes objetivos:

- Desarrollar competencias técnicas para el desempeño como brigadista industrial en conjunto con sus responsabilidades diarias en el área de trabajo, a fin de contribuir al logro del éxito de la gestión preventiva de la empresa.
- Comprender la importancia del liderazgo ante situaciones de contingencia.
- Describir la seguridad industrial como fundamento de la prevención de accidentes laborales y sus modelos preventivos.
- Entender la teoría del fuego (forma es que se produce y se mantiene un incendio), modelos de prevención y combate de incendios con modelos de simulación real
- Conocer las situaciones de riesgo que se presentan durante un desalojo.
- Conocer las diferentes técnicas de primeros auxilios y de traslado de lesionados.

Una vez realizado este curso, se le puede dar la oportunidad al personal que realice otros cursos alternativos para lograr que se sienta como parte activa de la seguridad y se fomente entre el personal la participación en ellos. Entre esos cursos tenemos los siguientes.

- Soporte básico de vida.
- Rescate de personas en ascensores.
- Taller de técnicas de desalojo y ejercicios de simulación.

- Manejo de cuerdas.
- Manejo de estrategias y patrón de búsqueda.
- Sistemas fijos de detección y extinción de incendios.
- Manejo de emergencias.
- Estructuras colapsadas.

Elaboración de la documentación

Además de elaborar los documentos nuevos para el plan de recuperación se deben reorganizar la documentación existente. Esta se puede catalogar en tres tipos de documentos:

1. Manuales y publicaciones oficiales sobre hardware, software, productos, conceptos y soluciones
2. Estándares y procedimientos para operaciones diarias
3. Documentación específica de recuperación de desastres.

Elaborar los documentos para un plan de recuperación es un trabajo extenso y detallado donde se reflejen todas las acciones a tomar en caso de contingencia. Se deben expresar las acciones antes, durante y después; antes se refiere a labores preventivas y mantenimiento del plan, durante es lo referente a las acciones a tomar en caso de una situación anormal y después hace referencia a la gestión necesaria para volver a la normalidad de las operaciones.

El plan de recuperación debe incluir lo siguiente como:

- Alcance y supuestos de la recuperación.
- El proceso para reconocer un desastre y ejecutar el plan.

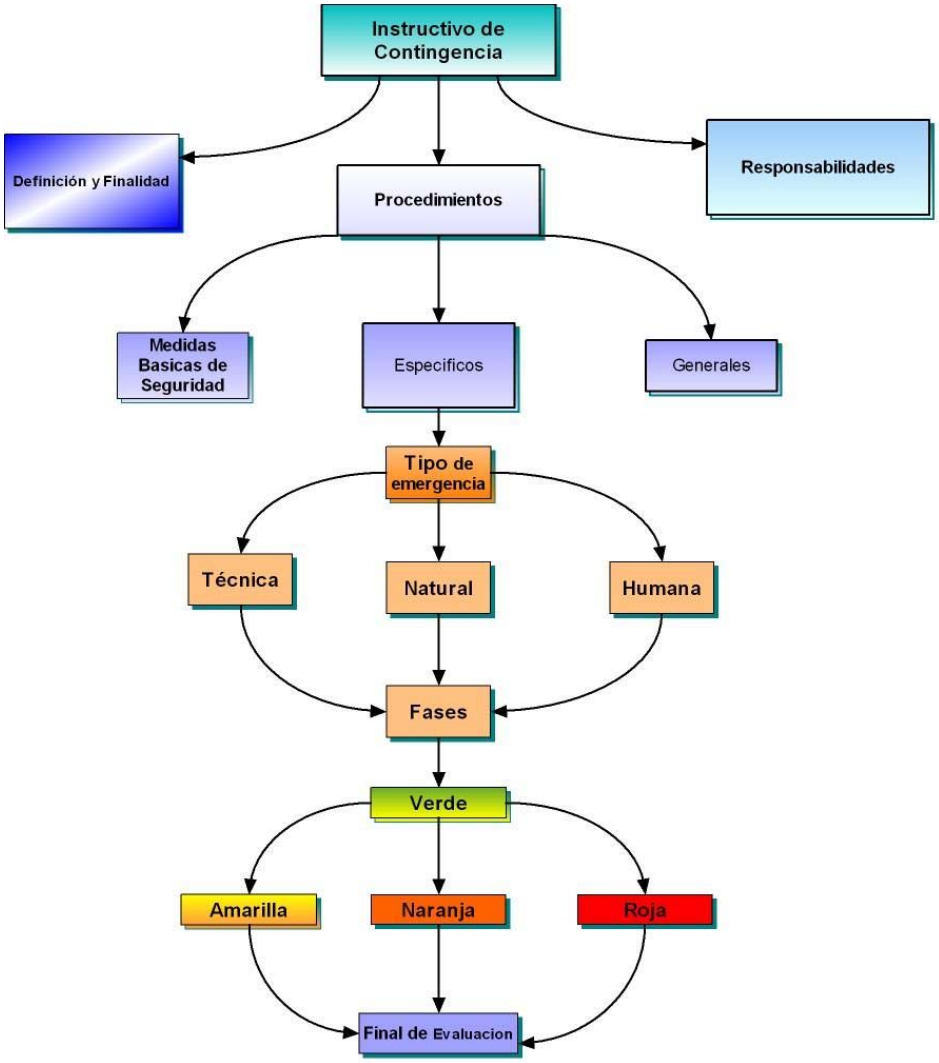
- Identificación de los equipos de trabajo de recuperación y de sus miembros.
- Tareas y responsabilidades principales de los equipos de trabajo de recuperación.
- El propietario del plan.
- La forma en que se probará el plan.

Como en el caso de cualquier proyecto grande, es extremadamente importante que todos los implicados comprendan el alcance del trabajo que habrá de realizarse. El alcance, los supuestos y las directrices generales debieron haberse definido y documentado claramente en el plan de recuperación.

Una forma tentativa de organizar la documentación del plan de recuperación es la siguiente:

- **Definición y finalidad:** se debe expresar que es y para que sirve el plan de contingencia.
- **Responsabilidades:** en este punto se debe expresar las acciones que cada unidad de trabajo debe realizar para el mantenimiento del plan de contingencia y las pertinentes en caso de alguna emergencia.
- **Procedimientos:** aquí se debe estructurar los pasos a seguir como medidas preventivas y básicas de seguridad, establecer los acciones a seguir en caso de alguna eventualidad y especificarlos según sea la intensidad de la situación.

Figura 6. diagrama del instructivo de contingencia
Fuente: Elaboración propia



Definición y Finalidad

Establecer los procedimientos generales y específicos, así como también, definir responsabilidades y niveles de autoridad, necesarios para enfrentar con éxito situaciones especiales resultantes por fallas operacionales, eventos de la naturaleza o actos provocados por terceros que pudieran causar daños o pérdidas de vida de empleados y bienes al centro de operaciones de la

red, con la finalidad de minimizar el impacto en las operaciones y los daños potenciales a las instalaciones de la corporación, apoyados por los planes de emergencia y desalojo.

Procedimientos

Medidas básicas de seguridad ante cualquier tipo de contingencia

1. Reconocer según las características del evento la fase de la contingencia y el impacto que puede tener en la Red de telecomunicaciones y como se ven afectadas las actividades en el centro de operaciones.
2. Mantener la calma
3. Realizar notificación y escalación vía mensajes de texto de acuerdo al nivel de responsabilidad y jerarquía establecido en los procedimientos internos de la compañía .

Generales

1. Confirmar la existencia de eventos que impidan el normal desarrollo de las actividades en el centro de operaciones.
2. Notificar a los niveles de escalación según sea el caso.
3. En caso de ser necesaria la evacuación del centro de operaciones principal, se debe proceder según lo establecido en el plan de desalojo. Se deberán retirar los recursos de contingencia (cintas de respaldo, documentación de backup, medios comunicación portátiles alternos) por el Coordinador de guardia, el Analista de mayor antigüedad y conocimientos de manejo de emergencias.

4. De ser necesario el traslado al centro de operaciones alterno o redundante, se deben realizar los siguientes pasos:
    a. Notificar vía voz al personal en el centro de operaciones alternativo para que se comience para que este comience el monitoreo y la gestión de fallas de la red que ha dejado de ser monitoreada.
    b. El traslado al centro de operaciones redundante se realizará utilizando los medios de transporte establecidos por la alta gerencia. Por ejemplo: vía área y terrestre, se debe establecer una ruta predeterminada con las personas a contactar y las acciones a realizar para el movimiento del personal indispensable.
5. Una vez en el centro de operaciones redundante, se procederá a la actualización vía voz y mensajes de texto a los niveles anteriormente notificados sobre la situación ocurrida.
6. Utilizar solo y exclusivamente los recursos de emergencia en el centro de operaciones (abastecimiento de comida, primeros auxilios, camas portátiles, etc.) en caso de no poder realizar el desalojo de las instalaciones por el personal de guardia.
7. Tramitar ante el personal de seguridad, en caso de ser necesario el uso de salvo conductos al personal de guardia con los organismos competentes.
8. Proporcionar la seguridad necesaria para el traslado a sus destinos al personal de guardia que laborará durante la emergencia.
9. Actualizar el estado de la falla por mensajes de texto al ocurrir algún cambio o hecho relevante en la situación.

10. El coordinador de guardia realizará un informe sobre los eventos ocurridos y el cual será enviado a la alta gerencia.

Específicos

DEFINICION FASES

Fase 1 o Verde: El desarrollo de las actividades se realiza en su normalidad, no hay eventos que pueda afectar el normal desarrollo de las actividades dentro del centro de operaciones.

En caso de ocurrir alguna situación que impida el normal desarrollo de las actividades se deberá activar en forma secuencial 3 fases de contingencia que se definen a continuación.

Fase 2 o Amarilla: Las cctividades en el centro de operaciones se pueden ver comprometidas por distintos factores sin necesidad de realizar una movilización del personal al sitio alterno.

Eventos posibles listados para entrar a fase amarilla:

2.1 Falla en la red del centro de operaciones.

2.2 Falla en los sistemas de comunicaciones del centro de operaciones.

2.3 Falla en el suministro eléctrico.

Fase 3 o Naranja: En esta fase algunas de las actividades del centro de operaciones se ven afectadas por eventos que impiden su normal desarrollo en la sede principal o en sus adyacencias.

. 3.1 Desastres naturales.

3.1.1 Incendios.

3.1.2 Sismos

3.1.3 Inundaciones

3.2 Desastres hechos por el hombre.

3.2.1 Conmoción Social

3.2.2 Sabotaje.

Fase 4 o Roja: Fase de riesgo no controlable por la empresa. Hechos continuos e intermitentes que impiden el desarrollo de las actividades normales del centro de operaciones, tanto en su sede principal como en el redúndate, las labores esenciales de la gestión de fallas de realizarán en forma remota motivado al alto riesgo que recae sobre el personal al movilizarse desde sus hogares, hasta que se pueda activar nuevamente las actividades en el centro de operaciones primario o en su defecto en el redundante.

FASE DE ACTUALIZACION O EVALUACION FINAL

En esta fase el evento que causo la alerta ha desaparecido o ha cambiado su estado, en estos momentos se deben analizar las fallas causadas por la anomalía, realizar un inventario de los daños que englobe las pérdidas humanas y

materiales y causas posibles del evento, con la finalidad de determinar el tiempo estimado de recuperación de actividades a su normalidad, o pasar a una etapa de menor o mayor criticidad.

FASE 2 o AMARILLA

2.1 Falla en la red del centro de operaciones

2.1.1 Chequeo, de ser posible de los sistemas que han sido afectados.

2.1.2 Notificación vía voz y mensajes de texto a los primeros niveles de atención de fallas.

2.1.3 En caso de estar afectada la red, se debe proceder a realizar el monitoreo y control con los equipos que se encuentran conectados a otro segmento de red o en forma inalámbrica.

2.1.4 Actualizar el estado de la falla vía mensaje de texto al ocurrir algún cambio o al realizar alguna maniobra relevante en su resolución.

2.2 Falla en los medios de comunicación del centro de operaciones.

2.2.1 Implica problemas con la central interna de comunicaciones o con las vías regulares de comunicación (líneas de telefonía fija, celulares).

2.2.2 Realizar un chequeo y utilización de sistemas alternos de comunicación. (Sistemas celulares, teléfonos satelitales, etc.);

2.2.3 Notificación vía voz y mensajes de texto a los primeros niveles de atención de fallas.

2.2.4 Actualizar el estado de la falla vía SMS al ocurrir algún cambio o al realizar alguna maniobra relevante en su resolución.

2.3 Falla en suministro eléctrico, centro de operaciones en baterías.

2.3.1 Chequeo de las Instalaciones y equipos informáticos que han sido afectados por la avería. Confirmar si la falla es en todo el edificio.

2.3.2 Confirmar la falla con la compañía de energía eléctrica.

2.3.3 Notificación y escalación a los niveles que sean definidos según la falla.

2.3.4 Actualizar el estado de la falla vía SMS al ocurrir algún cambio o al realizar alguna maniobra relevante en su resolución.

FASE 3 o NARANJA

Eventos que impidan la entrada y salida de las instalaciones: Disturbios callejeros, eventos que afecten la libre circulación a nivel nacional (suspensión de garantías, toque de queda etc.)

Desastres Naturales:

3.1 Incendios

Durante el Incendio:

3.1.1 Buscar el extintor más cercano.

3.1.2 Si el fuego es de origen eléctrico no intentar apagarlo con agua.

3.1.3 Si el fuego es incontrolable, evacuar el centro de operaciones, de acuerdo al plan de desalojo, no usar el ascensor, usar las escaleras.

3.1.4 La ultima persona debe activar el sistema de extinción de incendios, en caso de que éste no se haya activado anteriormente. No se debe cerrar la puerta, sólo ajustarla.

3.1.5 Mantenerse cerca del piso para evitar el humo y los gases tóxicos, así que hay gatear de ser necesario.

Después del incendio:

3.1.6 Se contactará al personal del turno siguiente o de respaldo para que se traslade al centro de operaciones redundante, mientras el personal afectado en el siniestro deberá chequearse médicamente y estar en condiciones de volver a sus puestos de trabajo si es posible o trasladarse al centro de operaciones redundante en su próximo turno de ser necesario.

3.1.7 El centro de operaciones redundante procederá a la actualización vía voz y mensajes de texto a los niveles pertinentes sobre la situación ocurrida.

3.2 SISMOS.

Durante el sismo:

3.2.1 Dirigirse a los lugares seguros previamente establecidos (marcos de puertas, columnas o cimiento de la instalación, o agacharse bajo un

mueble sólido: mesa o escritorio); cúbrase la cabeza con ambas manos colocándola junto a las rodillas.

3.2.2 No apresurarse a salir, ya que el sismo dura solo unos segundos y es posible que termine antes de que lo haya logrado.

3.2.3 Evacue el COR, de acuerdo al plan de desalojo, no usar el ascensor, usar las escaleras.

Después del sismo:

En caso de que las labores de monitoreo no se puedan realizar desde el centro de operaciones primario, el centro de operaciones redundante asumirá la labor de monitoreo y control de toda la red. De no ser así, se notificará al personal de guardia de las distintas áreas para que realice la labor de monitoreo mientras el personal de backup es notificado para realizar las labores de monitoreo en forma remota, hasta que la situación es declarada normal por personal calificado en caso de ser dañada la infraestructura del centro de operaciones.

3.2.4 Se permanecerá fuera de la edificación del centro de operaciones, el tiempo que las autoridades consideren pertinente. Evitar que se encuentre personal dentro del edificio en caso de sismos secundarios.

3.2.5 El personal afectado en el siniestro deberá chequearse médicamente y estar en condiciones de volver a sus puestos de trabajo si es posible o trasladarse al centro de operaciones redundante.

3.2.6 Mientras el personal del centro de operaciones primario es trasladado al centro de operaciones redundante este procederá a la actualización vía voz y mensajes de texto a los niveles pertinentes.

3.3 INUNDACIONES.

Durante la inundación:

3.3.1 En caso que el agua ingrese a la sala de monitoreo, se desconectara la energía eléctrica en los tableros de alimentación donde están ubicados los breakers.

3.3.2 En caso de suspender la labor de monitoreo momentáneamente por peligro a que ocurra un corto circuito, se le notificara al personal de guardia de cada área y al personal del centro de operaciones redundante.

3.3.3 De prolongarse la inundación, se procederá a realizar el monitoreo desde el centro de operaciones redundante.

Después de la inundación.

3.3.4 Se estimará, de acuerdo a los daños ocurridos, el tiempo aproximado en que se pueden reanudar las actividades normales.

3.3.5 Se continuará con el monitoreo en el centro de operaciones redundante hasta que normalice el funcionamiento de los equipos del primario.

3.3.6 Se mantendrá informado a los niveles definidos de la situación del evento.

3.3.7 Una vez controlada la situación, el personal de guardia al turno siguiente se dirigirá al centro de operaciones primario y constatará que se pueden realizar las labores de M&C en forma satisfactoria.

Desastres hechos por el hombre: Sabotaje y daño de instalaciones críticas, actos vandálicos.

3.4 CONMOCION SOCIAL

Durante la conmoción social:

3.4.1 Una vez confirmada la existencia de alguna clase de estos eventos, se procederá a notificar y tramitar con el personal de seguridad interno y los cuerpos de seguridad competentes las medidas necesarias para salvaguardar las instalaciones y la integridad del personal el cual trabaja en el sitio.

3.4.2 En caso de que las actividades en el centro de operaciones se vean afectadas y no se pueda realizar el traslado a sus hogares del personal de guardia o imposibilidad de trasladarse al centro de operaciones alterno, el personal de monitoreo y control permanecerá en el centro de operaciones realizando las labores de monitoreo hasta que el personal del siguiente turno o de respaldo pueda trasladarse al centro de operaciones primario o al redundante dependiendo de los acontecimientos.

3.4.3 En caso de ocurrir suspensión de garantías o toque de queda, se tramitarán salvoconductos de ser necesario con los organismos

gubernamentales necesarios para el personal de guardia, tanto para el centro de operaciones primario como para el secundario.

3.4.4 En caso de ser estrictamente necesario y por seguridad, el personal de guardia permanecerá por su seguridad en las instalaciones del centro de operaciones hasta que puedan trasladarse en forma segura por sus propios medios a sus hogares.

Después de la conmoción social:

3.4.5 La alta gerencia determinará en que momento es seguro restablecer las actividades en el centro de operaciones primario o secundario.

3.4.6 El coordinador de guardia o el analista con mayor antigüedad actualizará el estado de la situación presente en el COR a los niveles que sea requerido.

3.4.7 El personal del centro de operaciones primario o secundario podrá hacer uso de los vehículos de flota en caso de que necesiten movilizarse a sus casas y aun no exista un medio de transporte seguro.

3.5 EN CASO DE SABOTAJE

3.5.1 En caso de que las labores de monitoreo no se puedan realizar desde el centro de operaciones primario, el redundante asumirá todas las labores de monitoreo y control, de no ser así, se notificara al personal de guardia de las distintas áreas para que se realice la

labor de monitoreo mientras el personal de respaldo es notificado para realizar las labores de monitoreo en forma remota.

DESPUES DE SABOTAJE

3.5.2 Se estimarán de acuerdo a los daños ocurridos ya evaluados, el tiempo aproximado en que se pueden reanudar las actividades normales.

3.5.3 Se continuará con el monitoreo en el centro de operaciones redundante hasta que normalice el funcionamiento de los equipos del primario.

3.5.4 Se mantendrá informado a los niveles de la compañía que sea necesario de la situación del evento.

3.5.5 Una vez normalizada las actividades en la sede del centro de operaciones primario se reanudaran las labores de monitoreo y control. Durante el cambio de turno de monitoreo, el personal que labora en el secundario se mantendrá monitoreando hasta que el personal del siguiente turno en el primario constate que las labores de monitoreo se pueden hacer de manera normal.

Responsabilidades

La responsabilidad por la protección de los activos de la compañía es de todos.

La alta gerencia es la responsable por la activación, ejecución y desarrollo del plan de contingencia en caso de situaciones que interfieran con el normal desarrollo de las actividades en el centro de operaciones,

Así mismo, los directores, gerentes, supervisores y coordinadores deberán tener conocimiento apropiado de los pisos de la edificación y dedicar particular atención a aspectos como:

- Canalizar la información respecto a las acciones a seguir en el caso de situaciones que alteren el normal desarrollo de las actividades en la compañía y el centro de operaciones de la red.
- Apoyar la participación del personal entrenado para situaciones de desastre en las prácticas de activación del plan de contingencia y las acciones necesarias para la puesta en marcha del monitoreo desde el centro de operaciones redundante, prevención y extinción de incendios, cualquier otro riesgo y situaciones .

Los *supervisores o cordinadores* deberán asumir las funciones siguientes:

- Liderar la ejecución de prácticas seguras durante las operaciones y trabajos rutinarios, a fin de evitar accidentes o contingencias.
- Mantener disponibilidad inmediata de los números telefónicos de los servicios de emergencias.
- Conservar un registro actualizado de las direcciones y teléfonos de los empleados de sus unidades.
- Verificar que cada persona de su equipo esté familiarizado con las señales de prevención, las regulaciones contra incendios, los procedimientos de

emergencia y que además esté entrenado en el uso de equipos contra incendios.

- Instruir al personal con órdenes claras y precisas sobre los pasos a seguir durante una contingencia de su área.
- Ordenar que se apaguen los sistemas para protección de los equipos.
- En caso de evacuación controlar al personal durante la emergencia, para que éste no se disperse del área de concentración.
- Mantener al personal lejos de los peligros o condiciones riesgosas.
- Coordinar la espera para el retorno al centro de operaciones mientras se llevan a cabo las acciones para normalizar la emergencia.

Verificar la implementación del plan, distribución y mantenimiento del plan

Realizar esta labor no es tarea fácil, ya que requiere no solo un gran esfuerzo de las personas dedicadas a la elaboración del plan de prevención y recuperación de desastres. Requiere también la colaboración de todas las áreas de la compañía, y que todos los integrantes se sientan involucrados en la seguridad tanto personal como la del trabajo que realizan. Una forma de chequear el grado de implementación es realizar simulacros de situaciones de contingencia.

Estos pueden ser a nivel operacional de los sistemas informáticos; como a nivel de personal, realizando por ejemplo evacuaciones controladas con ayuda y coordinación de personal calificado como los bomberos y defensa civil. En estas situaciones, la práctica ante situaciones de emergencia, el conocer los

procedimientos y las acciones a realizar pueden significar la diferencia entre salvar vidas y el negocio y la pérdida total de un segmento o una organización completa.

Una vez que se ha elaborado el plan de recuperación de desastres y que se ha implementado la solución de recuperación, deben ponerse en práctica los procedimientos para mantenerla viable, antes de cerrar el proyecto. Los cambios en las organizaciones y la tecnología son constantes, y cualquiera podría inutilizar el plan de recuperación. Estos procedimientos deben incorporar estos tres elementos distintos:

- Mantenimiento
- Auditoría
- Prueba

Mantenimiento

El propósito de los procedimientos de "mantenimiento" es proporcionar un mecanismo para actualizar la solución de recuperación cuando se hagan cambios en el ambiente que puedan tener impacto en la viabilidad del plan, así como proveer la prueba continua del plan y llevar a cabo la capacitación constante del personal.

Los cambios que pueden afectar a la solución de recuperación pueden provenir de muchas fuentes:

- Desarrollo de nuevas aplicaciones
- Cambios a la configuración actual de hardware
- Cambios a la red
- Cambios organizacionales
- Cambios del sistema
- Cambios al sitio alterno

Auditar el plan

La única manera segura de determinar si se han aplicado los cambios al documento del plan de recuperación de desastres es auditarlos. El contenido del plan debe auditarse de manera semestral o anual tomando en cuenta lo siguiente:

- No deben tomarse todos los datos y documentos para auditoría al mismo tiempo estos deben devolverse en un plazo no mayor de 24 horas a quien los tenía
- Los documentos deben auditarse contra la copia al responsable del plan de contingencia
- Las deficiencias deben anotarse y corregirse antes de devolver el documento a su depositario original
- Debe entregarse un informe a la administración que documente el estado de cada documento de quien conserva el plan (es decir, completo o incompleto)

Además de auditar el contenido de los planes de recuperación de desastres, deben auditarse mensual o bimestralmente todos los componentes importantes del proceso de recuperación. Entre los ejemplos de tales componentes se encuentran:

- La lista de cintas de archivos vitales para asegurarse de que todos los respaldos requeridos se encuentran fuera del sitio.

VI. Conclusiones.

- Un plan de contingencia para desastres es necesario ya que si existe una póliza de seguro puede cubrir los costos materiales de los activos de una organización en caso de una calamidad, no servirá para recuperar el negocio y las perdidas humanas. No ayudará a conservar a los clientes y en la mayoría de los casos, no proporcionará fondos por adelantado para mantener funcionando el negocio hasta que se haya recuperado.
- La creación de un plan de prevención y recuperación de desastres es necesario para asegurar la continuidad de las operaciones de cualquier empresa en caso de catástrofes.
- Un centro de operaciones redundante asegura de una forma eficiente y eficaz la continuidad en el monitoreo y gestión de fallas a nivel nacional, garantizando el servicio a los clientes tanto internos como externos.

- Crear una cultura de seguridad entre los empleados permite una respuesta organizada minimizando los efectos secundarios en las operaciones de la compañía y las perdidas humana

VII. Recomendación

- La Compañía debería disponer previamente de los recursos necesarios para la creación de un plan de recuperación de desastres adaptado a sus necesidades y no descartar la creación de un sitio alterno o de respaldo.
- El plan de recuperación y desastres debe actualizarse en forma periódica y cada vez que se produzcan cambios en la estructura interna de la compañía.
- Se debe mantener un entrenamiento constante en el personal para disminuir el tiempo de reacción antes calamidades y reducir las perdidas humanas.
- Las practicas de pruebas y mantenimiento periódicas aseguran que el plan de recuperación de desastre mantenga un alto nivel con el personal de recuperación y la administración.

VIII. Glosario

Centrales de Conmutación Digital: Encargadas de realizar las conexiones tanto de voz como de datos entre los clientes del sistema.

STP (Signaling tranfer point) Punto de Transferencia de señal: actúa como un punto de transmisión para el procesamiento de llamadas y señalización. Proporciona encaminamiento alternativo para una llamada y administración eficiente entre los elementos de la red.

Radio Bases: Son los elementos que forman la red de acceso inalámbrica a las centrales de conmutación digital permitiendo que los usuarios finales se puedan comunicar desde un dispositivo móvil; su operación varia dependiendo de la tecnología utilizada por ejemplo CDMA, TDMA o GSM.

Backbone Operacional: Red de área local formada por computadores y servidores esenciales para funcionamiento del sistema celular, entre los componentes más importantes se encuentran:

Correo de Voz: su función es almacenar los mensajes de voz de los usuarios al tratar de realizar una llamada y no poder establecerse entre dos clientes.
Servidores de mensajería de texto: se encargan de procesar el envió de mensajes de texto de los abonados.

HLR: Bases de datos de los clientes que forman el sistema celular, en ellas se almacenan los datos personales de los usuarios así como los privilegios que poseen para realizar llamadas en el sistema celular.

Intranet Corporativa: Red de área local encargada de interconectar a los computadores personales de los empleados de la compañía con servidores de uso común como lo son los de correo electrónico y proporcionar un acceso seguro tanto al backbone operacional como a Internet.

Bibliografía

- Kindersley, Dorling (2001), *Guia practica Primeros Auxilios y Emergencias.*

- Fundacion Venezolana de Investigaciones Sismologicas (FUNVISIS)
  - [en línea] Disponible en: http://www.funvisis.gob.ve

- **Centro Sismológico de México.**
  - [en línea] Disponible en: http://www.ssn.unam.mx/SSN/Doc/Cuaderno1/ch3.html

- **Hartford Fire Insurance Company (2001), *Un enfoque Inteligente para proteger su negocio.***
  - [en línea] Disponible en: **http://sb.thehartford.com/sba_spanish/SBA-Guide-Spanish.pdf**

- **Geoportal de Información en geociencias (2005)**
  - [en línea] Disponible en: **http://www.redgeociencias.org.ve/**

- **Análisis Sísmico en Edificios (2005)**
  - [en línea] Disponible en: **http://www.stormloader.com/rman/inb2c11.htm**

- **Mitigación de Desastres Naturales en Sistemas de Agua Potable y Alcantarillado Sanitario - Guías para el Análisis de Vulnerabilidad (Pan American Health Organization (PAHO) / Organización Panamericana de la Salud (OPS), 1998, 110 p.)**
  - [en línea] Disponible en: **http://cidbimena.desastres.hn/docum/ops/publicaciones/h0203s/h0203s.6.htm**

- **Normas Covenin, ARQING consultores**
  - [en línea] Disponible en: **http://www.aqc.com.ve/NormasCOVENIN.htm**

- **Protección Civil Andalucia, España (2005)**
  - [en línea] Disponible en:
    http://www.proteccioncivil-andalucia.org/Emergencias/Sismos.htm

- **Peligros Geológicos (2005).**
  - [en línea] Disponible en:
    http://www.oas.org/usde/publications/Unit/oea65s/ch16.htm

- **Centro de Sismología Universidad de Oriente**
  - [en línea] Disponible en:
    http://csudo.sucre.udo.edu.ve/index.html

ANEXOS

CURSOS BRIGADA INDUSTRIAL CORPORACION CANTV.

Curso de Iniciación de Brigadas Industriales

Practica de RCP

Prácticas de Inmovilización

Practica en Parque Nacional Macarao en conjunto con los Bomberos de Caracas.

Practica de Extinción de Incendios

Curso de Manejo de Cuerdas

Grupo preparado para la práctica

Puesta a punto de los Arneses de Seguridad en conjunto con los Bomberos de Caracas

Practica de Anclajes y Sistemas de Tracción

Sistemas de Extinción de Incendios

Central de incendio AFP - 400 Sistema de detección y alarma de incendio estandarizado

Central de incendio asociada al sistema principal (COR)

Sistema FM-200

Gabinete con Manguera de Extinción de Incendios Sotano COR